

## **ESPECIFICAÇÃO TÉCNICA MÍNIMA DA SOLUÇÃO**

**1. LOTE 01 (ÚNICO) - ITEM 1 – Solução tecnológica para atendimento das exigências da política de segurança da informação, compliance e governança de dados não estruturados, pelo período de 36 meses.**

- 1.1. Solução de tecnologia que permitirá o atendimento das exigências da política de segurança da informação, compliance e governança de dados não estruturados, elevando o nível de proteção das informações no ambiente tecnológico do Ministério da Cultura (MinC), de forma a atender ao que cabe a LGPD no tocante a dados não estruturados.
- 1.2. Permitir a detecção de comportamentos suspeitos em diretórios de usuários e servidores de arquivos. Além disso, a solução poderá ser migrada para a nuvem, modelo SAS, conforme necessidade futura ou preferência do contratante, desde que observadas as regulamentações legais referentes à localização dos dados e à privacidade das informações.
- 1.3. A solução tecnológica proposta será licenciada pelo período de 36 meses, para garantir a governança e conformidade dos ambientes de dados não estruturados presentes nos servidores AD, NAS, Windows da organização e aplicações web. Adicionalmente, será possível modificar o licenciamento durante o período contratual para se adequar a plataformas em nuvem, plataforma SAS, conforme as especificações detalhadas no termo de referência.
- 1.4. **Requisitos Mínimos Gerais**
- 1.5. A solução de proteção de credenciais deverá ser capaz de analisar em tempo real e prevenir comportamentos suspeitos em aplicações web, mesmo que estas não estejam integradas ao Active Directory;
- 1.6. Comunicar-se através de API HTTP REST ou UDP com a aplicação web protegida, calculando e fornecendo em tempo real um score de risco e o nível de risco que este score representa, para cada evento de autenticação que ocorre em uma dada aplicação;

- 1.7. Assegurar a comunicação entre a solução de proteção de credenciais e a aplicação web protegida através de criptografia de chaves simétricas;
- 1.8. Possibilitar a criação e configuração de políticas de risco, possuindo no mínimo 4 níveis de risco parametrizáveis a serem definidos em cada política;
- 1.9. Fornecer para cada autenticação analisada o score de risco processado acompanhado da ação (permitir, notificar, desafiar ou bloquear) indicada para o nível de risco do evento em questão, de acordo com a política definida;
- 1.10. Possibilitar o agrupamento de credencias, de modo que uma credencial possa estar associada a mais de uma aplicação web protegida;
- 1.11. Não exigir tokens, dispositivos móveis, códigos ou outras informações adicionais para o processamento de eventos;
- 1.12. Ser capaz de processar e fornecer o score de risco tanto para autenticações com a credencial e senha corretos como para autenticações com credencial e/ou senha incorretos;
- 1.13. Possuir uma base de inteligência de segurança para ser utilizada na mensuração do risco dos acessos, construída com informações próprias e públicas (OSINT), de modo a identificar IPs de má reputação e/ou utilizados para serviço de proxy;
- 1.14. Realizar a mensuração de risco no processo de autenticação sem armazenar e sem ter acesso a senha da credencial em questão, em nenhuma hipótese.
- 1.15. Construir padrão de comportamento de uma credencial com base no histórico de seu uso, composto minimamente por navegador, dispositivo, localização geográfica (cidade e país), sistema operacional, identificador do provedor de internet;
- 1.16. Identificar desvios no padrão de comportamento de uma credencial, possibilitando o envio de notificações, apresentação de desafios (token, captcha ou similares) e bloqueio de acesso, a depender da política de risco definida;
- 1.17. Realizar a mensuração de risco de todos os acessos levando em consideração o padrão de comportamento da credencial e a base de inteligência de segurança;

- 1.18. Todos os eventos processados e armazenados pela solução deverão ser georreferenciados de acordo com o endereço IP de origem, contendo minimamente país, cidade, latitude e longitude;
- 1.19. Permitir a notificação de usuários com base em política de risco, através do disparo via SMTP de e-mail, possibilitando a redação de mensagem personalizada em editor HTML, contendo detalhes do evento em questão como cidade de acesso, data e hora, ip de origem, navegador e um link para que o usuário responda se reconhece o acesso ou não;
- 1.20. Inserir no padrão de comportamento da credencial novas informações quando o usuário confirma através da notificação recebida a veracidade do acesso;
- 1.21. Possibilitar o envio de e-mail para administrador quando um usuário nega a veracidade de um acesso através da notificação recebida;
- 1.22. Ser capaz de bloquear o processo de autenticação de usuários com base no score de risco do evento, mesmo quando a credencial e a senha forem corretamente imputadas no ato da autenticação;
- 1.23. Identificar ataques do tipo “força bruta”, elevando de forma automática e proporcional o score de risco do IP de origem do acesso com base no número de tentativas de autenticações fracassadas em um curto intervalo de tempo;
- 1.24. A reputação das origens detectadas como geradores de ataques de força bruta deverá decair após determinado tempo, e o tempo de decaimento da reputação deverá aumentar em função da recorrência de tentativas de ataques de força bruta;
- 1.25. Enviar eventos, cifrados nativamente com chave simétrica, via webhook para URL a ser configurada em interface gráfica, com base na política de risco definida;
- 1.26. Elevar o score de risco de uma credencial ao detectar mudança geográfica de longa distância;

- 1.27. Identificar os top 10 usuários que representam maior atividade de risco acumulado em um intervalo de tempo escolhido, informando o nome do usuário (credencial) e score de risco acumulado;
- 1.28. Segmentar os eventos processados por credencial, possibilitando navegar por todos os eventos de uma dada credencial, informando no mínimo os seguintes detalhes de cada evento: Cidade, coordenadas geográficas, nome do navegador utilizado, nome do dispositivo utilizado no acesso, endereço ip de origem, score de risco e resultado da ação com base na política definida, código identificador do ISP (internet service provider) e descritivo com análise do evento;
- 1.29. Possuir gráfico que represente os eventos de uma credencial específica em um intervalo de tempo escolhido, distinguindo-os pelos níveis de risco definidos em política;
- 1.30. Possuir dashboard para visualização de eventos no formato de representação de mapa geográfico que possibilite distinguir diferentes níveis de risco, detalhando informações como cidade, usuário, score de risco do evento, data e hora do evento;
- 1.31. Possuir dashboard para visualização do risco organizacional em um intervalo de tempo escolhido, segmentado por aplicação protegida ou não, distinguindo o volume de eventos que representam o risco mitigado, o risco em mitigação (pendente) e o risco assumido;
- 1.32. Possuir dashboard para identificação e análise de ataques, contendo minimamente as seguintes estatísticas:
  - 1.32.1. Endereços IPs com maior incidência de credenciais únicas autenticadas com sucesso e com falha na autenticação;
  - 1.32.2. Credenciais com maior incidência de acessos originados em cidades distintas autenticados com sucesso e com falha na autenticação;
  - 1.32.3. Credenciais com maior incidência de eventos de autenticação com sucesso e com falha na autenticação;

