Política de Segurança da Informação

SRV-POL-0005	**Política**	Rev.0A 06/02/2024

Nº da revisão	Item	Descrição	Data
0A		Primeira emissão Revisão do antigo CORP-POL-003-Rev.09	06/02/2024

Política de Segurança da Informação

1. PROPÓSITOS E PRINCÍPIOS DA PSI

Esta Política de Segurança da Informação ("**Política**" ou "PSI") tem por finalidade principal promover uma cultura educativa organizacional de proteção aos dados e informações da SERVMAR, de clientes, fornecedores e de parceiros. De forma a atingir este objetivo, esta política atribui responsabilidades, define direitos, deveres, expectativas de acesso e uso e penalidades aplicáveis ao seu descumprimento.

Estabelece, ainda, as diretrizes para criação, transmissão, processamento, utilização, armazenamento, recuperação e descarte de informações a fim de preservar as informações quanto aos seguintes princípios:

- **Integridade:** garantia de que a informação seja mantida em seu estado original, exata e completa;
- **Confidencialidade:** garantia de que o acesso à informação esteja disponível somente para pessoas, entidades ou processos autorizados;
- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

A SERVMAR considera em suas políticas de segurança da informação o processo contínuo no qual os riscos são identificados, analisados, avaliados, tratados e reduzidos a um nível aceitável.

Esta PSI é complementada pelo "Procedimento de Resposta a Incidentes de Segurança Envolvendo Dados Pessoais", que estabelece métodos e responsabilidades dos colaboradores em casos de suspeita ou identificação de violação a informações pessoais tratadas pela SERVMAR.

2. REFERÊNCIAS

- NBR ISO IEC 27001: 2013
- NBR ISO IEC 27002: 2013
- CIS CONTROLS V7.1

3. RESPONSABILIDADES

Colaborador

- É da responsabilidade de cada Colaborador o prejuízo ou dano que vier a sofrer ou causar a SERVMAR ou a terceiros em decorrência da não obediência às diretrizes desta Política.
- Notificar via e-mail do Comitê de Compliance (compliance@servmarambiental.com) e do Encarregado pelo Tratamento de Dados Pessoais (tiago.villarvas@servmarambiental.com) os incidentes, fragilidades ou ainda suspeitas de fragilidades de segurança da informação observadas na SERVMAR. Para mais detalhes, conferir o procedimento SRV-PRO-1378-Resposta a Incidentes".

Política de Segurança da Informação

Gestor

- Incentivar e monitorar o cumprimento desta Política pelos Colaboradores sob sua gestão;
- Garantir a adaptação dos processos, procedimentos e sistemas sob sua responsabilidade para atender à esta Política;
- Definir os níveis de acesso dos Colaboradores sob sua gestão;
- Solicitar os acessos e os recursos para os Colaboradores sob sua gestão;
- Realizar análise crítica periódica das permissões de acesso aos ativos de segurança da informação;
- Definir os níveis de segurança para as informações pertinentes ao seu processo e promover a rotulagem conforme critérios de classificação e tratamento da informação, descritos abaixo; e
- Identificar os riscos associados aos ativos da informação pertinentes ao seu processo e realizar a análise crítica periódica dos riscos associados aos ativos da informação.

Comitê de Compliance

- O Comitê de Compliance é multidisciplinar, composto por representantes dos Departamentos Jurídico, Recursos Humanos, Tecnologia e Segurança da Informação, Qualidade e *Compliance;*
- O Comitê deve tratar de questões, propor soluções, metodologias e processos específicos de segurança da informação. Nesse contexto, é responsável por analisar criticamente esta Política;
- É responsável pela análise de suspeitas de infrações cometidas pelos Colaboradores frente a essa política, devendo examinar a gravidade e riscos sob o enfoque técnico e legal de cada infração cometida e recomendar, após apuração dos fatos, as ações disciplinares cabíveis e, quando aplicável, eventual encaminhamento às autoridades policiais ou judiciais.
- Todos os membros devem participar de um programa de conscientização de segurança, elaborado pelo grupo Servmar a fim de que possam compreender e exibir os comportamentos e habilidades necessários para ajudar a garantir a segurança da organização; e
- Este Comitê poderá ser acionado a qualquer momento pelos Colaboradores para esclarecer dúvidas, obter orientações, expressar opiniões, reportar situações de violação a esta Política ou outros eventos de segurança da informação, por meio da conta corporativa de e-mail compliance@servmarambiental.com.

