Argos - Analisador Forense
Documento de Requisitos de Software

1. Introdução

Este documento visa definir e consolidar os requisitos do sistema SaaS de análise e registro de logs de acessos, que será desenvolvido ao longo da disciplina de Análise e Projeto de Software pelos alunos do curso de Ciência da Computação da Universidade Católica de Brasília: Gustavo Horestee Santos Barros, Maria Clara Fernandes Rangel, Matheus Vinycius Vieira Batista, Pedro Henrique Oliveira Marques e Nathalia Gonçalves Silva. O sistema proposto é voltado para a área de análise forense digital, oferecendo suporte à detecção de atividades suspeitas, à condução de investigações de segurança e à geração de relatórios de conformidade prontos para auditorias. A solução pretende atender empresas com múltiplos clientes, equipes especialmente de SOC (Security Operations Center), fornecendo uma interface de monitoramento e controle interativo de logs baseada em regras heurísticas e integração com blacklists de IPs e domínios maliciosos.

A elicitação dos requisitos foi conduzida entre os dias 12/04/2025 e 21/04/2025, utilizando técnicas de análise de sistemas de segurança, levantamento de padrões recorrentes em incidentes forenses e prototipagem inicial com base na simulação de cenários de ataque e resposta. O sistema será desenvolvido como um serviço (Software as a Service – SaaS), com comunicação via API (Application Programming Interface), buscando garantir escalabilidade, segurança e facilidade de integração com outras ferramentas. Para mais informações sobre os objetivos, funcionalidades e limitações do projeto, recomenda-se a leitura do Documento de Visão, disponível em: Documento_Visao.

2. Visão geral dos requisitos funcionais

Backlog do Produto

ID	Título	Valor de Negócio	Prioridade (MoSCoW)	Estimativa (Escala de Fibonacci)	Dependências
HU1	Incluir um novo usuário	Um gestor de SOC, deve incluir novos usuários, coletando dados pessoais (nome, e-mail e perfil), que devem ser validados, após o registro. O novo usuário irá receber as novas credenciais por e-mail e deve cadastrar uma nova senha.	Deve ter	5	F1 RN01 RN02 RN03 RN04 RN05 RNF003 RNF004 RNF016 RNF018
HU2	Editar dados cadastrais dos usuários	Somente um gestor tem permissão para editar nome, e-mail e perfil	Poderia ter	2	F1 RN02 RN03 RN05 RN17 RNF003 RNF004 RNF018
HU3	Alterar senha de usuário	Somente um gestor tem permissão para resetar a senha de um usuário	Poderia ter	2	F1 RN03 RN04 RNF003

		para ser cadastrada novamente.			RNF004 RNF018
HU4	Visualizar usuários existentes	Um gestor de SOC, pode visualizar os usuários existentes do sistema e aplicar filtros para buscas rápidas.	Poderia ter	2	F1 RN01 RN02 RN03 RNF003 RNF004
HU5	Desativar usuários	Somente um gestor de SOC tem permissão para desativar um usuário que tenha sido desligado ou transferido de área.	Poderia ter	1	F1 RN01 RN02 RN05 RNF003 RNF004
HU6	Ativar usuários	Somente um gestor de SOC tem permissão para ativar um usuário que tenha sido religado ou transferido de área	Poderia ter	1	F1 RN01 RN02 RN05 RNF003 RNF004
HU7	Criar perfil de permissão	Um gestor de SOC, deve criar diferentes perfis configurando suas permissões e evitando duplicidade de perfis.	Deve ter	8	F2 RN02 RNF004 RNF018
HU8	Atribuir perfil ao usuário	Somente um gestor de SOC tem permissão para atribuir os perfis aos usuários	Deve ter	8	F2 RN02 RNF004

		correspondentes.			
HU9	Visualizar perfil de permissões existente	Somente um gestor de SOC pode visualizar o perfil de permissões existentes e aplicar filtros para buscas rápidas e objetivas.	Poderia ter	3	F2 RN02 RNF004
HU10	Editar permissões de perfil	Somente um gestor pode editar, alterar as permissões de acesso nos perfis existentes.	Deveria ter	5	F2 RN02 RN06 RNF004
HU11	Excluir perfil	Somente um gestor de SOC pode excluir um perfil de acesso.	Poderia ter	3	F2 RN02 RNF004
HU12	Realizar controle lógico de acesso	Os usuários só podem acessar as funcionalidades que tiverem atribuídas ao seu perfil. As tentativas de acessos a funcionalidades não autorizadas ao perfil solicitante devem ser bloqueadas e registradas para fins de auditoria.	Deve ter	8	F3 RN06 RNF003 RNF004.
HU13	Realizar monitoramento em tempo real de logs de acesso	Gestor de SOC ou analista de segurança (nível 1, 2 e 3) ou especialista forense ou	Deve Ter	13	F4 RN19 RN29 RNF002

		analista de risco ou DPO, devem monitorar os logs de acesso do sistema operacional da empresa em tempo real, visualizando atualizações a cada 5 minutos e recebendo informações detalhadas de eventos.			RNF003 RNF014 RNF016
HU14	Configurar ponto de monitoramento	Gestor de SOC ou analista de segurança (nível 1, 2 e 3) ou especialista forense ou analista de risco ou DPO, tem autorização para adicionar ponto de monitoramento, conectar e validar porta de escuta.	Deve Ter	13	F4 RN27 RN28 RNF004 RNF018
HU15	Aplicar filtros nos pontos de monitoramento	Devem utilizar filtros nos pontos de monitoramento para filtrar status, endereços e características dos sistemas.	Deveria ter	7	F4 RN27 RNF018
HU16	Configurar alerta de atividades suspeitas	Gestor de SOC ou analista de segurança (nível 1, 2 e 3) ou especialista forense ou analista de risco ou DPO, devem poder criar regras de alerta personalizadas, com nomes descritivos e nível de severidade.	Deve Ter	8	F5 RN07 RN08 RN09 RN18 RN19 RNF004 RNF013 RNF018

HU17	Notificação de alerta de atividade suspeita	Gestor de SOC ou analista de segurança (nível 1, 2 e 3) ou especialista forense ou analista de risco ou DPO, devem poder receber notificações automáticas no sistema sobre atividades suspeitas e deve ser usado cooldown para evitar o envio de notificações repetidas.	Deve ter	8	F5 RN07 RN08 RN09 RN12 RN18 RN23 RNF002
HU18	Ler alerta de atividades suspeitas	Gestor de SOC ou analista de segurança (nível 1, 2 e 3) ou especialista forense ou analista de risco ou DPO, devem poder ler as notificações com informações de alerta relevantes como identificação da regra de alerta, data, hora e detecção da atividade suspeita e nível de severidade.	Deveria ter	5	F5 RN12 RNF003
HU19	Disponibilizar Relatório Diário de Atividades Suspeitas	Analista de segurança (nível 1, 2 e 3), gestor de SOC, especialista forense, analista compliance, analista de risco, DPO, auditor interno, devem ter acesso fácil e regular	Deveria Ter	5	F6 RN11 RNF006 RNF014

		aos relatórios gerados automaticamente após 24hrs.			
HU20	Filtrar Relatório Diário de Atividades Suspeitas	Analista de segurança (nível 1, 2 e 3), gestor de SOC, especialista forense, analista compliance, analista de risco, DPO, auditor interno, podem filtrar as informações de atividades suspeitas, nível de severidade das atividades, atividades de um usuário específico e endereço IP, para gerar relatórios específicos.	Poderia ter	5	F6 RN11 RN12 RNF018
HU21	Exportar Relatório Diário de Atividades Suspeitas	Analista de segurança (nível 1, 2 e 3), gestor de SOC, especialista forense, analista compliance, analista de risco, DPO, auditor interno, devem poder exportar o relatório em formato de arquivo PDF e CSV/Excel.	Poderia ter	3	F6 RN11 RN12 RNF003
HU22	Visualizar Ameaças por Severidade em um Painel	Analista de segurança (nível 1, 2 e 3), gestor de SOC, especialista forense, analista de risco, DPO, devem poder visualizar as ameaças em um dashboard atualizado de 5 em 5 minutos, oferecendo as	Deve ter	8	F7 RN12 RNF002 RNF005 RNF030

		atividades suspeitas originadas de alertas agrupadas e quantificadas por nível de severidade.			
HU23	Filtrar de Lista de Incidentes por Nível de Severidade	Analista de segurança (nível 1, 2 e 3), gestor de SOC, especialista forense, analista de risco, DPO, devem poder filtrar as ameaças e incidentes por nível de severidade.	Deveria ter	5	F7 RN12 RNF018
HU24	Buscar incidentes no histórico	Analista de segurança (nível 1, 2 e 3), gestor de SOC, especialista forense, analista compliance, DPO, auditor interno, devem poder realizar buscas no histórico de incidentes, podendo ordenar os resultados por colunas e datas, podem aplicar filtros por categoria de data, IP, usuário, severidade e atividade suspeita.	Poderia ter	5	F8 RN10 RN13 RN20 RNF004 RNF006 RNF 015 RNF 016 RNF 019
HU25	Análise Detalhada de Incidente do Histórico	Analista de segurança (nível 1, 2 e 3), gestor de SOC, especialista forense, analista compliance, DPO, auditor interno, devem poder fazer comparação de incidentes por períodos e exportação dos dados no formato de imagem ou gráfico.	Poderia ter	3	F8 RN10 RN13 RN20 RNF006 RNF014 RNF015

HU26	Acompanhar Evolução do Volume de Incidentes	Analista de segurança (nível 1, 2 e 3), gestor de SOC, especialista forense, analista compliance, DPO, auditor interno, devem poder acessar uma visualização analítica que demonstra a evolução do volume total de incidentes de segurança ao longo do tempo, podendo fazer comparação e análise de períodos de tempo, além de exportar os dados em formato CSV/Excel.	Poderia ter	5	F9 RN21 RNF006 RNF015
HU27	Identificar os Tipos de Incidentes Recorrentes	Analista de segurança (nível 1, 2 e 3), gestor de SOC, especialista forense, analista compliance, DPO, auditor interno, devem fazer seleção de período para análise, usar o histórico de incidentes para agrupar e contar as ocorrências, além de usar Drill-Down para analisar incidentes individuais.	Poderia ter	5	F9 RN21 RNF006 RNF015
HU28	Disponibilizar relatório de tendências sobre incidentes	Analista de segurança (nível 1, 2 e 3), gestor de SOC, especialista forense, analista compliance, analista de risco, DPO, auditor interno, devem ter acesso a relatórios de	Deveria ter	2	F10 RN13 RN22 RNF006 RNF015

		tendências sobre incidentes, com detalhamento dos parâmetros de período, volume e nível de severidade.			RNF014
HU29	Exportar relatório de tendências sobre incidentes	Analista de segurança (nível 1, 2 e 3), gestor de SOC, especialista forense, analista compliance, analista de risco, DPO, auditor interno, devem poder exportar os relatórios com nomes padronizados no formato PDF e CSV/Excel.	Poderia ter	2	F10 RN21 RN22 RNF003
HU30	Disponibilizar relatório de incidentes com dados pessoais	Analista de segurança (nível 1, 2 e 3), gestor de SOC, especialista forense, analista compliance, analista de risco, DPO, auditor interno, devem ter acesso a relatórios de incidentes com dados pessoais, com detalhamento dos parâmetros de período, volume e nível de severidade. D	Poderia ter	2	F11 RN23 RN24 RNF003
HU31	Exportar relatório de incidentes com dados pessoais	Analista de segurança (nível 1, 2 e 3), gestor de SOC, especialista forense, analista compliance, analista de risco, DPO, auditor interno, devem poder	Poderia ter	2	F11 RN23 RN24 RNF003

		exportar os relatórios com nomes padronizados no formato PDF e CSV/Excel.			
HU32	Disponibilizar relatório de Atividade de Login Bem-Sucedido	Analista de segurança (nível 1, 2 e 3), gestor de SOC, especialista forense, analista compliance, analista de risco, DPO, auditor interno, devem ter acesso a relatórios de atividade de login bem-sucedido, com detalhamento dos parâmetros de período, volume e nível de severidade.	Poderia ter	2	F12 RN25 RNF006 RNF014 RNF015
HU33	Exportar relatório de Atividade de Login Bem-Sucedido	Analista de segurança (nível 1, 2 e 3), gestor de SOC, especialista forense, analista compliance, analista de risco, DPO, auditor interno, devem poder exportar os relatórios com nomes padronizados no formato PDF e CSV/Excel.	Poderia ter	2	F12 RN25 RNF006 RNF014 RNF015
HU34	Disponibilizar Relatório de Tentativas de Login Falhadas	Analista de segurança (nível 1, 2 e 3), gestor de SOC, especialista forense, analista compliance, analista de risco, DPO, auditor interno, devem ter	Poderia ter	2	F13 RN08 RN26 RNF006

		acesso a relatórios de tentativas de login falhadas, com detalhamento dos parâmetros de período, volume e nível de severidade.			RNF003 RNF014 RNF015
HU35	Exportar relatório de Atividade de Login Falhada	Analista de segurança (nível 1, 2 e 3), gestor de SOC, especialista forense, analista compliance, analista de risco, DPO, auditor interno, devem poder exportar os relatórios com nomes padronizados no formato PDF e CSV/Excel.	Poderia ter	2	F13 RN08 RN26 RNF003

3. Especificação dos requisitos funcionais

- **HISTÓRIA DE USUÁRIO 1:**

Título: HU1. Incluir um novo usuário.