- 1.32.4. Endereços IPs com maior número de eventos de autenticação com sucesso e com falha na autenticação;
- 1.32.5. Cidades com maior número de eventos;
- 1.32.6. Países com maior número de eventos;
- 1.32.7. Gráfico com quantidade de eventos classificados por resposta da política de risco em razão do tempo;
- 1.32.8. Possuir integração com soluções do tipo “single-sign-on”, disponibilizando no mínimo, de forma nativa, o RH-SSO e Keycloak;
- 1.32.9. Possuir integração nativa com a autenticação de tecnologias de mercado, sendo minimamente wordpress, openssh, cloudflare, moodle e keycloak;
- 1.32.10. Ser capaz de processar eventos originados em IPv4 e IPv6;
- 1.32.11. Possuir identificador único para todos os eventos processados pela solução;
- 1.32.12. Possuir mecanismo de processamento e armazenamento de eventos baseado em tecnologias escaláveis;
- 1.32.13. Possuir mecanismo de dissuasão de ataques de força-bruta baseado em desafio criptográfico a ser decifrado pelo navegador cliente, sem necessidade de interação dos usuários da aplicação protegida;
- 1.33. O nível de dificuldade do desafio criptográfico deverá ser parametrizável;
- 1.34. Deverá ser fornecido um painel para visualização e análise de eventos, inspeção e segurança de credenciais/usuários;
- 1.35. O painel deverá possuir um mecanismo nativo para gestão de usuários que podem acessá-lo, incluindo integração nativa com os seguintes sistemas de diretório de usuários: Active Directory, LDAP e Keycloak/RH-SSO;
- 1.36. O painel deverá ser desenvolvido em tecnologia web based, acessível através de protocolo https;

- 1.37. O painel deverá criptografar toda a comunicação com as fontes geradoras de eventos, e ao armazenar eventos em base de dados, anonimizar o campo que contém a informação de nome de usuário, seja este um CPF, matrícula, e-mail ou uma string (ex: nome.sobrenome);
- 1.38. As informações disponibilizadas no painel de visualização deverão ser orientadas a intervalo de datas, e fornecer estatísticas dos eventos de segurança que são protegidas pela solução, sendo minimamente: Usuários que mais geram eventos de segurança no ambiente protegido; Endereços IPs que mais geram eventos de segurança no ambiente protegido; Incidentes de segurança mais frequentes;
- 1.39. O painel deverá permitir visualizar detalhes de cada evento de segurança coletado;
- 1.40. Permitir filtrar eventos por usuário (credencial);
- 1.41. Permitir filtrar eventos por endereço IP de origem;
- 1.42. Todos os softwares fornecidos deverão ser licenciados pelo período mínimo de 36 (trinta e seis) meses, e contemplar garantia, suporte e atualização dos respectivos fabricantes. A solução deverá ser dimensionada para o volume de usuários indicados no quadro de itens do presente termo de referência, devendo ser considerado o período contratual de 36 (trinta e seis) meses para a licença de uso que integra a solução;
- 1.43. O fabricante ou a solução ofertada de governança de dados, deverá possuir certificação de compliance como ISO 27001 ou similar, garantindo que seus produtos atendam aos rígidos padrões da indústria e sejam auditados e revisados regularmente;
- 1.44. Por se tratar de solução entregue como serviço na nuvem, modelo SAS, o fabricante deve adotar abordagem baseada em risco para seu sistema de gestão de segurança da informação (SGSI), a implantação de um SGSI, reduz o risco de divulgação, modificação ou destruição não autorizada, acidental ou intencional das informações, além de constantemente, realizar testes de penetração de terceiros no

tenant e varredura automatizada para garantir a segurança do software; Por se tratar de software de proteção de dados sensíveis com análise comportamental de usuários para ambientes computacionais o fabricante ou a solução de governança de dados deverá ser certificada ISO/IEC 27017;

- 1.45. A solução deve suportar a utilização de servidores virtualizados para os componentes;
- 1.46. A solução deve possibilitar a configuração de credencial diferente para cada servidor/serviço a ser monitorado;
- 1.47. Por se tratar de software de proteção de dados sensíveis o fabricante ou a solução de governança de dados deverá ser certificada ISO/IEC 27701 que trata do gerenciamento de privacidade da informação dentro da organização;
- 1.48. A solução deverá monitorar múltiplos domínios e servidores de arquivos Windows e NAS (Network Attached Storage) do ambiente, incluindo: Contas, estruturas de diretórios, permissões e eventos;
- 1.49. A solução a ser fornecida deverá possuir compatibilidade comprovada no site dos fabricantes dos storage Netapp e EMC para que tenha compatibilidade com a Infraestrutura do órgão;
- 1.50. Caso a solução necessite da instalação de agente para o monitoramento dos eventos do Active Directory e servidores de arquivos, os agentes não devem gerar nenhuma queda de performance nos servidores;
- 1.51. O gerenciamento da solução deverá ser centralizado para todos os módulos;
- 1.52. A solução deverá monitorar todos os domain controllers instalados em qualquer versão do Windows Server 2003 até 2022;
- 1.53. A solução deverá monitorar todos os servidores de arquivos instalados em Windows Server 2012 até Windows Server 2022;
- 1.54. A solução deverá monitorar no mínimo, os seguintes eventos do Microsoft Active Directory: Conta habilitada e desabilitada; Autenticação de conta (TGT); Renovação



de acesso (TGS); Replicação de AD; Logon de conta no DC; Criação, deleção, renomeação, modificação, remoção e adição de membros no objeto do DS; Requisição de acesso NTLM; Alteração de senha de usuário; Conta de usuário bloqueada; Conta de usuário desbloqueada; Netlogon vulnerável; Criação, deleção e modificação de GPO; Tentativa de reset de senha; Criação, atualização, deleção, habilitação e desabilitação de tarefa agendada dentro do DC; Alteração de política de kerberos;