Diretoria de Recursos Humanos

- Atribuir aos Funcionários, na fase de formalização dos contratos individuais de trabalho a responsabilidade pelo cumprimento desta Política;
- Após o processo de contratação do Funcionário, independentemente do regime de contrato, realizar conscientização sobre segurança da informação e solicitar a assinatura do "Acordo de Confidencialidade";
- No processo de contratação, alinhar com o Gestor da área que deverá solicitar à área de Tecnologia e Segurança da Informação, via formulário, acesso à rede; equipamentos e sistemas;

- Registrar, nos arquivos dos Funcionários, as sanções previstas no Procedimento de Consequências em caso de violação desta política;
- Assegurar que os funcionários estejam conscientes e cumpram as suas responsabilidades pela segurança da informação; e
- Proteger os interesses da empresa como parte do processo de mudança, informando imediatamente à área de Tecnologia e Segurança da Informação sobre a mudança de área, cargo, empresa do grupo e/ou em caso encerramento da contratação.

Tecnologia da e Segurança Informação

- É responsável por realizar treinamento e enviar comunicações aos Colaboradores sobre segurança da informação;
- Segregar as funções administrativas e operacionais a fim de restringir ao mínimo necessário os acessos aos dados de cada indivíduo e reduzir o número de Colaboradores na área de Tecnologia e Segurança da Informação que possam excluir os logs e trilhas de auditoria das suas próprias ações;
- Monitorar e auditar o ambiente tecnológico, implantar sistemas de monitoramento de servidores, correio eletrônico, conexões com a Internet, dispositivos móveis ou *wireless* e outros componentes da rede; e
- Configurar os equipamentos, ferramentas e acesso a sistemas concedidos aos Colaboradores com todos os controles necessários para cumprir os requisitos de segurança da informação estabelecidos nesta Política; e
- Comunicar e divulgar esta política aos Colaboradores, devendo recomendar as medidas que entender cabíveis, incluindo treinamentos periódicos e eventos de conscientização.

4. CONTROLE DE ACESSO

A área de Tecnologia e Segurança da Informação deve manter um inventário de cada um dos sistemas de autenticação da organização.

- Os dispositivos de identificação e senhas devem proteger a identidade do Colaborador, evitando e prevenindo que uma pessoa se faça passar por outra perante a SERVMAR ou terceiros;
- São de responsabilidade do Colaborador quaisquer acessos realizados com o seu identificador/login, por se tratar de dado pessoal e intransferível;
- Todos os dispositivos de identificação utilizados na SERVMAR, como o número do crachá do Colaborador, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm que estar associados a uma pessoa física e atrelados aos seus documentos oficialmente reconhecidos;
- O Colaborador, vinculado a tais dispositivos identificadores, é responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal);

- Devem ser identificados os prestadores de serviço terceirizados, distintamente dos funcionários;
- Deverá constar em todos os contratos da SERVMAR com Colaboradores, o Acordo de Confidencialidade como condição imprescindível para que possa ser concedido o acesso às informações disponibilizadas pela SERVMAR;
- O acesso à informação e às funções dos sistemas de aplicação devem ser solicitados via formulário, com autorização do gestor e devem ser restringidos por meio de controle dos direitos de acesso dos Colaboradores, de forma a limitar quais dados ou funções dos sistemas de aplicação poderão ser acessados por determinado Colaborador e qual o nível de permissão;
- Independentemente do sistema acessado pelo usuário, existe por parte da área de Tecnologia e Segurança da Informação uma revisão periódica semestral de todos os usuários e seus respectivos perfis de acesso, com isso podemos suspender tempestivamente os acessos indevidos a transações críticas, arquivos e/ou sistemas;
- Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários;
- Sempre que possível, os sistemas deverão estar integrados e/ou realizar autenticação com a senha de acesso à rede local; e
- Deve ser considerada a autenticação de múltiplos fatores e canais criptografados, principalmente para contas com privilégios administrativos. Quando esse tipo de autenticação não for suportado (como por exemplo administrador local ou contas de serviço), as contas deverão ter senhas exclusivas. Entende-se como múltiplos fatores, combinações entre:
  - ✓ O que você sabe. Ex: Senha
  - ✓ O que você tem. Ex: Token
  - ✓ O que você é. Ex: Biometria