Responsável: Nathalia G. Silva

Descrição estendida:
COMO gestor de uma área SOC, **QUERO** incluir um novo usuário, **PARA** que ele utilize o sistema de acordo com seu Perfil de Acesso **E** receba as credenciais por e-mail.

Critérios de aceite:

1. Dados obrigatórios não informados
   DADO que o gestor de uma área SOC não informou alguns dados obrigatórios, **QUANDO** o gestor realizar a inclusão do usuário, **ENTÃO** o sistema deve informar mensagem de erro próximo ao campo vazio destacando quais são os dados obrigatórios.

2. Usuário existente
   DADO que o gestor de uma área SOC informou um usuário já existente, **QUANDO** informar os dados de novo usuário, **ENTÃO** o sistema deve apresentar mensagem informando que o usuário já existe.

3. Validação de e-mail
   DADO que o gestor de uma área SOC informou um endereço de e-mail, **QUANDO** o gestor inserir um texto que não segue um formato de e-mail válido ("usuario@dominio_sem_ponto", "@dominio.com", "usuario@.com"), **ENTÃO** o sistema deve exibir uma mensagem de erro próxima ao campo de e-mail, indicando que o formato do endereço de e-mail é inválido, **E** o processo de inclusão do novo usuário deve ser impedido até que um endereço de e-mail com formato válido seja fornecido.

4. Validação de senha
   DADO que um novo usuário recebeu um link para definição de senha, **QUANDO** ele inserir uma senha no campo "Senha" que não atende os critérios, ter menos de 8 caracteres, ou não contém pelo menos uma letra maiúscula, ou não contém pelo menos um número, ou não contém pelo menos um caractere especial, **ENTÃO** o sistema deve exibir uma mensagem de erro, indicando quais critérios não foram atendidos **E** o processo de inclusão do novo usuário deve ser impedido até que uma senha que atenda a todos os critérios de complexidade seja fornecida.

Dependência/notas técnicas:
RN01: Identificação Única de Usuário;
RN02: Atribuição Obrigatória de Perfil de Acesso;
RN03: Dados Obrigatórios para Cadastro de Usuário;
RN04: Política de Complexidade de Senha;
RN05: Armazenamento Seguro de Credenciais.

Rastreabilidade (Documento de Visão):
F1. Manter cadastro de usuários;
RNF003 - Proteção de Dados Sensíveis;
RNF004 - Trilha de Auditoria;
RNF018 - Validação de Entrada de Dados.

- **HISTÓRIA DE USUÁRIO 2:**

Título: HU2. Editar dados cadastrais dos usuários.

Responsável: Nathalia G. Silva

Descrição estendida:

COMO gestor de uma área SOC, **QUERO** editar o nome, e-mail e perfil, **PARA** manter os dados cadastrais atualizados ou realizar ajustes em suas permissões.

Critérios de aceite:

1. Atualização de dados pessoais
   DADO que o gestor de uma área SOC solicitou a edição de um dado pessoal (nome, e-mail), **QUANDO** o gestor realizar a edição solicitada, **ENTÃO** o sistema deve informar mensagem de atualização bem-sucedida **E** realizar atualização no banco de dados.

2. Alteração de perfil de acesso
   DADO que o gestor de uma área SOC solicitou a alteração de um perfil de acesso, **QUANDO** o gestor realizar a alteração de usuário, **ENTÃO** o sistema deve apresentar mensagem de alteração bem-sucedida **E** realizar atualização no banco de dados.

Dependência/notas técnicas:
RN02: Atribuição Obrigatória de Perfil de Acesso;
RN03: Dados Obrigatórios para Cadastro de Usuário;
RN05: Armazenamento Seguro de Credenciais;
RN17: Atualização de Lista de Perfis na Edição de Usuário.

Rastreabilidade (Documento de Visão):
F1. Manter cadastro de usuários;
RNF003 - Proteção de Dados Sensíveis;
RNF004 - Trilha de Auditoria;
RNF018 - Validação de Entrada de Dados.

- **HISTÓRIA DE USUÁRIO 3:**

Título: HU3. Alterar senha de usuário.

Responsável: Nathalia G. Silva

Descrição estendida:
COMO gestor de uma área SOC, **QUERO** resetar a senha de um usuário existente, **PARA** que o usuário possa recuperar o acesso ao sistema em caso de esquecimento ou suspeita de comprometimento.

Critérios de aceite:

1. Alterar a senha
   DADO que o gestor de uma área SOC recebeu a solicitação de alteração de senha, **QUANDO** o gestor resetar a senha do usuário solicitante, **ENTÃO** o usuário recebe um link para alterar a senha.

Dependência/notas técnicas:
RN03: Dados Obrigatórios para Cadastro de Usuário;
RN04: Política de Complexidade de Senha.

Rastreabilidade (Documento de Visão):
F1. Manter cadastro de usuários;
RNF003 - Proteção de Dados Sensíveis;
RNF004 - Trilha de Auditoria;
RNF018 - Validação de Entrada de Dados.

- **HISTÓRIA DE USUÁRIO 4:**

Título: HU4. Visualizar usuários existentes

Responsável: Nathalia G. Silva

Descrição estendida:
COMO gestor de uma área SOC, **QUERO** visualizar através de uma lista todos os usuários cadastrados e seus perfis vinculados, **PARA** que eu possa ter uma visão geral de quem tem acesso ao sistema **E** mantenha o controle dos acesso.

Critérios de aceite:

1. Listar por filtro de perfil
   DADO que o gestor de uma área SOC deseja filtrar a lista de usuários por perfil, **QUANDO** o gestor selecionar o perfil desejado, **ENTÃO** o sistema deve listar os usuários que são vinculados àquele perfil.

2. Listar por ordem alfabética dos nomes
   DADO que o gestor de uma área SOC deseja filtrar a lista de usuários por ordem alfabética dos nomes **QUANDO** o gestor selecionar o listar por ordem alfabética, **ENTÃO** o sistema deve listar os usuários em ordem alfabética.

3. Buscar usuário
   DADO que o gestor de uma área SOC deseja selecionar um usuário, **QUANDO** o gestor seleciona os dados específico do usuário, **ENTÃO** o sistema apresenta o usuário correspondente com as especificações.

Dependência/notas técnicas:
RN01: Identificação Única de Usuário;
RN02: Atribuição Obrigatória de Perfil de Acesso;
RN03: Dados Obrigatórios para Cadastro de Usuário.

Rastreabilidade (Documento de Visão):
F1. Manter cadastro de usuários;
RNF003 - Proteção de Dados Sensíveis;
RNF004 - Trilha de Auditoria;

- **HISTÓRIA DE USUÁRIO 5:**

Título: HU5. Desativar usuário.

Responsável: Nathalia G. Silva

Descrição estendida:
COMO gestor de uma área SOC, **QUERO** desativar usuários que foram desligados ou transferidos de área, **PARA** que não possam acessar o sistema, mantendo o histórico de suas atividades anteriores para fins de auditoria.

Critérios de aceite:
1. Desativar usuário desligado ou transferido de área
   DADO que o gestor de uma área SOC deseja desativar um usuário, **QUANDO** o gestor desativar o usuário, **ENTÃO** o status do usuário desativado deve mudar para “inativo” e suas permissões devem ser retiradas.

2. Negar acesso de usuário desativado
   DADO que o usuário está desativado, **QUANDO** tentar realizar o login no sistema, **ENTÃO** o sistema deve gerar uma mensagem de acesso negado.

Dependência/notas técnicas:
RN01: Identificação Única de Usuário;

RN02: Atribuição Obrigatória de Perfil de Acesso;
RN05: Armazenamento Seguro de Credenciais.

Rastreabilidade (Documento de Visão):
F1. Manter cadastro de usuários;
RNF003 - Proteção de Dados Sensíveis;
RNF004 - Trilha de Auditoria;

- **HISTÓRIA DE USUÁRIO 6:**

Título: HU6. Ativar usuário

Responsável: Nathalia G. Silva

Descrição estendida:
COMO gestor de uma área SOC, **QUERO** ativar usuários que foram religados ou transferidos de volta para sua área, **PARA** que possam acessar o sistema, mantendo o histórico de suas atividades anteriores para fins de auditoria.

Critérios de aceite:

1. Ativar usuário religados ou transferido de área
   DADO que o gestor de uma área SOC deseja ativar um usuário, **QUANDO** o gestor ativar o usuário, **ENTÃO** o status do usuário ativado deve mudar para "ativo" e suas permissões devem ser renovadas.

2. Autorizar acesso de usuário ativado.
   DADO que o usuário está ativado, **QUANDO** tentar realizar o login no sistema, **ENTÃO** o sistema deve gerar uma mensagem de acesso autorizado.

Dependência/notas técnicas:
RN01: Identificação Única de Usuário;
RN02: Atribuição Obrigatória de Perfil de Acesso;
RN05: Armazenamento Seguro de Credenciais.

Rastreabilidade (Documento de Visão):
F1. Manter cadastro de usuários;
RNF003 - Proteção de Dados Sensíveis;
RNF004 - Trilha de Auditoria;

- **HISTÓRIA DE USUÁRIO 7:**

Título: HU7. Criar Perfil de Permissão.

Responsável: Nathalia G. Silva

Descrição estendida:
COMO gestor de uma área SOC, **QUERO** criar perfil de analista de segurança (nível 1, 2 e 3), gestor de SOC, especialista forense, analista compliance, analista de risco, DPO e auditor interno, **PARA** atribuir as permissões ao sistema apropriadas a cada usuário **E** manter os dados contidos no sistema Argos protegidos.

Critérios de aceite:

1. Dados obrigatórios não informados
   DADO que o gestor de uma área SOC não informou alguns dados obrigatórios, **QUANDO** o gestor realizar a criação do perfil, **ENTÃO** o sistema deve exibir uma mensagem de erro próxima ao campo vazio e destacar quais são os dados obrigatórios.

2. Perfil existente
   DADO que o gestor de uma área SOC informou um perfil já existente, **QUANDO** o gestor informar os dados de novo perfil, **ENTÃO** o sistema deve exibir uma mensagem de erro próxima ao campo vazio e informar que o perfil já existe.

Dependência/notas técnicas:
RN02: Atribuição Obrigatória de Perfil de Acesso.

Rastreabilidade (Documento de Visão):
F2. Manter perfil de permissões;
RNF004 - Trilha de Auditoria;
RNF018 - Validação de Entrada de Dados.

- **HISTÓRIA DE USUÁRIO 8:**

Título: HU8. Atribuir perfil ao usuário.