- 1.55. A solução deverá monitorar no mínimo, os seguintes eventos do servidor de Arquivos Windows: Arquivo criado; Arquivo deletado; Arquivo aberto; Arquivo renomeado; Arquivo modificado; Mudança de proprietário do arquivo; Permissões adicionadas no arquivo; Permissões removidas no arquivo; Proteção adicionado no arquivo; Proteção removida no arquivo; Pasta criada; Pasta deletada; Pasta renomeada; Mudança de proprietário da pasta; Permissões adicionadas na pasta; Permissões removidas na pasta; Proteção adicionada na pasta; Proteção removida na pasta;
- 1.56. Deverá ser possível definir os proprietários das pastas através da console;
- 1.57. A solução deverá exibir uma lista com todas as contas de usuários monitoradas, indicando no mínimo, o tipo de conta (serviço, executiva ou administrativa) e grupos que fazem parte;
- 1.58. A solução deverá exibir o repositório monitorado em formato hierárquico, expandindo as pastas e sub-pastas até o nível do arquivo, permitindo a visualização de quais usuários tem acesso a cada recurso e as permissões concedidas;
- 1.59. A solução deverá possuir uma visão bi-direcional indicando através de uma visualização gráfica e interativa, todas as permissões dos usuários e grupos, e quais as permissões aplicadas nos objetos (arquivos e pastas);
- 1.60. A solução deverá disponibilizar a visibilidade de permissões, sejam elas NTFS ou share;

- 1.61. A solução deverá realizar a classificação do conteúdo do arquivo, fornecendo visibilidade sobre onde residem os dados confidenciais e sensíveis no sistema de arquivos;
- 1.62. A solução deverá utilizar múltiplos fatores para realizar a classificação do conteúdo do arquivo, incluindo: Metadados, padrões, dicionários, palavras-chave e expressão regular;
- 1.63. A solução deverá indicar para qualquer arquivo e pasta no servidor monitorado, uma visualização gráfica contendo o nível de exposição e indicando se o arquivo é sensível ou não a partir da classificação realizada;
- 1.64. A solução deverá fornecer filtros para visualizar apenas determinados objetos de dados em exibição gráfica interativa, incluindo pastas protegidas e pastas únicas;
- 1.65. A solução deverá incluir informações de classificação de dados na tela das permissões, incluindo: nome da regra classificada, e quantidade de instâncias sensíveis encontradas no arquivo;
- 1.66. A solução deverá fornecer para as permissões, tipos de exibição diferentes, incluindo exibições hierárquicas e de lista;
- 1.67. A solução deverá realizar a classificação de imagens através de OCR ou tecnologia similar;
- 1.68. A solução deverá possibilitar a criação de regras customizadas para que os administradores possam definir o que deve ser encontrado dentro do conteúdo do arquivo, de acordo com a necessidade organizacional;
- 1.69. Deve ser possível realizar o agendamento do escaneamento das regras de classificação, podendo especificar: horário, dia e tempo de duração;
- 1.70. Deve ser possível exportar eventos e informações apenas referente aos dados classificados como sensíveis;

- 1.71. Deve ser possível definir o escopo do ambiente que vai ser classificado, podendo definir: repositório, arquivo, pasta, tipo de arquivo, quantidade mínima de hits e outros;
- 1.72. A solução deverá auxiliar na conformidade com a LGPD, identificando aonde os dados pessoais (CPF, RG, CNH e outros) são armazenados, quem tem acesso aos dados e quais são as atividades em cima destes dados;
- 1.73. A solução deverá escanear e classificar no mínimo os seguintes tipos de arquivos: doc, docx, dwg, rtf, ppt, xls, txt, csv, pdf, xml, log, eml, jpg, jpeg, gif, png, rar e zip;
- 1.74. A solução deverá encontrar em arquivos com formato tabular, palavras chaves em cabeçalhos e colunas;
- 1.75. Deve ser possível limitar escopo dentro dos sistemas de arquivos a ser analisado;
- 1.76. Deve ser possível definir partes específicas do arquivo a serem analisadas no escopo como: Colunas específicas de arquivos do tipo Microsoft Excel, cabeçalho, rodapé e marca d'água de arquivos Microsoft Office, links de arquivos Microsoft Office e PDF;
- 1.77. A solução deverá indicar no painel de diretórios: o nome da regra, a quantidade de hits do termo sensível encontrado nos arquivos e pastas e a quantidade de hits incluindo sub-pastas;
- 1.78. A solução deverá ser entregue utilizando a infraestrutura em nuvem disponibilizada pelo fabricante, e poderá ser ofertada e instalada localmente desde que não retenha os logs nativos e não seja baseada em software livre.
- 1.79. A solução deve ser capaz de identificar tanto desvios quantitativos de comportamento como desvios qualitativos. Ou seja, deve ser capaz de identificar um aumento na quantidade de eventos gerados, assim como identificar acesso a dados que o usuário não costuma acessar;

- 1.80. Nos alertas em tempo real, deve ser possível configurar para que, um usuário, uma pasta, um período ou uma ação específica seja alertada, caso ocorra ação que os envolva;
- 1.81. A solução deverá notificar os administradores através de alertas para qualquer tipo de atividade incomum e comportamentos suspeitos de usuários;
- 1.82. Os alertas da solução deverão ser encaminhados via SMTP e SNMP;
- 1.83. A solução deverá suportar a configuração de respostas automáticas para os alertas gerados, possibilitando a execução automática de scripts ou comandos pré-configurados;
- 1.84. A solução deverá realizar a análise comportamental dos usuários de forma automática, através de machine learning, entendendo o comportamento e rotina de todos os usuários, o que acessam, quando acessam e onde;
- 1.85. A solução deverá contemplar a assinatura de uma base de conhecimentos do fornecedor com mais de 150 modelos de alertas pré-configurados de eventos suspeitos tais como: Ataques de sequestro de dados (ransomware); Detecção de ferramentas nocivas ao ambiente; Ações com acessos negados; Ações de escalasões de privilégios; Excesso de tentativas de autenticação ou contas bloqueadas; Atividades suspeitas em dados parados e/ou inativos; Alterações anormais em GPO; Ataques de golden ticket; Ataques de injeção de códigos maliciosos; Ataques de descoberta de contas com NTLM e Kerberos; Ataques de força bruta;
- 1.86. Os modelos de alertas devem ser atualizados de forma automática;
- 1.87. A solução deverá detectar ameaças em todos os estágios de um ataque cibernético, incluindo dashboard que indica algumas categorias como: Reconhecimento, intrusão, exploração, escalação de privilégio, movimento lateral, negação de serviço e exfiltração de dados;
- 1.88. A solução deverá monitorar a atividade do usuário para construir perfis de comportamento e usar os modelos de ameaça baseados em comportamento para alertar quando uma atividade anormal no Active Directory é detectada;