5. SENHA

- Ao realizar o primeiro acesso ao ambiente de rede local, o Colaborador deverá trocar imediatamente a sua senha conforme as orientações da equipe de suporte, seguindo o número mínimo de caracteres e a complexidade exigida pelo sistema;
- A senha de acesso à rede local expirará automaticamente a cada 6 (seis) meses, sendo o Colaborador notificado pelo sistema a partir de 5 (cinco) dias antes do prazo máximo para sua alteração;
- Quando da renovação da senha, não serão aceitas as últimas 6 (seis) senhas já registradas;
- Em caso de digitação errônea por 3 (três) vezes consecutivas da senha de acesso, a conta será bloqueada;
- A alteração da senha de acesso à rede também poderá ser feita a qualquer tempo pelo próprio Colaborador;
- As senhas não devem ser expostas, compartilhadas ou reveladas a outras pessoas;
- O Colaborador não deve transcrever a senha em papel ou outros meios;

- Em caso de descoberta da senha por terceiros, esquecimento da senha ou bloqueio de conta, a equipe de suporte deverá ser acionada por meio de abertura de chamado no *Service Desk* para troca de senha ou desbloqueio da conta; e
- Senhas de alto nível (Administrador, ROOT ou SA) são de utilização restrita e controlada aos Colaboradores da área de Tecnologia e Segurança da Informação.

6. CLASSIFICAÇÃO E TRATAMENTO DA INFORMAÇÃO

- A definição do grau de sensibilidade para a informação deve possibilitar:
  - ✓ A determinação das salvaguardas mínimas para proteger tais informações; e
  - ✓ A garantia da continuidade operacional de processamento das informações.
- A classificação da informação é de responsabilidade do gestor do processo no qual a informação teve origem.
- Classificação da informação quanto ao sigilo:

Classificação	PÚBLICA	CONFIDENCIAL	SIGILOSO
Impacto quanto à perda de Confidencialidade	Inexistente	Média	Alta
Definição	Toda informação que tenha sido recebida através de domínio público. O conhecimento desta informação pelo público não expõe a SERVMAR a prejuízo financeiro ou constrangimento, tampouco compromete a segurança dos ativos.	Toda informação, incluindo comunicações orais ou escritas transmitidas ou divulgadas pela SERVMAR, seus clientes ou fornecedores.	Toda informação secreta, incluindo as comunicações orais ou escritas.

A tabela acima não se aplica a **Incidentes de Segurança que envolvam dados pessoais**, ocasião em que a tabela de classificação aplicável será aquela constante no "Procedimento de Resposta a Incidentes de Segurança Envolvendo Dados Pessoais" disponibilizado pela **SERVMAR** aos colaboradores.

7. SEGURANÇA FÍSICA E DO AMBIENTE

Controles de acesso ao *Datacenter*

- A SERVMAR controla todos os acessos físicos ao seu *Datacenter*, possuindo câmeras de segurança monitoradas por Sistema de Monitoramento por CFTV – Circuito Fechado de Televisão;
- O controle de acesso é restrito a pessoas autorizadas e a quem detém da chave da porta de acesso.

8. USO DOS ATIVOS

- A SERVMAR disponibiliza para seus Colaboradores equipamentos exclusivamente para o desempenho de suas atividades profissionais; portanto o uso inadequado desses equipamentos para fins não delineados pela empresa é proibido;
- O Colaborador deve zelar pelo bom uso dos recursos de informática a ele disponibilizados, não removendo, alterando ou acrescentando qualquer tipo de componente interno de *hardware* ou *software*;
- Todos os dispositivos de armazenamento de dados portáteis (DVD's, CD's, *pendrives*) que, excepcionalmente, precisem ser utilizados - especialmente os de origem externa -, devem ser submetidos a uma rotina de verificação quanto à existência de vírus antes de serem utilizados no ambiente da SERVMAR;
- É vedado o armazenamento, na rede da empresa, ou em quaisquer equipamentos de propriedade da SERVMAR, de material obsceno, ilegal ou não ético, fato que ensejará a apuração de responsabilidade;
- Arquivos particulares ou não pertinentes ao negócio da SERVMAR não devem ser copiados/movidos para a rede da empresa, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles serão excluídos definitivamente, sem aviso prévio;
- Informações relacionadas a concorrentes, propostas comerciais, protótipos e projetos da concorrência não devem ser armazenadas na rede da SERVMAR ou em quaisquer equipamentos de propriedade da empresa;
- Documentos necessários para as atividades da SERVMAR devem ser salvos na rede. Tais arquivos, se gravados apenas localmente nos computadores, não terão garantia de *backup* e poderão ser perdidos caso ocorra uma falha no computador;
- O Colaborador não deve executar nenhum tipo de comando ou programa que venha a sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e autorização da Diretoria;