Responsável: Nathalia G. Silva

Descrição estendida:
COMO gestor de uma área SOC, **QUERO** atribuir um perfil de analista de segurança (nível 1, 2 e 3), gestor de SOC, especialista forense, analista compliance, DPO, auditor interno a um

usuário, **PARA** que cada usuário tenha acesso às informações que lhe são relevantes **E** evite acesso indevido de usuários não autorizados a dados sensíveis do sistema.

Critérios de aceite:

1. Atribuir um perfil ao usuário
   DADO que o gestor de uma área SOC atribui um perfil (exemplo: especialista forense) a um usuário, **QUANDO** o gestor realizar a atribuição do perfil ao usuário, **ENTÃO** o sistema deve informar mensagem de atribuição bem-sucedida.

2. Atribuir mais de um perfil a um usuário
   DADO que o gestor de uma área SOC atribui um perfil (exemplo: especialista forense) a um usuário que já está atribuído a analista compliance, **QUANDO** o gestor realizar a atribuição do perfil ao usuário, **ENTÃO** o sistema deve apresentar mensagem de erro informando que o usuário já tem um perfil atribuído.

Dependência/notas técnicas:
RN02: Atribuição Obrigatória de Perfil de Acesso.

Rastreabilidade (Documento de Visão):
F2. Manter perfil de permissões;
RNF004 - Trilha de Auditoria.

- **HISTÓRIA DE USUÁRIO 9:**

Título: HU9. Visualizar perfil de permissões existente.

Responsável: Nathalia G. Silva

Descrição estendida:
COMO gestor de uma área SOC, **QUERO** visualizar através de uma lista todos os perfis cadastrados e suas permissões, **PARA** que eu possa ter uma visão geral de qual perfil pode acessar as áreas do sistema **E** mantenha o controle dos acesso.

Critérios de aceite:

1. Listar por filtro de perfil
   DADO que o gestor de uma área SOC deseja filtrar a lista dos perfis, **QUANDO** o gestor selecionar o perfil desejado, **ENTÃO** o sistema deve apresentar o perfil selecionado com todas as suas permissões ativas e inativas.

2. Listar por filtro de permissão
   DADO que o gestor de uma área SOC deseja filtrar a lista dos perfis por permissões, **QUANDO** o gestor selecionar a permissão desejada, **ENTÃO** o sistema deve apresentar os perfis que apresentam aquela permissão ativada.

Dependência/notas técnicas:
RN02: Atribuição Obrigatória de Perfil de Acesso.

Rastreabilidade (Documento de Visão):
F2. Manter perfil de permissões;
RNF004 - Trilha de Auditoria

- **HISTÓRIA DE USUÁRIO 10:**

Título: HU10. Editar permissões de perfil.

Responsável: Nathalia G. Silva

Descrição estendida:
COMO gestor de uma área SOC, **QUERO** realizar edição de permissão de acesso nos perfis existente, **PARA** que eu possa alterar permissões de acesso quando necessário.

Critérios de aceite:

1. Ativar permissão
   DADO que o gestor de uma área SOC deseja ativar uma permissão, **QUANDO** o gestor selecionar a permissão que deseja ativar no perfil existente, **ENTÃO** o sistema deve ativar aquela permissão no perfil.

2. Desativar permissão
   DADO que o gestor de uma área SOC deseja desativar uma permissão, **QUANDO** o gestor selecionar a permissão que deseja desativar no perfil existente, **ENTÃO** o sistema deve desativar aquela permissão no perfil.

Dependência/notas técnicas:
RN02: Atribuição Obrigatória de Perfil de Acesso;
RN06: Controle de Acesso Baseado em Perfil.

Rastreabilidade (Documento de Visão):
F2. Manter perfil de permissões;
RNF004 - Trilha de Auditoria.

- **HISTÓRIA DE USUÁRIO 11:**

Título: HU11. Excluir perfil.

Responsável: Nathalia G. Silva

Descrição estendida:
COMO gestor de uma área SOC, **QUERO** realizar exclusão de um perfil existente, **PARA** que eu possa manter atualizado novos perfis com diferentes permissões.

Critérios de aceite:

1. Desvincular perfil com usuário.
   DADO que o gestor de uma área SOC deseja desvincular um perfil (DPO) de um usuário, **QUANDO** o gestor realizar a desvinculação, **ENTÃO** o sistema deve retirar aquele usuário da lista de perfil DPO..

2. Excluir Perfil com usuário vinculado.
   DADO que o gestor de uma área SOC deseja excluir um perfil com um usuário vinculado, **QUANDO** o gestor selecionar excluir perfil, **ENTÃO** o sistema deve apresentar mensagem erro, informando que ainda existe usuários vinculados.

3. Excluir Perfil sem usuário vinculado.
   DADO que o gestor de uma área SOC deseja excluir um perfil sem usuários vinculados, **QUANDO** o gestor selecionar excluir perfil, **ENTÃO** o sistema deve apresentar mensagem de exclusão bem-sucedida e excluir o perfil.

Dependência/notas técnicas:
RN02: Atribuição Obrigatória de Perfil de Acesso.

Rastreabilidade (Documento de Visão):
F2. Manter perfil de permissões;
RNF004 - Trilha de Auditoria.

- **HISTÓRIA DE USUÁRIO 12:**

Título: HU12. Acesso às Funcionalidades pelo Perfil

Responsável: Matheus Vinycius V. Batista

Descrição estendida:
COMO usuário cadastrado no sistema, **QUERO** realizar acesso apenas às funcionalidades e informações que são permitidas para o meu perfil de permissões, **PARA** que eu possa realizar meu trabalho de forma eficiente e segura, sem ter acesso a dados ou ações que não me dizem respeito, garantindo a integridade e a segurança do sistema.

Critérios de aceite:

1. Acessar funcionalidade não autorizada
   DADO que um usuário com um perfil específico (exemplo: Analista de Segurança - Nível 2) está logado no sistema, **QUANDO** ele tentar acessar uma funcionalidade não autorizada para o seu perfil (exemplo: Configurações de Administrador), **ENTÃO** o sistema deve bloquear o acesso e apresentar uma mensagem informativa: “Você não tem permissão para acessar esta funcionalidade”.

2. Acessar funcionalidade autorizada
   DADO que um usuário com um perfil específico (exemplo: analista compliance) está logado no sistema, **QUANDO** ele acessar uma área ou funcionalidade permitida para o seu perfil (exemplo: “Consultar histórico de incidentes”), **ENTÃO** o sistema deve permitir o acesso e exibir o histórico de incidentes.

3. Acessar funcionalidade por URL
   DADO que um usuário (exemplo: Analista de Segurança - Nível 1) tenta acessar uma funcionalidade (exemplo: “Editar permissões de perfil”) através de uma URL direta para a qual não tem permissão, **QUANDO** o usuário acessar a URL, **ENTÃO** o sistema deve direcioná-lo para uma página de acesso negado, impedindo a visualização ou interação com a funcionalidade.

4. Registrar acessos a funcionalidade não autorizado
   DADO que um usuário tenta realizar o acesso a uma funcionalidade não compatível com o seu perfil, **QUANDO** a tentativa de acesso for realizada, **ENTÃO** o sistema deve registrar as tentativas de acesso a funcionalidade não autorizadas para fins de auditoria.

Dependência/notas técnicas:
RN06: Controle de Acesso Baseado em Perfil

Rastreabilidade (Documento de Visão):
F3. Realizar controle lógico de acesso
RNF003 - Proteção de Dados Sensíveis
RNF004 - Trilha de Auditoria

- **HISTÓRIA DE USUÁRIO 13:**

Título: HU13. Realizar monitoramento em tempo real de logs de acesso

Responsável: Nathalia G. Silva

Descrição estendida:
COMO um usuário com perfil de gestor de SOC ou analista de segurança (nível 1, 2 e 3) ou especialista forense ou analista de risco ou DPO, **QUERO** monitorar tentativas de login (bem-sucedidas e falhas), usuários que fizeram login, endereços IP de origem, timestamps, comandos executados, **PARA** detectar tentativas de acesso não autorizado, escalonamento de privilégios e atividades suspeitas de usuários comprometidos.

Critérios de aceite:

1. Visualizar novos eventos
   DADO que estou logado com um perfil de gestor de SOC, analista de segurança (nível 1, 2 e 3), especialista forense, analista de risco e DPO, **QUANDO** eu acessar a funcionalidade de monitoramento de logs, **ENTÃO** devo visualizar novos eventos de log de acesso do sistema operacional, sendo exibidos na tela assim que ocorrem, sem a necessidade de atualizar a página manualmente.

2. Informações detalhadas de eventos
   DADO que estou monitorando os logs em tempo real, **QUANDO** um evento de acesso específico ocorrer (login bem-sucedido, falha de login, login de IP suspeito), **ENTÃO** o log correspondente deve exibir informações detalhadas como: Timestamp do evento (data e hora com precisão de segundos), nome de usuário (username), endereço IP de origem, método de acesso (SSH, login local, RDP), hostname do servidor, status do acesso (sucesso, falha, acesso negado) e Event ID (para Windows).

Dependência/notas técnicas:
RN19: Detecção Heurística de Eventos Suspeitos;
RN29: Normalização de Logs.

Rastreabilidade (Documento de Visão):
F4. Monitoramento em tempo real de logs de acesso;
RNF002 - Processamento em Tempo Real;
RNF003 - Proteção de Dados Sensíveis;
RNF014 - Integridade dos Dados de Log e Análises.

- **HISTÓRIA DE USUÁRIO 14:**

Título: HU14. Configurar ponto de monitoramento

Responsável: Nathalia G. Silva

Descrição estendida:
COMO um usuário com perfil de gestor de SOC e analista de segurança (nível 3), **QUERO** configurar um servidor da empresa como um ponto de monitoramento dedicado, especificando os parâmetros de coleta e centralização dos logs de acesso ao sistema operacional de outros servidores, **PARA** que eu possa consolidar os dados de log em um local seguro, facilitando a coleta e transporte.

Critérios de aceite:

1. Adicionar ponto de monitoramento
   DADO que estou logado com um perfil de gestor de SOC e analista de segurança (nível 3), **QUANDO** eu adicionar um ponto de monitoramento especificando endereço IP ou hostname, **ENTÃO** o sistema deve iniciar a coleta dos dados a partir do ponto de monitoramento adicionado.

2. Validando porta de recebimento
   DADO que estou logado com um perfil de gestor de SOC e analista de segurança (nível 3), **QUANDO** eu especificar a porta de escuta para o recebimento dos logs de acesso do sistema operacional, **ENTÃO** o sistema deve validar a conectividade, tentando detectar essa condição durante a configuração ou através de um teste de conectividade iniciado pelo administrador.

3. Conectado na porta de escuta
   DADO que estou logado com um perfil de gestor de SOC e analista de segurança (nível 3), tentando validar a conectividade da porta de escuta, **QUANDO** a conectividade for estabelecida, **ENTÃO** o status do ponto de monitoramento deve indicar, conectado, e receber os dados de logs através da porta especificada.

4. Falha de conectividade na porta de escuta
   DADO que estou logado com um perfil de gestor de SOC e analista de segurança (nível

3), tentando validar a conectividade da porta de escuta, **QUANDO** a porta de escuta estiver obstruída, **ENTÃO** o status do ponto de monitoramento deve indicar um problema de conectividade ou falha no recebimento de logs.

Dependência/notas técnicas:
RN27: Integridade dos Dados de Log e Análises;
RN28: Validação de Entrada de Dados.

Rastreabilidade (Documento de Visão):
F4. Monitoramento em tempo real de logs de acesso;
RNF004 - Trilha de Auditoria;
RNF018 - Validação de Entrada de Dados.

- **HISTÓRIA DE USUÁRIO 15:**

Título: HU15. Aplicar Filtros nos pontos de monitoramento

Responsável: Nathalia Gonçalves Silva

Descrição estendida:
COMO um usuário com perfil de gestor de SOC ou analista de segurança (nível 1, 2 e 3) ou especialista forense ou analista de risco ou DPO, **QUERO** aplicar filtros nos pontos de monitoramento, **PARA** que eu possa localizar rapidamente pontos de monitoramento específicos, analisar subconjuntos deles com base em critérios relevantes, como status, localização, tipo de sistema operacional e gerenciar de forma mais eficiente a infraestrutura de coleta de logs.