- 1.89. A solução deverá construir perfis de comportamento comparando as atividades dos usuários e entidades e identificando a relação entre eles;
- 1.90. A solução deverá possuir um período de aprendizado, para que seja feito a coleta de eventos e identificação do comportamento dos usuários para a criação do perfil comportamental;
- 1.91. A solução deverá realizar a descoberta de contas privilegiadas de forma automática, identificando contas executivas, contas de serviço e contas administrativas baseado no seu comportamento e nos grupos de segurança que a conta está inserida;
- 1.92. A solução deverá exibir uma lista com todas as contas de usuários monitoradas, indicando no mínimo, o tipo de conta (serviço, executiva ou administrativa) e grupos que fazem parte;
- 1.93. A solução deverá possuir dashboard de alertas indicando os usuários mais alertados, dispositivos e modelos de alertas gerados;
- 1.94. A solução deverá possuir política de automação para remediação de exposição de dados para toda a organização, removendo as permissões globais das pastas e arquivos;
- 1.95. A solução deverá possuir política de automação para remediar permissões inconsistentes, garantindo que não exista permissão quebrada e aplicando as entradas de permissão corretamente para as sub-pastas e arquivos;
- 1.96. As políticas de automação para remediação devem ser executadas de forma manual e automática;
- 1.97. A solução deverá possuir política de automação para remediar permissões inconsistentes, garantindo que não exista permissão quebrada e aplicando as entradas de permissão corretamente para as sub-pastas e arquivos;

- 1.98. Para análise forense do usuário mais alertado, o dashboard deve possuir página que agregue dados importantes do comportamento daquele usuário. Isso permite que se identifique o cenário do possível ataque;
- 1.99. No dashboard, a partir de um alerta selecionado, a solução deve exibir página que liste todos os eventos ocorridos que motivaram a ferramenta a gerar o alerta. A lista desses eventos deve ser customizável podendo ser filtrada, exibidas ou ocultas colunas e agregada por valores das colunas exibidas;
- 1.100. A solução deverá suportar na busca dos eventos a utilização de operadores relativos, auxiliando na investigação e nos resultados esperados;
- 1.101. Deve ser possível salvar uma pesquisa customizada, agendando para que ela possa ser executada de forma automática e que os administradores recebam as informações necessárias de forma periódica;
- 1.102. A solução deverá suportar a criação e utilização de flags para serem aplicadas as contas de usuários e aos recursos monitorados, essas flags podem ser utilizadas nos filtros e na aba de eventos;
- 1.103. A solução deverá identificar dados que não foram acessados por um período, podendo especificar a quantidade de dias desejado;
- 1.104. A solução deverá disponibilizar dashboard das informações correlacionadas dos dados do Active Directory, com painéis, indicando no mínimo: Usuários com senha que nunca expira, contas de usuários obsoletas, contas executivas, contas desabilitadas e contas habilitadas com a senha expirada;
- 1.105. A solução deverá disponibilizar dashboard com painéis dos dados correlacionados dos servidores de arquivos Windows, indicando no mínimo: Arquivos sensíveis expostos para toda organização, pastas expostas, permissões obsoletas, permissões direta nas pastas, pastas com permissões inconsistentes e pastas com dados obsoletos;

- 1.106. Deve possuir visualização de indicadores de risco para o Active Directory com configurações que podem ser exploradas por usuários maliciosos, como: Admins com SPNs, contas habilitadas, porém sem uso e contas sem senha;
- 1.107. Deve ser possível comparar os gráficos do dashboard através da console, indicando a diferença dos valores atuais com o período anterior;
- 1.108. Os widgets devem ser configuráveis e customizáveis, podendo alterar o modo de visualização, para alguns tipos, como: widgets de métrica única, widgets de porcentagem e widgets com linha do tempo;
- 1.109. Os alertas devem ser apresentados também em dashboard web que apresente: quantidade de alertas e suas severidades em determinado período, usuários mais alertados em determinado período, tipos de comportamentos suspeitos que mais ocorreram, máquinas que foram mais utilizadas para as ações suspeitas, classificação dos alertas dentro de um cenário de ataque cibernético;
- 1.110. A solução deverá possuir Widget de geolocalização com mapa indicando a origem da ação para os alertas gerados;
- 1.111. A solução deverá possuir uma tela de visualização de eventos, podendo realizar pesquisas e filtros à cerca de todas as atividades e dados do ambiente;
- 1.112. Todos os eventos podem ser filtrados e organizados no mínimo por: tipo de evento, ID do evento, operação, status e plataforma;
- 1.113. A solução ofertada deve manter o log das operações de abrir, criar, apagar, modificar, renomear e acesso negado aos arquivos e pastas;
- 1.114. A solução deverá fornecer a visão das permissões efetivas, ou seja, agregando permissões de Share e NTFS;
- 1.115. A solução deve fornecer método para assinalar ou associar um ou mais usuários como "Proprietário(s)" de uma pasta ou grupo;
- 1.116. Deve ser possível definir uma data e horário para busca dos eventos;

- 1.117. A solução deverá possuir filtro para última atividade registrada do usuário, facilitando a busca de contas que estão atualmente inativas;
- 1.118. Os logs apresentados pela solução ofertada devem conter informações completas de cada uma das operações com data e horário, nome do servidor, tipo do objeto, caminho (path) dos dados, domínio, arquivo impactado e nome do usuário;
- 1.119. A solução deverá fornecer relatório dos níveis de exposição das permissões, no contexto de dados sensíveis para qualquer pasta e arquivo;
- 1.120. A solução deverá permitir filtragem gráfica, ordenação e agrupamento dos logs;
- 1.121. A solução deverá permitir que os usuários realizem pesquisas baseadas em critérios como: data do evento, servidor ou plataforma em que o evento ocorreu, tipo de evento, arquivos ou diretórios acessados;
- 1.122. Deve ser possível alterar o conjunto de dados (colunas) retornados da consulta aos logs de acordo com a necessidade da informação;
- 1.123. A solução deve ser capaz de identificar qual dado ou arquivo contém informações sensíveis ou confidenciais por meio de busca em seu conteúdo por informações definidas em dicionários fornecidos pelo fabricante ou por informações definidas e customizadas pelo usuário;
- 1.124. A solução deverá fornecer relatório das permissões, incluindo dados da classificação;
- 1.125. A solução deverá fornecer relatório das atividades de acesso dos usuários aos arquivos e pastas;
- 1.126. A solução deverá fornecer relatório dos resultados da classificação dos dados, incluindo o número de hit e regra classificada;
- 1.127. A solução deverá fornecer relatório dos dados que estão com permissões de grupos globais e quem está utilizando estas permissões para acessar as informações;
- 1.128. A solução deve exibir na mesma interface gráfica das informações sobre os permissionamentos e ACL's, a quantidade de informações sensíveis e qual tipo de



informação sensível classificada para facilitar a identificação de potenciais repositórios e pastas superexpostos;