- O Colaborador não deve consumir alimentos e bebidas próximo aos recursos tecnológicos e aos documentos físicos corporativos, podendo ser responsabilizado por danos causados em decorrência deste ato;
- O Colaborador deve manter a configuração do equipamento disponibilizado pela equipe de suporte, o qual possui os controles de segurança definidos pela SERVMAR;
- A conexão de quaisquer equipamentos que não sejam de propriedade da SERVMAR deve ser realizada em rede específica;
- É vedada a conexão de quaisquer equipamentos que não sejam de propriedade da SERVMAR ou homologados pela SERVMAR em sua rede corporativa, especialmente os *notebooks* e *smartphones* particulares, já que comprometem a segurança da informação e a qualidade dos serviços;
- Na utilização de equipamentos de propriedade da SERVMAR, o Colaborador deverá tomar os seguintes cuidados:
    - ✓ Desligar o equipamento ao final do expediente;
    - ✓ Sempre que tiver dúvidas ou problemas relacionados aos equipamentos, o Colaborador deverá se comunicar com a equipe de suporte por meio de abertura de chamado no *Service Desk*;
    - ✓ O uso das impressoras deve ser feito, exclusivamente, para impressão de documentos ou de outras informações que sejam de interesse da SERVMAR;
    - ✓ Ao se ausentar o usuário deve bloquear sua estação de trabalho, caso não siga a recomendação, a estação de trabalho do usuário será bloqueada quando fique ociosa por 5 (cinco) minutos e só poderá ser desbloqueada pelo usuário logado ou por um usuário administrador. Desta maneira será evitado o acesso por pessoas não autorizadas; e
    - ✓ O Colaborador deve retirar imediatamente da impressora os documentos para ela enviados caso contenham informações sensíveis.
- A SERVMAR tem propriedade legal sobre todos os arquivos produzidos em seus computadores, reservando-se o direito de manter, a seu critério, histórico de acessos e transações realizadas com uso da Internet ou Intranet, quando considerado necessário por motivos de segurança ou para fins de auditoria; e
- A forma da informação impõe restrições às medidas necessárias para sua proteção, porém não importa a forma que a informação toma ou os meios pelos quais é compartilhada: ela deve sempre ser apropriadamente protegida. A informação eletrônica, física ou verbal, deve ser tratada conforme a política de classificação e tratamento da informação.

9. PUBLICAÇÕES NAS REDES SOCIAIS

COMUNICAÇÃO COM A MÍDIA E INFLUENCIADORES

- Apenas os porta vozes indicados e designados pela Diretoria da SERVMAR estão autorizados a dar declarações e/ou entrevistas para a imprensa e/ou perfis de influenciadores digitais se recomendado pela Diretoria da SERVMAR.

- Qualquer contato de imprensa realizado diretamente com o colaborador deverá ser encaminhado imediatamente à Diretoria da SERVMAR.
- Imagens de incidentes, acidentes e situações fora da normalidade que ocorram na empresa, em instalações, empreendimentos ou ativos de clientes e/ou na parceiros deverão ser encaminhadas à Diretoria da SERVMAR.
- Não será permitida a disseminação externa de fotos, vídeos e áudios de incidentes, acidentes e situações fora da normalidade relacionados a empresa, instalações, empreendimentos ou ativos de clientes e parceiros via aplicativos de mensagem instantânea, e-mail ou qualquer outro meio digital.