Critérios de aceite:

1. Filtrar por Status do Ponto de Monitoramento
   DADO que estou logado com um perfil de gestor de SOC ou analista de segurança (nível 1, 2 e 3) ou especialista forense ou analista de risco ou DPO, **QUANDO** seleciono um ou mais status ("Ativo", "Inativo", "Com Erro", "Degradado", "Manutenção") no filtro, **ENTÃO** o sistema deve exibir apenas os pontos de monitoramento que correspondem aos status selecionados.

2. Filtrar por Endereço IP ou Hostname do Servidor
   DADO que cada ponto de monitoramento é um servidor com um endereço de rede, **QUANDO** eu insiro um endereço IP (parcial ou completo) ou hostname no campo de filtro, **ENTÃO** a lista deve exibir apenas os pontos de monitoramento que correspondem ao endereço de rede especificado.

3. Filtrar por Características dos Sistemas Monitorados
   DADO que um ponto de monitoramento pode ser dedicado a certos tipos de sistemas operacionais ("Servidores Linux", "Desktops Windows"), **QUANDO** eu seleciono um tipo de sistema operacional ou grupo lógico no filtro, **ENTÃO** a lista deve exibir apenas os pontos de monitoramento responsáveis por coletar logs dessas fontes.

Dependência/notas técnicas:
RN27: Integridade dos Dados de Log e Análises.

Rastreabilidade (Documento de Visão):
F4. Monitoramento em tempo real de logs de acesso;
RNF018 - Validação de Entrada de Dados.

- **HISTÓRIA DE USUÁRIO 16:**

Título: HU16. Configurar alerta de atividades suspeitas

Responsável: Pedro Henrique O. Marques

Descrição estendida:
COMO um usuário com perfil de gestor de SOC ou analista de segurança (nível 1, 2 e 3) ou especialista forense ou analista de risco ou DPO, **QUERO** configurar regras de alerta personalizadas para serem notificadas sobre atividades suspeitas detectadas nos logs de acesso, **PARA** identificar proativamente potenciais ameaças à segurança, investigá-las rapidamente e tomar as medidas corretivas necessárias.

Critérios de aceite:

1. Criar regra de alerta
   DADO que desejo criar uma regra de alerta, **QUANDO** acesso a plataforma de monitoramento de segurança e selecione criar regra de alerta, **ENTÃO** o sistema deve solicitar um nome descritivo, uma descrição detalhada para a regra e atribuir um nível de severidade (baixo, médio, alto e crítico).

2. Regra com o mesmo nome descritivo
   DADO que uma regra foi criada com o mesmo nome de uma regra já existente, **QUANDO** eu criar a nova regra, **ENTÃO** o sistema deve apresentar mensagem informando que a regra já existe .

3. Regra com mais de um nível de severidade

DADO que uma regra foi criada e tentam atribuir mais de um nível de severidade, **QUANDO** eu seleciono dois níveis de severidade para a mesma regra, **ENTÃO** o sistema deve apresentar mensagem informando que a regra só pode ter um nível de severidade atribuído.

Dependência/notas técnicas:
RN07: Identificação de IP fora do horário permitido;
RN08: Detecção de Múltiplas Tentativas de Login com Erro;
RN09: Verificação de IP em Lista de Blacklist;
RN18: Definição de "Acessos Constantes" como Atividade Suspeita;
RN19: Detecção Heurística de Eventos Suspeitos.

Rastreabilidade (Documento de Visão):
F5. Emitir alerta para atividades suspeitas;
RNF004 - Trilha de Auditoria;
RNF013 - Configuração de Alerta Padrão;
RNF018 - Validação de Entrada de Dados.

- **HISTÓRIA DE USUÁRIO 17:**

Título: HU17. Notificação de alerta de atividade suspeita

Responsável: Pedro Henrique O. Marques

Descrição estendida:
COMO um usuário com perfil de gestor de SOC ou analista de segurança (nível 1, 2 e 3) ou especialista forense ou analista de risco ou DPO, **QUERO** receber notificações de alerta por e-mail e na tela do sistema argos, **PARA** identificar proativamente potenciais ameaças à segurança, investigá-las rapidamente e tomar as medidas corretivas necessárias.

Critérios de aceite:

1. Acionamento Automático da Notificação
   DADO que uma regra de alerta para atividade suspeita está configurada e ativa, **QUANDO** um evento de log de acesso ao sistema operacional corresponde aos critérios dessa regra, **ENTÃO** o sistema deve gerar e disparar automaticamente uma notificação de alerta.

4. Envio por e-mail
   DADO que uma regra de alerta para atividade suspeita está configurada e ativa,

QUANDO um evento de log de acesso ao sistema operacional corresponde aos critérios dessa regra, **ENTÃO** a notificação deve ser entregue no e-mail vinculado aos usuários com perfil gestor de SOC ou analista de segurança (nível 1, 2 e 3) ou analista de risco.

5. Envio de notificações repetidas:
   DADO que a mesma ocorrência de alerta aconteça continuamente, **QUANDO** for identificado a repetição da mesma ocorrência, **ENTÃO** o sistema deve entrar em estado de cooldown, impedindo o envio de notificações repetidas.

Dependência/notas técnicas:
RN07: Identificação de IP fora do horário permitido;
RN08: Detecção de Múltiplas Tentativas de Login com Erro;
RN09: Verificação de IP em Lista de Blacklist;
RN12: Classificação Automática da Gravidade de Incidentes;
RN18: Definição de "Acessos Constantes" como Atividade Suspeita;
RN23: Identificação de Incidentes com Dados Pessoais (PII).

Rastreabilidade (Documento de Visão):
F5. Emitir alerta para atividades suspeitas;
RNF002 - Processamento em Tempo Real.

- **HISTÓRIA DE USUÁRIO 18:**

Título: HU18. Ler alerta de atividades suspeitas

Responsável: Pedro Henrique O. Marques

Descrição estendida:
COMO um usuário com perfil de gestor de SOC ou analista de segurança (nível 1, 2 e 3) ou especialista forense ou analista de risco ou DPO, **QUERO** ler alertas de atividades suspeitas de forma clara, precisa e ágil, **PARA** identificar de forma rápida a estratégia a ser tomada.

Critérios de aceite:

1. Informações de alerta relevantes
   DADO que estou logado com com perfil de gestor de SOC ou analista de segurança (nível 1, 2 e 3) ou especialista forense ou analista de risco ou DPO, fazendo o monitoramento dos logs, **QUANDO** uma notificação de alerta é recebida, **ENTÃO** ela deve conter informações de Identificação da regra de alerta que foi acionada (Nome da Regra), data e hora exatas da detecção da atividade, tipo de atividade suspeita detectada ("Tentativa de acesso fora de hora", "Múltiplas falhas de login para o usuário X", "Acesso

detectado do IP suspeito Y.Y.Y.Y"), nível de severidade do alerta (baixa, média, alta, crítica), se o alerta for por email enviar link direto para a visualização detalhada do alerta.

2. Envio por e-mail
   DADO que uma regra de alerta para atividade suspeita está configurada e ativa, **QUANDO** um evento de log de acesso ao sistema operacional corresponde aos critérios dessa regra, **ENTÃO** a notificação deve ser entregue no e-mail vinculado aos usuários com perfil gestor de SOC, analista de segurança (nível 1, 2 e 3) e analista de risco.

Dependência/notas técnicas:
RN12: Classificação Automática da Gravidade de Incidentes

Rastreabilidade (Documento de Visão):
F5. Emitir alerta para atividades suspeitas;
RNF003 - Proteção de Dados Sensíveis

- **HISTÓRIA DE USUÁRIO 19:**

Título: HU19. Disponibilizar Relatório Diário de Atividades Suspeitas

Responsável: Pedro Henrique O. Marques

Descrição estendida:
COMO um usuário com perfil de analista de segurança(nível 1, 2 e 3), gestor de SOC, especialista forense, analista compliance, analista de risco, DPO, auditor interno, **QUERO** ter acesso fácil e regular a um relatório diário que consolide todas as atividades suspeitas detectadas nos logs de acesso ao sistema operacional da empresa durante as últimas 24 horas, **PARA** que eu possa revisar a postura de segurança do dia anterior de forma eficiente, identificar padrões ou tendências emergentes de ameaças, fornecer resumos concisos para a gestão executiva, e manter um registro documentado para fins de auditoria, conformidade e análise histórica.

Critérios de aceite:

1. Geração automática de relatório
   DADO que o sistema de monitoramento de segurança está operacional, **QUANDO** iniciar um dia às 00hrs, **ENTÃO** um relatório consolidado de atividades suspeitas, cobrindo o período completo das 24 horas anteriores, deve ser gerado automaticamente pelo sistema e disponibilizado nos Relatório Diário de Atividades Suspeitas.

2. Tratamento de dias sem atividades suspeitas
   DADO que em um determinado dia não houve nenhuma atividade suspeita detectada que correspondesse às regras de alerta configuradas, **QUANDO** o relatório diário para esse dia é gerado, **ENTÃO** ele deve indicar explicitamente que "Nenhuma atividade suspeita foi detectada durante o período".

Dependência/notas técnica:
RN11: Geração de Relatório Diário de Atividades Suspeitas

Rastreabilidade (Documento de Visão):
F6. Gerar relatório diário de atividades suspeitas;
RNF006 - Consultas Analíticas Complexas;
RNF014 - Integridade dos Dados de Log e Análises .

- **HISTÓRIA DE USUÁRIO 20:**

Título: HU20. Filtrar Relatório Diário de Atividades Suspeitas

Responsável: Pedro Henrique O. Marques

Descrição estendida:
COMO um usuário com perfil de analista de segurança(nível 1, 2 e 3), gestor de SOC, especialista forense, analista compliance, analista de risco, DPO, auditor interno, **QUERO** filtrar dados específicos (atividades de um determinado tipo, nível de severidade, usuários, endereços IP) do relatório de atividades suspeitas, **PARA** isolar, focar e analisar subconjuntos específicos de eventos, tornando minha revisão, investigação e identificação de padrões mais eficientes e direcionadas dentro do volume de dados do dia.

Critérios de aceite:

1. Filtrar por atividades suspeitas
   DADO que desejo isolar os casos de atividades suspeitas, **QUANDO** filtrar uma atividade do tipo falhas repetidas de login, acesso fora de hora, login de IP suspeito, **ENTÃO** o sistema deve exibir uma lista apenas com a atividade suspeita selecionada.

2. Filtrar por nível de severidade
   DADO que desejo isolar os casos por nível de severidade, **QUANDO** filtrar uma atividade por nível de severidade baixo, médio, alto ou crítico, **ENTÃO** o sistema deve

exibir uma lista apenas com as atividades correspondentes ao nível selecionado.

3. Filtrar por usuários
   DADO que desejo isolar as atividades suspeitas de um usuário, **QUANDO** filtrar as atividades de um usuário específico, **ENTÃO** o sistema deve exibir uma lista apenas com as atividades correspondentes ao usuário selecionado.

4. Filtrar por endereços IP
   DADO que desejo isolar as atividades suspeitas de um endereços IP, **QUANDO** filtrar as atividades de um endereços IP específico, **ENTÃO** o sistema deve exibir uma lista apenas com as atividades correspondentes ao endereços IP selecionado.

Dependência/notas técnicas:
RN11: Geração de Relatório Diário de Atividades Suspeitas;
RN12: Classificação Automática da Gravidade de Incidentes.

Rastreabilidade (Documento de Visão):
F6. Gerar relatório diário de atividades suspeitas;
RNF018 - Validação de Entrada de Dados.

- **HISTÓRIA DE USUÁRIO 21:**

Título: HU21. Exportar Relatório Diário de Atividades Suspeitas

Responsável: Pedro Henrique O. Marques

Descrição estendida:
COMO um usuário com perfil de analista de segurança (nível 1, 2 e 3), gestor de SOC, especialista forense, analista compliance, analista de risco, DPO, auditor interno, **QUERO** exportar o Relatório Diário de Atividades Suspeitas, tanto na sua visualização completa quanto na filtrada, em formatos de arquivo comuns (como PDF e CSV/Excel), **PARA** que eu possa realizar análises de dados offline, compartilhar as informações de forma estruturada com stakeholders que não possuem acesso direto ao sistema de monitoramento, arquivar os relatórios para fins de conformidade e auditoria de longo prazo, ou importar os dados.