- 1.129. A solução deverá fornecer relatório para SID não resolvido em ACLs;
- 1.130. A solução deverá fornecer relatório sobre grupos de segurança não utilizados ou vazios;
- 1.131. A solução deverá fornecer relatório para usuários desabilitados;
- 1.132. Deve ser possível exportar o relatório em no mínimo 3 tipos de formatos: CSV, Excel e PDF;
- 1.133. Deverá ser possível realizar o agendamento de relatórios;
- 1.134. Deverá ser possível encaminhar o relatório apenas para o proprietário do dado;
- 1.135. A solução deverá coletar informações de ferramentas de perímetro para monitorar atividades na borda da organização de forma e adicionar contexto a segurança dos dados não estruturados e usuários internos;
- 1.136. A solução deverá ser totalmente compatível e integrada ao módulo de análise de comportamento dos usuários e alerta em tempo real;
- 1.137. A solução deverá coletar eventos de auditoria das ferramentas de borda monitoradas através de integração nativa ou syslog;
- 1.138. A solução deverá suportar criptografia para receber os dados de auditoria da borda;
- 1.139. A solução deverá suportar a coleta de eventos de DNS, VPN e Web Proxies;
- 1.140. A solução deverá coletar no mínimo os seguintes eventos e metadados das ferramentas de borda:
  - 1.140.1. DNS: Client DNS query, Upstream DNS query, DNS Zone Transfer e DNS Client Update;
  - 1.140.2. Tipo de evento;

- 1.140.3. Nome da máquina ou objeto para quem a requisição foi feita;
- 1.140.4. Categoria da URL;
- 1.140.5. Reputação da URL
- 1.140.6. DNS record type;
- 1.140.7. Status do evento e motivo do status;
- 1.140.8. VPN: Login e Logout/Disconnect;
- 1.140.9. IP Externo;
- 1.140.10. Tipo de evento;
- 1.140.11. Nome de usuário;
- 1.140.12. Status do evento e Razão do status;
- 1.140.13. Agente
- 1.140.14. Sistema operacional
- 1.140.15. Endereço MAC
- 1.140.16. Tipo de conexão
- 1.140.17. IP de destino
- 1.140.18. Dispositivo de destino
- 1.140.19. Reputação do IP Externo;
- 1.140.20. Web proxies: Proxy access/HTTP Request
- 1.140.21. URL da requisição HTTP;
- 1.140.22. Categorização da URL;
- 1.140.23. Reputação da URL;
- 1.140.24. IP de origem;

- 1.140.25. Nome de usuário;
  - 1.140.26. Tamanho do Upload;
  - 1.140.27. Tamanho do Download
  - 1.140.28. Duração da sessão;
  - 1.140.29. Código do status HTTP;
- 1.141. A solução deverá ter pesquisas pré-definidas de eventos do tipo:
- 1.141.1. Requisições DNS feitas para sites malicioso;
  - 1.141.2. Falhas de requisições web para sites maliciosos;
  - 1.141.3. Falhas de logins de VPN a noite;
  - 1.141.4. Falhas de logins de VPN durante o fim de semana;
  - 1.141.5. Falhas de logins de VPN partindo de fontes suspeitas;
  - 1.141.6. Falhas de logins de VPN feitos por usuários desabilitados ou inativos;
  - 1.141.7. Lista de todas as conexões VPN abertas por mais de um dia esse mês;
  - 1.141.8. Login de VPN a partir de país listado em Blacklist;
  - 1.141.9. Login de VPN a partir de fonte suspeita;
  - 1.141.10. Login de VPN a partir de fonte anonima;
  - 1.141.11. Falhas de requisições web feitas por usuários desabilitados ou inativos;
  - 1.141.12. Maior download de sites de storage na semana;
  - 1.141.13. Maior upload de sites de storage na semana;
  - 1.141.14. Maior download de site web suspeito no dia e na semana;
  - 1.141.15. Maior upload de site web suspeito no dia e na semana;
  - 1.141.16. Requisições a sites web suspeitos;

- 1.141.17. A solução deverá suportar receber eventos syslog de dispositivos que utilizem TLS;
- 1.141.18. A solução deverá identificar e alertar eventos originados em geolocalização suspeita para a organização que serão identificadas a partir do IP externo do usuário, quando coletado;
- 1.142. A solução deverá oferecer proteção e alerta para ataques do tipo:
  - 1.142.1. Mudança entre localização física distante em curto período;
  - 1.142.2. Credentials stuffing;
  - 1.142.3. Força bruta;
  - 1.142.4. Tunelamento por DNS;
  - 1.142.5. Reconhecimento por DNS Zone Transfer;
  - 1.142.6. DNS Cache Snooping;
  - 1.142.7. DNS Cache poisoning

## **2. ITEM 2: SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO**

- 2.1.Os serviços de instalação e configuração deverão compreender, no mínimo:
- 2.2.a implantação completa do projeto, ou seja, deverão contemplar todos os componentes no ambiente tecnológico dessa administração;
- 2.3.responsabilização por todos os instrumentais necessários durante o período de implantação e testes de aceitação;
- 2.4.instalação e configuração de todo ferramental tecnológico fornecido para atender as funcionalidades e requisitos descritos.
- 2.5.providenciar o planejamento de testes, fornecendo um “Plano de Homologação e Testes” contendo todo o processo de homologação dos produtos e detalhamento dos testes que serão executados para validar a solução implementada;

- 2.6. execução de uma série de testes funcionais básicos para verificar o perfeito funcionamento do ambiente, seguindo os procedimentos definidos no “Plano de Homologação e Testes”, sendo tais testes a serem obrigatoriamente executados nos componentes de hardware e software envolvidos no projeto;
- 2.7. elaboração da “Documentação e Finalização do Projeto”, que consiste na consolidação de toda a documentação gerada no projeto, seja esta técnica e ou gerencial.
- 2.8. Caberá à Contratada a disponibilização de todos os recursos necessários à instalação da solução.