10. REGRAS PARA MESA E TELA LIMPAS

- As mesas de trabalho devem estar limpas de papéis e mídias de armazenamento removíveis que contenham informações sensíveis;
- Os papéis e mídias contendo informações sensíveis devem ser guardados em mobília segura, imediatamente após o uso;
- As áreas de trabalho dos computadores devem estar limpas de arquivos que contenham informações sensíveis. Estes arquivos devem estar armazenados apropriadamente na rede;
- Sempre que não for utilizar o computador ou tiver que se ausentar da sala, o Colaborador deverá efetuar procedimento de desconexão: *logoff* ou o bloqueio do computador; e
- O sistema operacional deve fazer o bloqueio automático de tela a partir de 5 (cinco) minutos de inatividade.

11. REGRAS PARA TRANSFERÊNCIA DE INFORMAÇÕES

Visa manter a segurança da informação transferida dentro da organização e com quaisquer entidades externas.

- Os requisitos para confidencialidade da informação estão descritos no “SRV-FOR-0442-Termo Consentimento Geral - Dados Sensíveis de Colaboradores - LGPD”;
- Os Colaboradores devem ser extremamente cautelosos na utilização de quaisquer meios de comunicação, ficando proibida qualquer troca de informações com o meio exterior sobre informações com mais alto grau de sensibilidade sem autorização e justificativa; e
- Entende-se por disseminação de informações com mais alto grau de sensibilidade específicas da SERVMAR toda e qualquer troca de mensagens com o meio exterior, que contenha qualquer referência a:

  - ✓ Documentos sobre clientes, faturamento e dados financeiros da SERVMAR;
  - ✓ Diagramas, propostas, *checklists* operacionais, projetos, *papers* técnicos ou da empresa;

- ✓ Decisões sobre aquisições, fusões e incorporações, ou qualquer tipo de informação privilegiadas; e
- ✓ Patentes, pesquisas, desenvolvimento de *software* e de soluções.

E-mail

- O correio eletrônico corporativo fornecido pela SERVMAR deve ser utilizado em função das atividades da empresa;
- É expressamente proibido:
  - ✓ O envio de material obsceno, ilegal ou não ético, propagandas, mensagem do tipo "corrente", de entretenimento, discriminatórias, preconceituosas ou ofensivas no que se refere a nacionalidade, raça, orientação sexual, religião ou opinião política;
  - ✓ O envio simultâneo de mensagens para todos os usuários da rede da SERVMAR, salvo para comunicações administrativas e previamente autorizadas que devam ser dirigidas a todos os funcionários;
  - ✓ A inserção ou disseminação de arquivos que contenham vírus ou qualquer espécie de programas nocivos;
  - ✓ O envio de grande quantidade de mensagens de *e-mail* que prejudique a capacidade técnica da rede;
  - ✓ Divulgar conteúdo que viole quaisquer direitos autorais, patentes, marcas registradas, marcas de serviço, nomes comerciais, segredos comerciais ou outros direitos de propriedade intelectual da SERVMAR ou de terceiros;
  - ✓ Participar de listas de discussão que possam abordar assuntos alheios às áreas fins da empresa e de suas gerências;
  - ✓ Anunciar quaisquer produtos ou serviços, bem como promover qualquer marca, setor, empresa ou outras formas de autopromoção;
  - ✓ Forjar quaisquer das informações do cabeçalho do remetente; e
  - ✓ Expor contas de *e-mail* em provedores de acesso à internet para coletar respostas e mensagens enviadas, quando tais mensagens violem esta Política.
- As mensagens de correio eletrônico sempre devem incluir assinatura com as seguintes informações:
  - ✓ Nome Completo
  - ✓ Área/Setor
  - ✓ Cargo
  - ✓ Telefone
  - ✓ Logo da empresa
- Todas as mensagens trafegadas no domínio da SERVMAR permitem rastreabilidade.

12. REGRAS PARA USO DE DISPOSITIVOS MÓVEIS E TRABALHO REMOTO

Visa garantir a segurança das informações no trabalho remoto e no uso de dispositivos móveis.