Critérios de aceite:

1. Nomeação Padrão e Informativa dos Arquivos
   DADO que o processo de exportação é concluído e o download do arquivo é iniciado, **QUANDO** o arquivo é oferecido para download, **ENTÃO** ele deve ter um nome de

arquivo: "Relatorio_Atividades_Suspeitas_AAAA-MM-DD.[extensao_do_arquivo]".

2. Erros na Exportação
   DADO que estou logado com perfil de analista de segurança (nível 1, 2 e 3), gestor de SOC, especialista forense, analista compliance, analista de risco, DPO, auditor interno e desejo exportar um relatório, **QUANDO** um erro impede a geração ou o download do relatório (erro interno do servidor, permissões insuficientes, solicitação inválida), **ENTÃO** o sistema deve exibir uma mensagem de erro, explicando a natureza do problema e sugerindo próximos passos e quem contatar.

Dependência/notas técnicas:
RN11: Geração de Relatório Diário de Atividades Suspeitas;
RN012: Classificação Automática da Gravidade de Incidentes.

Rastreabilidade (Documento de Visão):
F6. Gerar relatório diário de atividades suspeitas;

RNF003 - Proteção de Dados Sensíveis;

- **HISTÓRIA DE USUÁRIO 22:**

Título: HU22. Visualizar Ameaças por Severidade em um Painel

Responsável: Maria Clara F. Rangel Marques

Descrição estendida:
COMO um usuário com perfil de analista de segurança(nível 1, 2 e 3), gestor de SOC, especialista forense, analista de risco, DPO, **QUERO** acessar um painel (dashboard) que exiba de forma visual e consolidada as ameaças (originadas de alertas de atividades suspeitas nos logs de acesso ao SO) agrupadas e quantificadas por seu nível de severidade (Baixo, Médio, Alto, Crítico), **PARA** que eu possa rapidamente identificar a distribuição e o volume das ameaças mais críticas, priorizar efetivamente as ações de resposta e investigação com base no risco, e obter uma compreensão imediata e panorâmica do estado atual da segurança da empresa.

Critérios de aceite:

1. Frequência de Atualização dos Dados
   DADO que estou logado com perfil de analista de segurança(nível 1, 2 e 3), gestor de SOC, especialista forense, analista de risco, DPO, **QUANDO** o painel está sendo exibido**,**

ENTÃO os dados de contagem de ameaças por severidade devem ser atualizados automaticamente a cada 5 minutos para refletir o estado mais recente possível..

2. Interatividade
   DADO que estou logado com perfil de analista de segurança(nível 1, 2 e 3), gestor de SOC, especialista forense, analista de risco, DPO, **QUANDO** em um determinado período não há ameaças ativas ou detectadas para um ou todos os níveis de severidade, **ENTÃO** o painel deve comunicar a ausência de ameaças.

Dependência/notas técnicas:
RN12: Classificação Automática da Gravidade de Incidentes.

Rastreabilidade (Documento de Visão):
F7. Visualizar ameaças por níveis de severidade;

RNF002 - Processamento em Tempo Real;
RNF005 - Personalização de Dashboards;
RNF030: Personalização de Dashboards por Papel.

- **HISTÓRIA DE USUÁRIO 23:**

Título: HU23. Filtrar de Lista de Incidentes por Nível de Severidade

Responsável: Maria Clara F. Rangel

Descrição estendida:
COMO um usuário com perfil de analista de segurança(nível 1, 2 e 3), gestor de SOC, especialista forense, analista de risco, DPO, **QUERO** filtrar a lista de ameaças/incidentes de segurança (originados de alertas de atividades suspeitas) por um ou mais níveis de severidade específicos, (Baixo, Médio, Alto, Crítico), **PARA** concentrar minha atenção e esforços de análise, investigação e resposta nas ocorrências mais importantes para minha tarefa atual, e encontrar rapidamente itens específicos.

Critérios de aceite:

1. Nenhum Resultado Encontrado
   DADO que apliquei um filtro de nível de severidade que não corresponde a nenhuma ameaça/incidente existente na lista, **QUANDO** a filtragem é concluída, **ENTÃO** o sistema deve exibir uma mensagem clara e informativa na área da lista, "Nenhuma ameaça/incidente encontrado para os níveis de severidade selecionados”.

Dependência/notas técnicas:
RN12: Classificação Automática da Gravidade de Incidentes.

Rastreabilidade (Documento de Visão):
F7. Visualizar ameaças por níveis de severidade;
RNF018 - Validação de Entrada de Dados.

- **HISTÓRIA DE USUÁRIO 24:**

Título: HU24. Buscar incidentes no histórico

Responsável: Maria Clara F. Rangel

Descrição estendida:
COMO um usuário com perfil de analista de segurança (nível 1, 2 e 3), gestor de SOC, especialista forense, analista compliance, DPO, auditor interno, **QUERO** buscar no histórico incidentes de segurança (alertas de atividades suspeitas que foram registrados, investigados e possivelmente encerrados/arquivados ao longo do tempo), **PARA** consultar o histórico completo de incidentes de segurança como alertas de atividades suspeitas que foram registrados, investigados e possivelmente encerrados/arquivados ao longo do tempo.

Critérios de aceite:

1. Ordenação dos Resultados da Busca
   DADO que a lista de resultados da busca é exibida, **QUANDO** preciso organizar os resultados para melhor análise**, ENTÃO** devo ter a opção de ordenar a lista de resultados por colunas principais, como Data do Incidente (mais recente ou mais antigo primeiro), Nível de Severidade (do maior para o menor ou vice-versa), ID do Incidente.

2. Opção de Filtro por categoria
   DADO que estou visualizando o histórico principal de incidentes de segurança na interface do sistema, **QUANDO** desejo realizar uma filtragem específica por data/hora, endereço IP, usuário, severidade, atividade suspeito**, ENTÃO** o sistema deve filtrar o histórico, exibindo apenas os dados solicitados.

3. Buscas Sem Resultados
   DADO que executei uma busca com critérios específicos, **QUANDO** não encontram

correspondência no histórico de incidentes, **ENTÃO** o sistema deve apresentar a mensagem : "Nenhum incidente encontrado no histórico."

Dependência/notas técnicas:
RN10: Retenção de Trilhas de Auditoria de Usuário;
RN13: Retenção de Logs por 6 Meses para Auditoria;
RN20: Conteúdo Mínimo para Consulta de Histórico de Incidentes.

Rastreabilidade (Documento de Visão):
F8. Consultar histórico de incidentes;
RNF004 - Trilha de Auditoria;
RNF006 - Consultas Analíticas Complexas;
RNF014 - Integridade dos Dados de Log e Análises;
RNF015 - Armazenamento de Dados Históricos;
RNF018 - Validação de Entrada de Dados.

- **HISTÓRIA DE USUÁRIO 25:**

Título: HU25. Análise Detalhada de Incidente do Histórico

Responsável: Maria Clara F. Rangel

Descrição estendida:
COMO um usuário com perfil de segurança (nível 1, 2 e 3), gestor de SOC, especialista forense, analista compliance, DPO, auditor interno, **QUERO** realizar análises detalhadas do histórico de incidentes, **PARA** isolar, focar e analisar subconjuntos específicos de eventos, tornando minha revisão, investigação e identificação de padrões mais eficientes e direcionadas dentro do volume de dados do dia.

Critérios de aceite:

1. Comparação de Períodos
   DADO que preciso entender a performance em relação a períodos anteriores, **QUANDO** analiso a evolução do histórico**, ENTÃO** o sistema deve comparar a tendência de um período selecionado com um período anterior equivalente (comparar "Este Mês" com "Mês Passado", ou "Este Trimestre" com "Mesmo Trimestre do Ano Anterior").

2. Exportação da Visualização e/ou Dados
   DADO que preciso utilizar a informação em relatórios externos ou para análises mais profundas, **QUANDO** visualizo o gráfico de evolução do volume de incidentes**, ENTÃO**

devo ter opções claras para exportar a visualização gráfica como uma imagem (PNG, JPG, SVG) ou os dados agregados que formam o gráfico (em formato CSV ou Excel).

3. Períodos Sem Incidentes
   DADO que podem existir intervalos de tempo nos quais nenhum incidente foi registrado, **QUANDO** o gráfico do histórico é exibido**, ENTÃO** esses períodos devem ser representados com uma mensagem "Nenhum incidente identificado nesse período".

Dependência/notas técnicas:
RN10: Retenção de Trilhas de Auditoria de Usuário;
RN13: Retenção de Logs por 6 Meses para Auditoria;
RN20: Conteúdo Mínimo para Consulta de Histórico de Incidentes.

Rastreabilidade (Documento de Visão):
F8. Consultar histórico de incidentes;

RNF006 - Consultas Analíticas Complexas;
RNF014 - Integridade dos Dados de Log e Análises;
RNF015 - Armazenamento de Dados Históricos.

- **HISTÓRIA DE USUÁRIO 26:**

Título: HU26. Acompanhar Evolução do Volume de Incidentes

Responsável: Gustavo Horeste S. Barros

Descrição estendida:
COMO um usuário com perfil de analista de segurança (nível 1, 2 e 3), gestor de SOC, especialista forense, analista compliance, DPO, auditor interno, **QUERO** acessar uma visualização analítica, que demonstra a evolução do volume total de incidentes de segurança (detectados/reportados) ao longo do tempo, **PARA** que eu possa identificar tendências de aumento, diminuição ou sazonalidade na ocorrência de incidentes, avaliar a eficácia das contramedidas e políticas de segurança implementadas.

Critérios de aceite:

1. Comparação de Períodos
   DADO que preciso entender a performance em relação a períodos anteriores, **QUANDO** analiso a evolução do volume de incidentes**, ENTÃO** o sistema deve comparar as tendência de um período selecionado com um período anterior equivalente (comparar

"Este Mês" com "Mês Passado", ou "Este Trimestre" com "Mesmo Trimestre do Ano Anterior").

2. Selecionar período de análise
   DADO que preciso entender a performance em relação a períodos anteriores, **QUANDO** analiso a evolução do volume de incidentes**, ENTÃO** o sistema deve selecionar um período de tempo específico ("Últimos 7 dias", "Últimos 30 dias", "Últimos 90 dias", "Último Ano", "Ano Atual", e um seletor de intervalo de datas personalizado "De" e "Até").

3. Exportação da Visualização e/ou Dados
   DADO que preciso utilizar a informação em relatórios externos, **QUANDO** visualizo a evolução do volume de incidentes**, ENTÃO** o sistema deve exportar os dados agregados que formam o gráfico (em formato CSV ou Excel).

4. Períodos Sem Incidentes
   DADO que podem existir intervalos de tempo nos quais nenhum incidente foi registrado, **QUANDO** o gráfico do histórico é exibido**, ENTÃO** esses períodos devem ser representados visualmente com um volume de "0".

Dependência/notas técnicas:
RN21: Tipos de Insights de Tendências sobre Incidentes.

Rastreabilidade (Documento de Visão):
F9. Gerar insights de tendências sobre incidentes;

RNF006 - Consultas Analíticas Complexas;
RNF015 - Armazenamento de Dados Históricos.

- **HISTÓRIA DE USUÁRIO 27:**

Título: HU27. Identificar os Tipos de Incidentes Recorrentes

Responsável: Gustavo Horeste S. Barros

Descrição estendida:
COMO um usuário com perfil de analista de segurança (nível 1, 2 e 3), gestor de SOC, especialista forense, analista compliance, DPO, auditor interno, **QUERO** analisar quais são os tipos de incidentes (Ataques de Força Bruta, Password Spraying, Acesso de Localizações Geográficas Suspeitas/Incomuns, Tentativas de Login Fora do Horário Comercial, Uso de Credenciais Vazadas/Comprometidas, Logins Bem-Sucedidos Após Múltiplas Falhas, Padrões de

Login Anormais para Usuários Legítimos, Violações de Política de Segurança, Reconhecimento e Movimentação Lateral, Logins Interativos com Contas de Serviço) que ocorrem com maior frequência ou recorrência em um período de tempo selecionável, **PARA** direcionar esforços para a investigação aprofundada das causas raízes desses problemas, priorizar a implementação de soluções preventivas e corretivas mais eficazes, otimizar os playbooks de resposta para esses cenários comuns.