### **3. ITEM 3: SERVIÇO DE TREINAMENTO**

- 3.1. Os treinamentos deverão contemplar a explanação teórica e prática para administradores da solução adquirida.
- 3.2. Os treinamentos poderão ser remotos ou a CONTRATANTE disponibilizará em seu ambiente uma sala para a execução dos treinamentos, com infraestrutura e apoio básicos (mesas, cadeiras, projetor, tela de projeção, computadores); em caso de impossibilidade de realização no ambiente da CONTRATANTE, caberá à Contratada arcar com toda a infraestrutura (salas, instalações e equipamentos, recursos audiovisuais, coffee-break etc.).
- 3.3. O treinamento a ser ofertado não possui obrigatoriedade de ser oficial do Fabricante da solução, contudo deve ser baseado em documentação oficial ou autorizado por ele.
- 3.4. A carga mínima exigida para este treinamento é de 20 horas.
- 3.5. A atividade de treinamento e capacitação deverá ser realizada em dias úteis, com duração máxima de até 4 (quatro) horas de instrução diária, com a possibilidade de dividir a turma em dois períodos.
- 3.6. Poderão ser demandadas a quantidade de até 2 (duas) turmas, sendo cada uma com no máximo 10 (dez) participantes.

3.7.A CONTRATANTE resguardar-se-á do direito de acompanhar e avaliar o treinamento com instrumento próprio e, caso a mesma não atinja os requisitos mínimos especificados, esta deverá ser reestruturada e aplicada novamente, sem nenhum custo adicional à CONTRATANTE.

3.8.O conteúdo programático do treinamento deverá contemplar, no mínimo, mas não se restringindo, informações necessárias a:

3.9.Procedimentos de instalação física e lógica;

3.10. Procedimentos necessários à configuração técnica e a completa operação do produto;

3.11. Procedimentos de manutenção do produto que devem ser realizados pelos técnicos do Órgão;

3.12. Apresentação geral da solução fornecida;

3.13. Descrição detalhada das partes e componentes de toda a solução, apresentando suas características funcionais;

3.14. Introdução do conceito de classificação, monitoramento e auditoria de dados e comportamento de usuários;

3.15. Visão completa da estrutura do AD, com possibilidades de administrar seu repositório de usuários e grupos de segurança utilizando uma interface única, juntamente com a gestão de seus servidores de arquivos;

3.16. Auditoria eficiente do Active Directory e File Server, fornecendo à equipe de TI visibilidade de todos os eventos ocorridos;

3.17. Gestão e controle de Permissionamento, de Registro de Eventos, de Análise Comportamental e Forense de todas as plataformas monitoradas;

3.18. Criação e/ou emissão de Relatórios, visando facilitar o controle sobre o que acontece em todos os ambientes;

3.19. Alertas de eventos, quando alguma ação for disparada;

- 3.20. Consultas e pesquisas de eventos fora de comportamento normal.
- 3.21. Auditoria de autenticação em aplicações web.
- 3.22. Outros tópicos da solução necessários ao pleno domínio da solução e suas Integrações poderão ser explanados em comum acordo ente as partes na Reunião Inicial de Projeto.
- 3.23. Quando da conclusão do treinamento, a Contratada disponibilizará à CONTRATANTE relatório da execução do evento, contendo no mínimo os seguintes dados:
  - 3.24. Nomes dos participantes e respectivo controle de frequência;
  - 3.25. Conteúdo do treinamento aplicado;
  - 3.26. Data e Hora;
  - 3.27. Carga horaria executada.

#### **4. DA GARANTIA E SUPORTE TÉCNICO**

- 4.1.A contratada deverá prover a garantia, atualização e suporte técnico da solução durante toda a vigência contratual, a partir da data de emissão do Termo de Recebimento Definitivo referente à implantação e operacionalização da solução no ambiente tecnológico do MinC, e deverá contemplar obrigatoriamente no mínimo:
  - 4.2.Atualização das versões dos softwares fornecidos, se novas versões forem disponibilizadas;
  - 4.3.Atualização dos softwares fornecidos se houver lançamento de novos softwares em substituição aos fornecidos, ou mesmo não sendo uma substituição, se ficar caracterizada uma descontinuidade dos softwares fornecidos;
  - 4.4.Correções de falhas (bugs) de software durante o período contratual, sendo executadas pela Contratada e/ou pelo Fabricante da solução, sem ônus adicionais;

- 4.5. Entrega, por parte da Contratada, de manuais técnicos e/ou documentação da solução fornecida, já entregues anteriormente, em caso de alterações dos mesmos, sem ônus adicionais para a Contratante;
- 4.6. As novas versões do objeto contratado deverão ser disponibilizadas em até 5 (cinco) dias corridos, a partir do lançamento oficial da versão.
- 4.7. Caso os serviços de manutenção e suporte técnico para todos os componentes da solução não sejam executados diretamente pela Contratada, mas sim pelo próprio Fabricante ou por empresa(s) representante(s) ou credenciada(s) por este, a Contratada deverá comunicar tal fato ao MinC, e assegurar que todos os padrões de atendimento e demais requisitos contratuais serão cumpridos. O aceite por parte dessa administração do atendimento não exime a Contratada da responsabilidade integral pelo atendimento e cumprimento dos prazos acordados.
- 4.8. Somente serão aceitas soluções originais do fabricante dos componentes da solução.
- 4.9. A Contratada deverá disponibilizar acesso total ao conteúdo presente em área restrita de suporte no endereço eletrônico (website) para todos os produtos que compõem a solução, contemplando toda a documentação técnica (guias de instalação/configuração atualizados, FAQ's, "troubleshootings", com pesquisa efetuada através de ferramentas de busca) e atualizações.
- 4.10. O atendimento deverá ser sob o regime 24x7 (24 horas por dia, 7 dias na semana), com disponibilidade de Central de Atendimento para abertura de chamados via sistema, e-mail, ligação gratuita ("0800") ou por Ordem de Serviço (O.S.).
- 4.11. O acesso para 'downloads' de 'patches', 'fixes', 'drivers' e quaisquer outras atualizações necessárias, devem estar disponíveis 24x7 (vinte e quatro horas por dia, sete dias por semana), durante todo o período de suporte, e podem ser feitos através de http ou ftp, no sítio do fabricante do 'software';
- 4.12. A Contratante deve ter o direito de realizar a atualização do software durante todo o período de suporte técnico, por uma versão mais recente quando disponibilizada, e



sempre que julgar necessário. As novas versões devem estar disponíveis para ‘download’, no sítio do fabricante do ‘software’;

4.13. Caso seja necessária a utilização de senha para ‘download’ de ‘patches’, ‘fixes’, ‘drivers’ e quaisquer outras atualizações no sítio do fabricante do ‘software’, esta deverá ser fornecida diretamente à Contratante, durante todo o período de manutenção;

4.14. Todo e qualquer licenciamento deverá ser feito em nome da Contratante, durante todo o período de manutenção;

4.15. A vigência contratual abrangerá a prestação de suporte, manutenção e atualização da solução pelo período contratual a partir da emissão do Termo de Recebimento Definitivo da solução.