- É responsabilidade do Colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela SERVMAR, notificar imediatamente a equipe de suporte e procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência;
- O Colaborador deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo ele o responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar a SERVMAR ou a terceiros;
- O Colaborador que deseje utilizar equipamentos portáteis particulares ou adquirir acessórios e posteriormente conectá-los à rede da Servmar deverá submeter previamente tais equipamentos ao processo de homologação da equipe de suporte;
- O trabalho remoto à rede da SERVMAR somente é permitido por meio do acesso via VPN – *Virtual Private Network;*
- A concessão do acesso remoto via VPN será de exclusivo critério da SERVMAR e mediante solicitação por meio de abertura de chamado no *Service Desk*, que optará para qual rede o Colaborador terá permissão de acesso. A referida concessão será feita de forma individual, sendo os Colaboradores responsáveis por seus acessos via VPN bem como por qualquer atividade irregular exercida por outra pessoa de posse de seu acesso remoto. Com isso, os Colaboradores deverão adotar medidas de cautela, para que terceiros não tenham acesso, sem autorização, à sua conexão de VPN;
- As sessões de videoconferência devem ser feitas por meio de software homologado pela área de Tecnologia e Segurança da Informação e sempre com controle de acesso às salas virtuais;
- Durante as sessões de videoconferência deve-se optar por locais reservados atentando sempre para o vazamento de informações, tanto pela exposição a câmera quanto à propagação do áudio;
- Proteja o acesso a salas de videoconferência com senha. Não envie o convite a terceiros, exceto se devidamente autorizado pelo gestor;
- Atente para as informações expostas pela câmera e não grave, tire *prints* ou "*selfies*" que exponham a sessão em andamento; e
- Não divulgue informações de "reuniões virtuais", exceto se devidamente autorizado pelo gestor.

13. REGRAS PARA USO E INSTALAÇÃO DE SOFTWARE

- A SERVMAR estabelece padrões de configuração de segurança para todos os sistemas operacionais e *softwares* autorizados;
- O uso de *software* pirata pode acarretar os seguintes prejuízos a SERVMAR:

- ✓ Infringência à Lei nº. 7.646, de 18 de dezembro de 1987 que proíbe a reprodução, comercialização, importação e utilização de cópias de programas de computador feitas sem a devida autorização do titular dos direitos autorais;
- ✓ Exposição negativa da imagem da SERVMAR perante a sociedade pelo descumprimento à lei;
- ✓ Incidência de multas, pagamento de indenizações e outras penalidades previstas em lei;
- ✓ Risco de incidência de vírus de computador, em função do desconhecimento da procedência; e
- ✓ Poderá causar lentidão ou parada de funcionamento dos computadores.

- É proibida a instalação de *software* sem que esteja devidamente identificado, licenciado e homologado pela SERVMAR;
- *Softwares* do tipo "jogos eletrônicos" não podem ser instalados, armazenados ou usados em qualquer computador da SERVMAR;
- Não é permitido o download de *software*, programas ou executáveis da Internet ou de quaisquer outros meios para os computadores da SERVMAR sem prévia autorização da área de Tecnologia e Segurança da Informação, evitando assim qualquer contaminação por vírus que possa comprometer os sistemas e informações da SERVMAR ou gerem problemas com a legislação de direitos autorais;
- A aquisição de *software* não constante da relação dos homologados deverá ser solicitada por meio de abertura de chamado no *Service Desk*;
- A SERVMAR deve possuir um catálogo de todos os *softwares* autorizados necessários na empresa para qualquer finalidade do negócio em qualquer sistema; e
- Os softwares fornecidos por entidades externas, sem ônus para a SERVMAR e acompanhados da autorização do detentor legal dos direitos autorais, deverão ser submetidos à equipe de suporte para homologação, quando serão realizados testes e verificações de sua integridade e compatibilidade com os recursos já existentes na rede da SERVMAR.

14. BACKUP

- As necessidades especiais de *backup* devem ser solicitadas à equipe de suporte por meio de abertura de chamado no *Service Desk*; e
- O Colaborador da área deve solicitar à equipe de suporte a restauração da cópia de segurança por meio de abertura de chamado no *Service Desk* em caso de perda ou danos na informação.

15. REGRAS PARA PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS

Visa implementar controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos (malwares).