Critérios de aceite:

1. Seleção do Período de Análise
   DADO que estou iniciando uma análise para identificar incidentes recorrentes, **QUANDO** configuro os parâmetros da análise**, ENTÃO** devo poder selecionar o período de tempo sobre o qual a análise de recorrência será realizada, utilizando opções predefinidas como "Últimos 30 dias", "Último Trimestre", "Último Semestre", "Último Ano", ou definindo um intervalo de datas personalizado "De" e "Até".

2. Fonte de Dados e Critério de Agrupamento
   DADO que desejo realizar uma análise de recorrência, **QUANDO** os resultados da análise são processados**, ENTÃO** o sistema deve utilizar o histórico de incidentes de segurança registrados, agrupando e contando as ocorrências.

3. Detalhamento (Drill-Down) para Incidentes Individuais
   DADO que a lista ou gráfico de tipos de incidentes recorrentes é exibida com suas respectivas frequências, **QUANDO** seleciono um tipo de incidente específico nessa visualização (exemplo: "Password Spraying" que indica 50 ocorrências)**, ENTÃO** devo ser capaz de visualizar uma lista detalhada de todos os 50 incidentes individuais classificados como "Password Spraying" que ocorreram dentro do período de análise originalmente selecionado.

Dependência/notas técnicas:
RN21: Tipos de Insights de Tendências sobre Incidentes.

Rastreabilidade (Documento de Visão):
F9. Gerar insights de tendências sobre incidentes;

RNF006 - Consultas Analíticas Complexas;
RNF015 - Armazenamento de Dados Históricos.

- **HISTÓRIA DE USUÁRIO 28:**

Título: HU28. Disponibilizar relatório de tendências sobre incidentes

Responsável: Matheus Vinycius V. Batista

Descrição estendida:
COMO um usuário com perfil de analista de segurança (nível 1, 2 e 3), gestor de SOC, especialista forense, analista compliance, analista de risco, DPO, auditor interno, **QUERO** ter acesso a um relatório de tendências sobre incidentes (Tentativas de Acesso Não Autorizado, Contas Comprometidas e Atividade Interna Maliciosa, Violações de Política de Segurança, Reconhecimento e Movimentação Lateral, Uso Indevido de Contas), **PARA** que eu possa analisar a evolução da postura de segurança, identificar padrões de ameaças emergentes ou em declínio, comunicar esses insights de forma documentada para a alta gestão, embasar o planejamento estratégico e orçamentário de segurança, e fornecer evidências para processos de auditoria e conformidade.

Critérios de aceite:

1. Configuração Detalhada dos Parâmetros do Relatório
   DADO que inicio o processo de geração de um relatório de tendências de incidentes, **QUANDO** define os parâmetros para a elaboração do relatório, **ENTÃO** devo ser capaz de configurar Período de Análise, Tendência da evolução do volume total de incidentes, Tendência da evolução do volume de incidentes segmentado por nível de severidade, Tendência da evolução do volume de incidentes segmentado por tipo.

2. Tratamento de Períodos com Dados Escassos ou Ausentes
   DADO o período de análise selecionado pode incluir intervalos de tempo com um volume muito baixo ou nenhum incidente registrado para certas categorias ou no geral, **QUANDO** o relatório de tendências é gerado, **ENTÃO** as visualizações gráficas devem representar esses períodos, mostrando valores zero nos gráficos, linhas contínuas no eixo zero e o relatório deve incluir notas explicativas e ressalvas se a escassez de dados em certos pontos puder afetar a significância estatística ou a interpretação de algumas tendências.

Dependência/notas técnicas:
RN13: Retenção de Logs por 6 Meses para Auditoria;
RN22: Conteúdo do Relatório de Tendências sobre Incidentes.

Rastreabilidade (Documento de Visão):
F10. Gerar relatório de tendências sobre incidentes;

RNF006 - Consultas Analíticas Complexas;

RNF015 - Armazenamento de Dados Históricos;
RNF014 - Integridade dos Dados de Log e Análises.

- **HISTÓRIA DE USUÁRIO 29:**

Título: HU29. Exportar relatório de tendências sobre incidentes

Responsável: Matheus Vinycius V. Batista

Descrição estendida:
COMO um usuário com perfil de analista de segurança (nível 1, 2 e 3), gestor de SOC, especialista forense, analista compliance, analista de risco, DPO, auditor interno, **QUERO** exportar o Relatório Diário de Atividades Suspeitas, tanto na sua visualização completa quanto na filtrada, em formatos de arquivo comuns (como PDF e CSV/Excel), **PARA** que eu possa realizar análises de dados offline, compartilhar as informações de forma estruturada com stakeholders que não possuem acesso direto ao sistema de monitoramento, arquivar os relatórios para fins de conformidade e auditoria de longo prazo, ou importar os dados.

Critérios de aceite:

1. Nomeação Padrão e Informativa dos Arquivos
   DADO que o processo de exportação é concluído e o download do arquivo é iniciado, **QUANDO** o arquivo é oferecido para download, **ENTÃO** ele deve ter um nome padrão "Relatorio_Tendencias_Sobre_Incidentes_AAAA-MM-DD.[extensao_do_arquivo]".

2. Erros na Exportação
   DADO que pode ocorrer um problema durante a tentativa de exportação (erro interno do servidor, permissões insuficientes, solicitação inválida), **QUANDO** um erro impede a geração ou o download do relatório, **ENTÃO** o sistema deve exibir uma mensagem de erro, explicando a natureza do problema e sugerindo próximos passos e quem contatar.

Dependência/notas técnicas:
RN21: Tipos de Insights de Tendências sobre Incidentes;
RN22: Conteúdo do Relatório de Tendências sobre Incidentes.

Rastreabilidade (Documento de Visão):
F10. Gerar relatório de tendências sobre incidentes;

RNF003 - Proteção de Dados Sensíveis;

- **HISTÓRIA DE USUÁRIO 30:**

Título: HU30. Disponibilizar relatório de incidentes com dados pessoais

Responsável: Gustavo Horeste S. Barros

Descrição estendida:
COMO um usuário com perfil de analista de segurança (nível 1, 2 e 3), gestor de SOC, especialista forense, analista compliance, analista de risco, DPO, auditor interno, **QUERO** ter acesso a um relatório de tendências sobre incidentes com dados pessoais (Violação de Confidencialidade, Violação de Integridade, Violação de Disponibilidade, Tratamento Indevido ou Não Conforme), **PARA** que eu possa analisar a evolução da postura de segurança, identificar padrões de ameaças emergentes ou em declínio, comunicar esses insights documentada para a alta gestão e outras partes interessadas, embasar o planejamento estratégico e orçamentário de segurança, e fornecer evidências para processos de auditoria e conformidade.

Critérios de aceite:

1. Configuração Detalhada dos Parâmetros do Relatório
   DADO que inicio o processo de geração de um relatório de tendências de incidentes com dados pessoais, **QUANDO** define os parâmetros para a elaboração do relatório, **ENTÃO** devo ser capaz de configurar Período de Análise, Tendência da evolução do volume total de incidentes, Tendência da evolução do volume de incidentes segmentado por nível de severidade, Tendência da evolução do volume de incidentes segmentado por tipo.

2. Tratamento de Períodos com Dados Escassos ou Ausentes
   DADO que o período de análise selecionado pode incluir intervalos de tempo com um volume muito baixo ou nenhum incidente registrado para certas categorias ou no geral, **QUANDO** o relatório de tendências é gerado, **ENTÃO** as visualizações gráficas devem representar esses períodos de forma apropriada (mostrando valores zero nos gráficos, linhas contínuas no eixo zero) e o relatório pode incluir notas explicativas e ressalvas se a escassez de dados em certos pontos puder afetar a significância estatística e a interpretação de algumas tendências.

Dependência/notas técnicas:
RN23: Identificação de Incidentes com Dados Pessoais (PII);
RN24: Conteúdo do Relatório de Incidentes com Dados Pessoais.

Rastreabilidade (Documento de Visão):
F11. Gerar relatório sobre incidentes com dados pessoais;

RNF003 - Proteção de Dados Sensíveis;

- **HISTÓRIA DE USUÁRIO 31:**

Título: HU31. Exportar relatório de incidentes com dados pessoais

Responsável: Gustavo Horeste S. Barros

Descrição estendida:
COMO um usuário com perfil de analista de segurança(nível 1, 2 e 3), gestor de SOC, especialista forense, analista compliance, analista de risco, DPO, auditor interno, **QUERO** exportar o relatório de incidentes com dados pessoais, tanto na sua visualização completa quanto na filtrada, em formatos de arquivo comuns (como PDF e CSV/Excel), **PARA** que eu possa realizar análises de dados offline, compartilhar as informações de forma estruturada com stakeholders que não possuem acesso direto ao sistema de monitoramento, arquivar os relatórios para fins de conformidade e auditoria de longo prazo, ou importar os dados.

Critérios de aceite:

1. Nomeação Padrão e Informativa dos Arquivos
   DADO que o processo de exportação é concluído e o download do arquivo é iniciado, **QUANDO** o arquivo é oferecido para download, **ENTÃO** ele deve ter um nome de arquivo padrão: "Relatorio_Incidentes_DPO_AAAA-MM-DD.[extensao_do_arquivo]".

2. Erros na Exportação
   DADO que pode ocorrer um problema durante a tentativa de exportação (erro interno do servidor, permissões insuficientes, solicitação inválida), **QUANDO** um erro impede a geração ou o download do relatório, **ENTÃO** o sistema deve exibir uma mensagem de erro clara na interface, explicando a natureza do problema e sugerindo próximos passos ou quem contatar.

Dependência/notas técnicas:
RN23: Identificação de Incidentes com Dados Pessoais (PII);
RN24: Conteúdo do Relatório de Incidentes com Dados Pessoais.

Rastreabilidade (Documento de Visão):
F11. Gerar relatório sobre incidentes com dados pessoais;

RNF003 - Proteção de Dados Sensíveis;

- **HISTÓRIA DE USUÁRIO 32:**

Título: HU32. Disponibilizar relatório de Atividade de Login Bem-Sucedido

Responsável: Maria Clara F. Rangel

Descrição estendida:
COMO um usuário com perfil de analista de segurança (nível 1, 2 e 3), gestor de SOC, especialista forense, analista compliance, analista de risco, DPO, auditor interno, **QUERO** ter acesso a um relatório de Atividade de Login Bem-Sucedido, **PARA** que eu possa estabelecer uma Linha de Base (Baseline) e detectar anomalias, analisar o comportamento de usuário comunicar esses insights documentado para a alta gestão, embasar o planejamento estratégico e orçamentário de segurança, e fornecer evidências para processos de auditoria e conformidade.

Critérios de aceite:

1. Configuração Detalhada dos Parâmetros do Relatório
   DADO que inicio o processo de geração de um relatório de Atividade de Login Bem-Sucedido, **QUANDO** define os parâmetros para a elaboração do relatório, **ENTÃO** devo ser capaz de configurar Período de Análise.

2. Tratamento de Períodos com Dados Escassos ou Ausentes
   DADO o período de análise selecionado pode incluir intervalos de tempo com um volume muito baixo ou nenhum incidente registrado para certas categorias ou no geral, **QUANDO** o relatório de tendências é gerado, **ENTÃO** as visualizações gráficas devem representar esses períodos de forma apropriada (mostrando valores zero nos gráficos, linhas contínuas no eixo zero) e o relatório pode incluir notas explicativas e ressalvas se a escassez de dados em certos pontos puder afetar a significância estatística ou a interpretação de algumas tendências.

Dependência/notas técnicas:
RN25: Conteúdo do Relatório de Atividade de Login Bem-Sucedido.