4.16. Durante o período de vigência contratual, o licitante vencedor deverá atender às solicitações da CONTRATANTE, em qualquer horário, respeitando as condições e níveis de serviço especificados.

4.17. Entende-se por “Garantia” ou “Suporte” ou “Manutenção”, doravante denominada unicamente como “Garantia”, toda atividade do tipo “corretiva” não periódica que variavelmente poderá ocorrer, durante todo o período de garantia; esta possui suas causas em falhas e erros no software, e trata da correção dos problemas atuais e não iminentes de desenvolvimento do mesmo. Esta “Garantia” inclui os procedimentos destinados a recolocar em perfeito estado de operação os serviços e produtos ofertados, devendo contemplar, sem nenhum ônus, as seguintes atividades incluindo, mas não se limitando a:

4.18. recuperação de desastres, desinstalações, reconfigurações ou reinstalações decorrentes de falhas de software;

4.19. atualização da versão de software – toda e qualquer evolução incluindo correções em bibliotecas, “patches”, “fixes”, “service packs”, “releases”, “versions”, “builds”, vacinas extras específicas, “updates”, “upgrades”, e englobando inclusive versões

não sucessivas, nos casos em que a liberação de tais versões ocorra durante o período de garantia especificado;

4.20. qualquer correção decorrente de erros ou falhas cometidas na execução dos serviços contratados e/ou decorrentes de integração e adequação sistêmica, desde que, comprovadamente, não tenham se dado em função de falhas nas especificações feitas pelo MinC.

4.21. Os serviços de manutenção e suporte técnico deverão ser executados com base nos seguintes parâmetros:

Modalidade	Descrição
Atendimento Telefônico (Help Desk)	Chamados abertos através de ligação telefônica, e-mail ou sistema Web, em regime de 24x7: 24 horas por dia, 7 dias por semana.
Atendimento Remoto	Atendimento remoto de chamados técnicos, por meio de acesso remoto via VPN, "TeamViewer", "Cisco Webex" "SysAid" ou outra ferramenta similar, desde que tecnicamente viável e mediante autorização expressa da dessa administração conforme os padrões de segurança do Órgão, objetivando análise e solução remota dos problemas apresentados.
Atendimento Presencial (on-site)	Atendimentos técnicos executados nas dependências da dessa administração, através de visita de profissional especializado, com a finalidade de resolver os chamados.

4.22. Quando couber, no caso de atendimento remoto por meio de ferramenta adequada (via VPN, por exemplo), este deverá ser comunicado previamente à CONTRATANTE, que efetuará o cadastramento do responsável pelo atendimento, e disponibilizará os recursos necessários para a execução da demanda.

4.23. Todo o serviço de suporte técnico/manutenção deve ser solicitado inicialmente via Help Desk, ficando a transferência do atendimento para o Atendimento Remoto condicionado à autorização da dessa administração.

4.24. Todo o serviço de suporte técnico/manutenção solicitado inicialmente via Help Desk, deve ser transferido para o Atendimento Presencial quando o atendimento do Help Desk não for suficiente para solução do problema sem a intervenção presencial de um técnico.

#### 4.25. Definição de prazos:

Prazo	Descrição
Início de Atendimento	Período que compreende o tempo entre o registro de abertura do chamado técnico até o primeiro contato do técnico e/ou comparecimento de um técnico ao local (quando necessário).
Solução de Contorno	Período compreendido entre o “Início de Atendimento” e a apresentação de solução de contorno, sendo definida como uma alternativa que viabilize a operacionalização do ambiente até o tratamento definitivo do incidente.
Solução Definitiva	Período decorrente entre o “Início de Atendimento” até o momento em que a solução for disponibilizada em plena e perfeita condição de funcionamento no local onde está implantada, estando condicionada à aprovação e ateste da equipe técnica da dessa administração, conforme o caso.

4.26. A critério dessa administração o Início do Atendimento, assim como sua execução poderá ser agendado ou adiado e, nestes casos, a contagem de horas para a resolução do chamado fica prorrogada para ser contabilizada a partir da data do novo agendamento.

4.27. A Contratada poderá solicitar a prorrogação de qualquer dos prazos de início e término de atendimento de chamados, desde que o faça antes do seu vencimento e com a devida justificativa.

#### 4.28. Níveis de Severidade:

Severidade	Descrição	Atendimento
CRÍTICA	Incidente que ocasiona a inoperância total da solução ou de algum componente, com a indisponibilidade para qualquer tipo de funcionalidade, comprometendo de forma crítica o ambiente negocial da dessa administração.	Os chamados de Severidade CRÍTICA deverão ser atendidos a qualquer hora do dia ou da noite (cobertura 24 x 7), seja em dia útil, final de semana ou feriado, e não poderão ser interrompidos até a recuperação plena do funcionamento da Solução, mesmo que se estenda para períodos noturnos e dias não úteis como sábados, domingos e feriados.

		O atendimento cuja severidade for classificada como CRÍTICA deverá ser realizado obrigatoriamente ON-SITE.
ALTA	Incidente que ocasiona a inoperância parcial da solução ou de algum componente, com o comprometimento do funcionamento e/ou performance da solução, porém sem interrupção completa.	Os chamados de Severidade ALTA deverão ser atendidos a qualquer hora do dia ou da noite (cobertura 24 x 7), seja em dia útil, final de semana ou feriado e não poderão ter o atendimento interrompido até a recuperação plena do funcionamento da Solução, mesmo que se estenda para períodos noturnos e dias não úteis como sábados, domingos e feriados.  Os chamados de Severidade ALTA poderão ser opcionalmente atendidos on-site a critério da dessa administração.
MÉDIA	Incidente que não ocasiona indisponibilidade do sistema, contudo afeta de modo significativo a performance desta, sendo preliminarmente solucionado temporariamente mediante aplicação de solução de contorno disponível.	Os chamados de Severidade MÉDIA deverão ser atendidos em dias úteis, em horário comercial (das 8:00 às 18:00), e opcionalmente em final de semana ou feriado, conforme agendamento prévio.
BAIXA	Atividades que não impactam na disponibilidade da solução, como diagnósticos, configurações, consultas técnicas, esclarecimentos.	Os chamados de suporte de Severidade BAIXA opcionalmente poderão ser atendidos em dias úteis, em horário comercial (das 8:00 às 18:00).