- A SERVMAR adota soluções de proteção contra *malware* (códigos maliciosos) gerenciadas centralmente, com medidas de detecção e de prevenção para monitorar e defender continuamente cada uma das estações de trabalho e servidores da organização;
- Todos os servidores e estações de trabalho da SERVMAR devem ter *software* antivírus instalado, ativado e atualizado sistematicamente;
- Todos os Colaboradores são responsáveis pela prevenção de contaminação da rede e, em caso de identificação ou suspeita de vírus, devem solicitar análise pela equipe de suporte por meio de abertura de chamado no *Service Desk*;
- Os Colaboradores também são responsáveis pela não interrupção da verificação periódica dos sistemas de proteção contra vírus em suas estações de trabalho; e
- Em quaisquer situações, qualquer *software* ou arquivo proveniente de redes ou usuários externos deverão ser verificados por sistemas de proteção contra vírus.

16. REGISTROS E MONITORAMENTO

- A SERVMAR registra eventos (*log*) das atividades dos usuários, exceções, falhas e eventos de segurança da informação produzidos, mantidos e analisados criticamente, a intervalos regulares;
- Assegura que os *logs* apropriados estejam sendo agregados a um sistema central de gerenciamento de *logs* para análise e revisão; e
- Os registros de eventos (*log*) são protegidos contra acesso não autorizado e adulteração.

17. REGRAS PARA GESTÃO DE VULNERABILIDADES TÉCNICAS

- As vulnerabilidades técnicas devem ser identificadas por meio de um scanner de vulnerabilidades, específico para este fim, e são registradas e tratadas através de chamados abertos no sistema de *Service Desk*; e
- A SERVMAR deve analisar sistemas de informação criticamente, através de testes de invasão externos e internos regulares para identificar vulnerabilidades e vetores de ataque que possam ser usados.

18. SEGURANÇA EM REDES

- O acesso à rede de visitantes da SERVMAR será liberado somente para fins de acesso à internet, por meio de abertura de chamado no *Service Desk* para a equipe de suporte;
- Os acessos originados na rede interna com destino a qualquer rede externa, só poderão ser realizados com equipamentos da SERVMAR ou homologados por ela;

- A navegação em sites não relacionados à atividade funcional do Colaborador não é proibida, porém seu uso deve ser feito de maneira responsável, antes do início do expediente ou no horário de almoço, de modo que abusos possam ser notificados aos gestores e punidos;
- A navegação em sites de categoria restringida pela SERVMAR é expressamente proibida conforme abaixo:
  - ✓ Violação de direito autoral;
  - ✓ Conteúdo ofensivo, difamatório, ilegal, discriminatório e similares;
  - ✓ Pornográfico;
  - ✓ Crackers (quebra de um sistema de segurança de forma ilegal ou sem ética);
  - ✓ Ferramentas de proxy (acesso à Internet de forma oculta ou disfarçada);
  - ✓ Violência e agressividade;
  - ✓ Acesso externo com a finalidade de divulgação de dados sensíveis;
  - ✓ Terrorismo e disseminação de violência a partir de crença ou posição política;
  - ✓ Práticas de comercialização, divulgação ou posicionamento sobre drogas; e
  - ✓ Pedofilia.

19. RELACIONAMENTO COM FORNECEDORES

- Os requisitos de segurança da informação devem ser acordados com o(s) fornecedor(es), e documentados no "SRV-FOR-0444- Termos e condições gerais de fornecimento.", a fim de mitigar os riscos associados com o acesso a ativos da SERVMAR; e
- O "SRV-FOR-0444- Termos e condições gerais de fornecimento." firmado com o(s) fornecedor(es) deve contemplar todas as diretrizes desta Política aplicáveis ao fornecedor.

20. PROCESSO DISCIPLINAR

Visa orientar os Colaboradores quanto as possíveis ações para os que cometerem violações de segurança da informação.

- O Colaborador tem por obrigação cumprir esta Política. Desta forma, o não cumprimento será considerado uma infração;
- Diante da constatação de um Incidente, reportado e constatado Encarregado e/ou pelo Comitê de Compliance, sanções serão aplicadas de acordo com o **Procedimento de Consequências**; e
- Com relação aos Colaboradores terceirizados será solicitado à empresa prestadora da respectiva mão de obra, o afastamento temporário ou definitivo do funcionário conforme a falta cometida, podendo, em último caso, a SERVMAR solicitar a rescisão do respectivo contrato de prestação de serviço.