Rastreabilidade (Documento de Visão):
F12. Gerar relatório de Atividade de Login Bem-Sucedido;

RNF006 - Consultas Analíticas Complexas;
RNF014 - Integridade dos Dados de Log e Análises;
RNF015 - Armazenamento de Dados Históricos.

- **HISTÓRIA DE USUÁRIO 33:**

Título: HU33. Exportar relatório de Atividade de Login Bem-Sucedido

Responsável: Maria Clara F. Rangel

Descrição estendida:
COMO um usuário com perfil de analista de segurança (nível 1, 2 e 3), gestor de SOC, especialista forense, analista compliance, analista de risco, DPO, auditor interno, **QUERO** exportar o Relatório de Atividade de Login Bem-Sucedido, tanto na sua visualização completa quanto na filtrada, em formatos de arquivo comuns (como PDF e CSV/Excel), **PARA** que eu possa realizar análises de dados offline, compartilhar as informações de forma estruturada com stakeholders que não possuem acesso direto ao sistema de monitoramento, arquivar os relatórios para fins de conformidade e auditoria de longo prazo, ou importar os dados.

Critérios de aceite:

1. Nomeação Padrão e Informativa dos Arquivos
   DADO que o processo de exportação é concluído e o download do arquivo é iniciado, **QUANDO** o arquivo é oferecido para download, **ENTÃO** ele deve ter um nome de arquivo:"Relatorio_Atividades_Login_BemSucedido_AAAA-MM-DD.[extensao_do_arquivo]".

2. Erros na Exportação
   DADO que pode ocorrer um problema durante a tentativa de exportação (erro interno do servidor, permissões insuficientes, solicitação inválida), **QUANDO** um erro impede a geração ou o download do relatório, **ENTÃO** o sistema deve exibir uma mensagem de erro, explicando a natureza do problema e sugerindo próximos passos ou quem contatar.

Dependência/notas técnicas:
RN25: Conteúdo do Relatório de Atividade de Login Bem-Sucedido.

Rastreabilidade (Documento de Visão):
F12. Gerar relatório de Atividade de Login Bem-Sucedido:

RNF006 - Consultas Analíticas Complexas;
RNF014 - Integridade dos Dados de Log e Análises;
RNF015 - Armazenamento de Dados Históricos.

- **HISTÓRIA DE USUÁRIO 34:**

Título: HU34. Disponibilizar relatório de Tentativas de Login Falhadas

Responsável: Gustavo Horeste S. Barros

Descrição estendida:
COMO um usuário com perfil de analista de segurança (nível 1, 2 e 3), gestor de SOC, especialista forense, analista compliance, analista de risco, DPO, auditor interno, **QUERO** ter acesso a um relatório de Tentativas de Login Falhadas, **PARA** que eu possa analisar profundamente a evolução da postura de segurança, identificar padrões de ameaças emergentes ou em declínio, comunicar esses insights de forma documentada para a alta gestão, embasar o planejamento estratégico e orçamentário de segurança, e fornecer evidências para processos de auditoria e conformidade.

Critérios de aceite:

1. Configuração Detalhada dos Parâmetros do Relatório
   DADO que inicio o processo de geração de um relatório de Tentativas de Login Falhadas, **QUANDO** define os parâmetros para a elaboração do relatório, **ENTÃO** devo ser capaz de configurar Período de Análise, usuários e IP.

2. Tratamento de Períodos com Dados Escassos ou Ausentes
   DADO o período de análise selecionado pode incluir intervalos de tempo com um volume muito baixo ou nenhum incidente registrado para certas categorias ou no geral, **QUANDO** o relatório é gerado, **ENTÃO** as visualizações gráficas devem representar esses períodos de forma apropriada (mostrando valores zero nos gráficos, linhas contínuas no eixo zero) e o relatório pode incluir notas explicativas e ressalvas se a escassez de dados em certos pontos puder afetar a significância estatística ou a interpretação de algumas tendências.

Dependência/notas técnicas:
RN08: Detecção de Múltiplas Tentativas de Login com Erro
RN26: Conteúdo do Relatório de Tentativas de Login Falhadas

Rastreabilidade (Documento de Visão):
F13. Relatório de Tentativas de Login Falhadas

RNF006 - Consultas Analíticas Complexas;
RNF014 - Integridade dos Dados de Log e Análises;

RNF015 - Armazenamento de Dados Históricos.

- **HISTÓRIA DE USUÁRIO 35:**

Título: HU35. Exportar relatório de Atividade de Login Falhada

Responsável: Gustavo Horeste S. Barros

Descrição estendida:
COMO um usuário com perfil de analista de segurança (nível 1, 2 e 3), gestor de SOC, especialista forense, analista compliance, analista de risco, DPO, auditor interno, **QUERO** exportar o Relatório de Atividade de Login Falhada, tanto na sua visualização completa quanto na filtrada, em formatos de arquivo comuns (como PDF e CSV/Excel), **PARA** que eu possa realizar análises de dados offline, compartilhar as informações de forma estruturada com stakeholders que não possuem acesso direto ao sistema de monitoramento, arquivar os relatórios para fins de conformidade e auditoria de longo prazo, ou importar os dados.

Critérios de aceite:

1. Nomeação Padrão e Informativa dos Arquivos
   DADO que o processo de exportação é concluído e o download do arquivo é iniciado, **QUANDO** o arquivo é oferecido para download, **ENTÃO** ele deve ter um nome de arquivo:"Relatorio_Atividade_de_Login_Falhadas_AAAA-MM-DD.[extensao_do_arquivo]".

2. Erros na Exportação
   DADO que pode ocorrer um problema durante a tentativa de exportação (erro interno do servidor, permissões insuficientes, solicitação inválida), **QUANDO** um erro impede a geração ou o download do relatório, **ENTÃO** o sistema deve exibir uma mensagem de erro, explicando a natureza do problema e sugerindo próximos passos ou quem contatar.

Dependência/notas técnicas:
RN08: Detecção de Múltiplas Tentativas de Login com Erro
RN26: Conteúdo do Relatório de Tentativas de Login Falhadas

Rastreabilidade (Documento de Visão):
F13. Relatório de Tentativas de Login Falhadas
RNF003 - Proteção de Dados Sensíveis

4. Lista de requisitos não funcionais

- **RNF001 – Latência de Visualização de Dados**

Descrição: O sistema deve apresentar visualizações de dados na interface (dashboards, gráficos) com uma latência inferior a 2 segundos para 95% das interações, quando o sistema estiver processando o volume médio de logs esperado.

Prioridade: Alta

Classificação ISO/IEC 25010: Desempenho.

Formulação SMART:

Específico: Todas as visualizações de dados interativos (gráficos, tabelas, dashboards) na interface do usuário devem carregar e ser renderizadas em menos de 2 segundos após a solicitação do usuário.

Mensurável: A latência será medida em segundos, do clique do usuário ao momento em que a visualização está completamente visível e interativa. O objetivo é < 2 segundos.

Alcançável: Viável com otimizações de front-end, consultas eficientes ao back-end e, se necessário, mecanismos de cache.

Relevante: Essencial para uma experiência de usuário fluida e responsiva, permitindo análises ágeis.

Temporizador: Deve ser atendido em todas as fases operacionais do sistema, a partir da primeira versão em produção.

Método de Verificação: Teste de Desempenho de UI, Teste de Carga.

Critérios de Aceitação: Relatório de teste de carga demonstrando que o 95º percentil do tempo de renderização das visualizações é ≤ 2 segundos sob a carga especificada.

Impacto no Plano de Testes: Exige testes de desempenho rigorosos da UI, incluindo testes de carga simulando múltiplos usuários acessando dashboards. Profiling de scripts de front-end para identificar gargalos.

Impacto na Arquitetura: Necessita de um framework de front-end responsivo, estratégias otimizadas de busca de dados (paginação, lazy loading, chamadas de API otimizadas), mecanismos de cache em vários níveis (navegador, CDN, lado do servidor) e processamento

eficiente de consultas no back-end para dados de visualização.

- **RNF002 – Processamento em Tempo Real**

Descrição: O sistema deve processar análises de logs em tempo real com uma latência inferior a 5 segundos desde a ingestão do log até a disponibilização da análise para alerta ou visualização, para 90% dos eventos, lidando com um volume de até 1 milhão de registros de log por hora.

Prioridade: Alta

Classificação ISO/IEC 25010: Desempenho.

Formulação SMART:

Específico: O sistema deve processar e apresentar os resultados de análises de logs em tempo real com uma latência inferior a 5 segundos, para um volume de entrada de até 1 milhão de novos registros de log.

Mensurável: A latência será medida em segundos, desde a ingestão do último registro de um lote de 1 milhão até a disponibilização do resultado da análise (alerta ou atualização de dashboard). O objetivo é < 5 segundos.

Alcançável: Requer um pipeline de processamento de dados otimizado e infraestrutura escalável.

Relevante: Fundamental para a detecção rápida de eventos suspeitos e resposta ágil, conforme objetivo do sistema.

Temporizado: Válido durante a operação contínua do sistema em ambiente de produção.

Método de Verificação: Teste de Desempenho, Teste de Volume.

Critérios de Aceitação: Para um conjunto de dados de 1 milhão de registros, 95% das tarefas de análise em tempo real devem ser concluídas dentro de 5 segundos.

Impacto no Plano de Testes: Testes de volume com conjuntos de dados de até 1M de registros, medindo a latência de ponta a ponta desde a ingestão até o alerta/exibição. Testes de estresse do motor de análise.

Impacto na Arquitetura: Demanda um pipeline de ingestão de dados de alta capacidade, um motor de processamento de stream eficiente ou processamento em lote otimizado para resultados quase em tempo real, banco de dados performático para armazenar e consultar resultados intermediários ou regras, e potencialmente capacidades de processamento distribuído.

- **RNF003 – Proteção de Dados Sensíveis**

Descrição: O sistema deve proteger todos os dados sensíveis, incluindo credenciais de acesso, informações de clientes e logs armazenados, contra acesso e modificação não autorizados, utilizando criptografia AES-256 para dados em repouso e TLS 1.2 para dados em trânsito, e controles de acesso baseados em papéis (RBAC) implementados em todas as interfaces de acesso aos dados.

Classificação ISO/IEC 25010: Segurança.

Prioridade: Alta

Formulação SMART:

Específico: Implementar criptografia (AES-256) para dados sensíveis em repouso (como credenciais de acesso e informações do cliente) e controles de acesso baseados em papéis (RBAC) para prevenir acesso ou modificação não autorizados desses dados.

Mensurável: Verificação dos algoritmos de criptografia (AES-256) e das políticas RBAC. Taxas de sucesso/falha em testes de penetração.

Alcançável: Práticas de segurança padrão, factíveis com tecnologias atuais.

Relevante: Essencial para proteger os dados do usuário, manter a confiança e atender a requisitos legais (LGPD).

Temporizado: Implementado até a primeira versão de produção e mantido ao longo do ciclo de vida do sistema.

Método de Verificação: Auditoria de Código, Teste de Penetração, Revisão de Configuração de Segurança.

Critérios de Aceitação: Todos os campos de dados sensíveis (conforme definido no documento de classificação de dados) são criptografados. As regras RBAC são aplicadas, impedindo usuários de acessar ou modificar dados fora de seus papéis definidos, confirmado por 0 vulnerabilidades críticas/altas relacionadas ao controle de acesso no relatório do teste de penetração.

Impacto no Plano de Testes: Testes de segurança, incluindo testes de penetração focados na exposição de dados e bypass de controle de acesso. Revisões de código para implementação de criptografia e lógica de controle de acesso.

Impacto na Arquitetura: Requer um componente robusto de Gerenciamento de Identidade e Acesso (IAM), implementação de criptografia (AES-256) para dados em repouso, para bancos

de dados, arquivos de configuração sensíveis e em trânsito (TLS/SSL). Design seguro de API (autenticação, autorização). Estratégia de gerenciamento de chaves.