4.29. A severidade do chamado poderá ser reavaliada quando verificado que esta foi erroneamente aplicada, passando a contar no momento da reavaliação os novos prazos de atendimento e resolução.

4.30. Para o atendimento das atividades demandadas, a Contratada deverá atender os seguintes prazos constantes no quadro a seguir, conforme o nível de severidade aplicado (Acordo de Níveis de Serviço):

Severidade	Início de Atendimento	Solução de Contorno	Solução Definitiva
CRÍTICA	Até 2 horas.	Até 24 horas.	Até 72 horas.
ALTA	Até 4 horas.	Até 48 horas.	Até 96 horas.
MÉDIA	Até 8 horas.	Até 72 horas.	Até 120 horas.
BAIXA	Até 12 horas.	Até 96 horas.	Até 240 horas.

- 4.31. Casos em que a Contratada não puder executar os serviços de suporte até o limite dos prazos de atendimento, tais chamados não atendidos deverão ser devidamente documentados, contendo a justificativa da Contratada e o aceite do Gestor, observando-se o preceito da razoabilidade e considerando-se os prejuízos à Contratante. Em caso de não aceite da justificativa por parte da Contratante, serão aplicadas as penalidades cabíveis à Contratada.
- 4.32. O não atendimento a um chamado técnico somente poderá ser justificado em casos de motivo de força maior ou por dependência da CONTRATANTE; neste caso, a Contratada deverá formalizar antecipadamente ao Gestor do Contrato ou ao Fiscal Técnico os motivos que impedem a execução do serviço demandado.
- 4.33. Todos os serviços deverão ser prestados em consonância com as melhores práticas e recomendações de mercado e do Fabricante da solução.
- 4.34. Um chamado técnico só poderá ser dado como concluído após verificação e aceite do responsável da CONTRATANTE.
- 4.35. Chamados fechados sem anuência da Contratante ou sem que a(s) demanda(s) tenha(m) sido de fato resolvida(s) deverão ser reabertos e os prazos contados a partir da abertura original dos chamados, inclusive para efeito de aplicação das sanções previstas.
- 4.36. A Contratada deverá manter um cadastro das pessoas indicadas pela Contratante, as quais poderão efetuar abertura e autorizar o fechamento de chamados.
- 4.37. Cada pessoa cadastrada no sistema deverá receber identificação e senha que permitam acesso seguro ao sistema de informação da Contratada, de maneira a evitar que pessoas não autorizadas possam acionar o serviço.

- 4.38. A conclusão do atendimento técnico se dará quando ocorrer a “Solução Definitiva” do problema mencionado no chamado (Severidades CRÍTICA, ALTA e MÉDIA), e/ou sanando a dúvida (Severidade BAIXA), estando a conclusão condicionada à aprovação do Fiscal Técnico do Contrato.
- 4.39. É vedado à Contratada interromper o atendimento até que o serviço seja recolocado em pleno estado de funcionamento, mesmo que se estendam para períodos noturnos, sábados, domingos e feriados, não cabendo custos adicionais à Contratante.
- 4.40. Em caso de vício(s) insanável(is) nos componentes da solução que impossibilitem o funcionamento da solução de segurança, o(s) componente(s) defeituoso(s) deverá(ão) ser substituído(s) definitivamente em até 10 (dez) dias úteis após a notificação da Contratante, juntamente com a descrição sucinta e precisa do problema ocorrido.
- 4.41. Sempre que houver quebra de Acordo de Nível de Serviços, a Contratante emitirá notificação à Contratada, que terá prazo máximo de 5 (cinco) dias corridos, contados a partir do recebimento do ofício, para apresentar as justificativas para as falhas verificadas. Caso não haja manifestação dentro desse prazo ou caso a Contratante entenda serem improcedentes as justificativas apresentadas, será iniciado processo de aplicação de penalidades previstas, conforme o nível de serviço transgredido.
- 4.42. Na ocorrência de uma situação emergencial na qual já exista chamado técnico aberto, é esperado que tanto o atendimento quanto o restabelecimento da solução sejam feitos de forma imediata, sem a necessidade de abertura de novo chamado técnico.
- 4.43. Chamados fechados sem anuência da Contratante ou sem que a(s) demanda(s) tenha(m) sido de fato resolvida(s) deverão ser reabertos e os prazos contados a partir da abertura original dos chamados, inclusive para efeito de aplicação das sanções previstas.
- 4.44. Os chamados técnicos só poderão ser encerrados após expressa anuência do Gestor do Contrato ou do Fiscal Técnico.

- 4.45. Chamados fechados sem anuência da dessa administração ou sem que a(s) demanda(s) tenha(m) sido de fato resolvida(s) deverão ser reabertos e os prazos contados a partir da abertura original dos chamados, inclusive para efeito de aplicação das sanções previstas.
- 4.46. A Contratada deverá manter um cadastro das pessoas indicadas pela dessa administração, as quais poderão efetuar abertura e autorizar o fechamento de chamados.
- 4.47. Cada pessoa cadastrada no sistema deverá receber identificação e senha que permitam acesso seguro ao sistema de informação da Contratada, de maneira a evitar que pessoas não autorizadas possam acionar o serviço.
- 4.48. No fechamento do chamado deverá ser emitido, por parte da Contratada, um "Relatório Técnico de Atendimento", a ser encaminhado à dessa administração, apresentando no mínimo as seguintes informações:
- 4.49. Número de identificação do chamado;
- 4.50. Data e hora do chamado;
- 4.51. Data e hora do início e do término do atendimento;
- 4.52. Total de horas utilizadas para atendimento completo;
- 4.53. Severidade da ocorrência;
- 4.54. Identificação do problema/incidente;
- 4.55. Solução de contorno aplicada (quando couber);
- 4.56. Solução definitiva aplicada.