- **RNF004 – Trilha de Auditoria**

Descrição: O sistema deve registrar as principais atividades dos usuários (logins bem-sucedidos e falhas, acessos a dados sensíveis, alterações de configuração crítica, criação/modificação de regras de alerta) em uma trilha de auditoria segura e imutável. Esses registros devem ser retidos por um período mínimo de 1 ano e ser acessíveis apenas por administradores do sistema para fins de investigação.

Classificação ISO/IEC 25010: Segurança.

Prioridade: Média

Formulação SMART:

Específico: Registrar todas as atividades principais dos usuários, como logins (sucesso/falha), acessos a dados sensíveis e alterações de configuração. Esta trilha de auditoria deve ser retida de forma segura por no mínimo 1 ano.

Mensurável: Presença e completude das entradas de log de auditoria para as atividades especificadas. Período de retenção verificado.

Alcançável: Viável com frameworks de logging padrão e políticas de armazenamento.

Relevante: Suporta investigações de segurança, responsabilização e conformidade.

Temporizado: Logging de auditoria ativo desde a primeira versão de produção. Dados retidos por 1 ano de forma contínua.

Método de Verificação: Inspeção de Logs, Teste Funcional (desencadeando eventos auditáveis e verificando os logs).

Critérios de Aceitação: Todas as atividades críticas de usuário definidas são registradas com timestamp, ID do usuário, tipo de atividade e resultado. Demonstra-se que os logs são à prova de adulteração e recuperáveis pelo período de 1 ano.

Impacto no Plano de Testes: Teste para verificar se todas as atividades especificadas (logins, acessos a dados sensíveis, alterações de configuração) são logadas de forma correta, completa e com os metadados necessários, testes para verificar a integridade e a não repudiação dos logs de auditoria (tamper-evidence), testes de recuperação e consulta dos logs de auditoria durante todo o período de retenção de 1 ano, teste de desempenho do mecanismo de logging sob carga.

Impacto na Arquitetura: Sistema de logging centralizado e seguro, armazenamento com capacidade suficiente para reter logs por 1 ano, com políticas de rotação e arquivamento, mecanismos para garantir a integridade dos logs (armazenamento WORM, hashing), APIs para consulta dos logs de auditoria por pessoal autorizado.

- **RNF005 – Personalização de Dashboards**

Descrição: O sistema deve permitir que usuários com papéis de “analista de segurança (nível 1, 2 e 3) ou especialista forense ou analista de risco ou DPO”, personalizem a disposição de widgets e visualizações nos dashboards. Essas configurações personalizadas devem ser salvas por usuário e persistir entre sessões, sendo carregadas automaticamente no próximo acesso.

Classificação ISO/IEC 25010: Usabilidade.

Prioridade: Baixa

Formulação SMART:

Específico: Usuários com os papéis “analista de segurança (nível 1, 2 e 3) ou especialista forense ou analista de risco ou DPO” devem poder personalizar o layout de seus dashboards adicionando, removendo ou rearranjando widgets e visualizações, e salvar essas configurações personalizadas, que devem persistir entre sessões.

Mensurável: Sucesso na personalização e salvamento/carregamento de pelo menos 3 configurações de dashboard diferentes por usuário de teste com os papéis especificados.

Alcançável: Funcionalidade comum em aplicações baseadas em dashboards.

Relevante: Aumenta a satisfação e eficiência do usuário ao adaptar a interface às necessidades individuais.

Temporizado: Implementado até a versão final do produto.

Método de Verificação: Teste de Usabilidade, Demonstração.

Critérios de Aceitação: Usuários nos papéis especificados conseguem realizar com sucesso tarefas de personalização (adicionar, remover, rearranjar widgets) e salvar/carregar seus layouts. Layouts salvos são corretamente restaurados em logins subsequentes. 90% dos usuários de teste conseguem completar estas tarefas sem assistência em menos de 5 minutos.

Impacto no Plano de Testes: Testes de usabilidade focados na facilidade e interatividade da personalização de dashboards, testes funcionais para verificar o salvamento e carregamento corretos das configurações personalizadas entre sessões e para os diferentes papéis, casos de teste

cobrindo a adição, remoção e reorganização de diversos tipos de widgets.

Impacto na Arquitetura: Arquitetura de front-end que suporte layouts dinâmicos e personalizáveis (sistemas de grid, componentes reutilizáveis), mecanismo no back-end para armazenar e recuperar configurações de dashboard específicas do usuário ou do papel, APIs para gerenciar essas configurações personalizadas.

- **RNF006 – Consultas Analíticas Complexas**

Descrição: O tempo de resposta para consultas analíticas complexas, que envolvam agregação de múltiplos campos de dados e sejam utilizadas em dashboards ou relatórios, não deve exceder 30 segundos para 90% das consultas, considerando um volume de dados correspondente aos últimos 30 dias de ingestão de logs.

Classificação ISO/IEC 25010: Eficiência de desempenho.

Prioridade: Baixa

Formulação SMART:

Específico: Consultas analíticas complexas, que envolvem a agregação de múltiplos tipos de dados ou um grande volume histórico (últimos 30 dias de ingestão), utilizadas em dashboards e relatórios, devem ter um tempo de resposta não superior a 30 segundos.

Mensurável: Tempo de resposta em segundos (≤ 30s). O volume de dados é definido como os "últimos 30 dias de ingestão" (requer uma estimativa da taxa média de ingestão diária para testes).

Alcançável: Viável com otimização de banco de dados, indexação e design de consultas.

Relevante: Garante que relatórios e análises mais profundas sejam gerados em tempo aceitável para o usuário.

Temporizado: Durante todas as operações envolvendo a geração de relatórios e dashboards analíticos complexos.

Método de Verificação: Teste de Desempenho (focado em performance de consultas).

Critérios de Aceitação: 95% de um conjunto predefinido de consultas analíticas complexas (mínimo de 5 representativas) sobre um volume de dados equivalente a 30 dias de ingestão típica devem ser concluídas em menos de 30 segundos.

Impacto no Plano de Testes: Testes de desempenho específicos para consultas analíticas complexas predefinidas, utilizando um volume de dados representativo de 30 dias de ingestão,

profiling de banco de dados para identificar e otimizar consultas lentas.

Impacto na Arquitetura: Esquema de banco de dados otimizado para consultas analíticas (modelagem dimensional, desnormalização seletiva), estratégias de indexação abrangentes para dados históricos, técnicas de otimização de consultas SQL, consideração de caches para resultados de relatórios frequentemente acessados, potencial uso de bancos de dados analíticos ou colunares se o RDBMS tradicional não atender.

- **RNF007 – Conformidade WCAG**

Descrição: A interface do sistema deve estar em conformidade com as Diretrizes de Acessibilidade para Conteúdo Web (WCAG) 2.1 Nível AA, garantindo acessibilidade para usuários com diferentes necessidades, a ser verificado ao final do ciclo de desenvolvimento da interface principal.

Classificação ISO/IEC 25010: Usabilidade.

Prioridade: Baixa

Formulação SMART:

Específico: A interface web do sistema deve atender os critérios das Diretrizes de Acessibilidade para Conteúdo Web (WCAG) 2.1 Nível AA.

Mensurável: Conformidade verificada contra a checklist WCAG 2.1 Nível AA. Número de não conformidades.

Alcançável: Viável com design e desenvolvimento cuidadosos, e uso de ferramentas de teste de acessibilidade.

Relevante: Garante que o sistema seja utilizável por pessoas com uma ampla gama de deficiências.

Método de Verificação: Auditoria de Acessibilidade (usando ferramentas e verificações manuais), Demonstração com tecnologias assistivas.

Critérios de Aceitação: Um relatório de auditoria de acessibilidade confirma a conformidade com todos os critérios WCAG 2.1 Nível AA, sem problemas de acessibilidade críticos ou de alta severidade identificados.

Impacto no Plano de Testes: Auditorias de acessibilidade utilizando ferramentas automatizadas e verificações manuais (navegação por teclado, testes com leitores de tela), testes de usabilidade com usuários com diferentes tipos de deficiência, validação contra a checklist WCAG 2.1 Nível AA.

Impacto na Arquitetura: Frameworks e componentes de front-end com bom suporte à acessibilidade, uso de HTML semântico e implementação correta de atributos ARIA (Accessible Rich Internet Applications), design que considere contraste de cores adequado, legendas para imagens, alternativas textuais para conteúdo não textual e navegabilidade via teclado.

- **RNF008 – Disponibilidade do Sistema**

Descrição: O sistema deve ter uma disponibilidade mínima de 99,5% em ambiente de produção, calculada mensalmente, excluindo janelas de manutenção planejadas comunicadas com 48 horas de antecedência.

Classificação ISO/IEC 25010: Confiabilidade.

Prioridade: Alta

Formulação SMART:

Específico: O sistema em produção deve alcançar um uptime mínimo de 99,5%, calculado mensalmente, excluindo janelas de manutenção programadas (máximo de 4 horas/mês).

Mensurável: Percentual de disponibilidade: (Tempo total no mês - Tempo de inatividade no mês) / Tempo total no mês * 100. Deve ser ≥ 99,5%.

Alcançável: Viável com infraestrutura robusta, redundância e monitoramento.

Relevante: Crítico para uma ferramenta de monitoramento de segurança que precisa estar operacional.

Temporizado: Medido mensalmente assim que o sistema estiver em produção.

Método de Verificação: Monitoramento de Uptime (usando ferramentas de monitoramento), Análise de Logs do Servidor.

Critérios de Aceitação: Relatórios mensais de uptime demonstram ≥ 99,5% de disponibilidade por 3 meses consecutivos pós-deployment. O tempo de inatividade não excede 3,65 horas por mês (0,5% de aprox. 730 horas).

Impacto no Plano de Testes: Testes de confiabilidade de longa duração, monitoramento de uptime em homologação e produção. Casos de teste para mecanismos de failover e recuperação.

Impacto na Arquitetura: Design para alta disponibilidade, incluindo redundância para componentes críticos (servidores, bancos de dados, unidades de processamento), balanceamento de carga, verificações de saúde automatizadas e mecanismos de failover. Sendo um SaaS, isso

depende dos SLAs do provedor de nuvem e do design resiliente interno.

- **RNF009 – Tolerância a Falhas e Recuperação**

Descrição: O sistema deve ser tolerante a falhas em seus componentes críticos (ex: módulo de ingestão de logs, banco de dados de análise). Em caso de falha, o sistema deve ser capaz de se recuperar e retomar a operação normal em até 1 hora, com uma perda máxima de dados de 15 minutos (RPO de 15 minutos, RTO de 1 hora).

Classificação ISO/IEC 25010: Confiabilidade.

Prioridade: Média

Formulação SMART:

Específico: Em caso de falha em um componente crítico do sistema (servidor de banco de dados, motor de processamento), o sistema deve se recuperar automaticamente ou ser manualmente recuperável para o status operacional completo em até 1 hora. A perda máxima de dados aceitável durante tal evento é de 15 minutos de logs ingeridos antes da falha.

Mensurável: Tempo de Recuperação Objetivo (RTO) ≤ 1 hora. Ponto de Recuperação Objetivo (RPO) ≤ 15 minutos.

Alcançável: Viável com mecanismos de failover, backups regulares e arquitetura resiliente.

Relevante: Garante a continuidade dos negócios e minimiza a perda de dados durante incidentes.

Temporizado: Testado antes do deployment em produção e verificado anualmente.

Método de Verificação: Teste de Falhas (princípios de Chaos Engineering), Teste de Recuperação de Desastres.

Critérios de Aceitação: Falhas simuladas de componentes críticos demonstram RTO de ≤ 1 hora e RPO de ≤ 15 minutos. Procedimentos de recuperação são documentados e executados com sucesso.

Impacto no Plano de Testes: Exercícios de "Chaos Engineering" para simular falhas inesperadas de componentes críticos, testes de recuperação de desastres, medindo o Tempo de Recuperação Objetivo (RTO) e o Ponto de Recuperação Objetivo (RPO), validação rigorosa dos procedimentos de backup e restauração.

Impacto na Arquitetura: Componentes redundantes e mecanismos de failover automatizados, estratégia de backups frequentes e consistentes (snapshots de banco de dados, proteção contínua de dados para logs), estratégias de replicação de dados (síncrona ou assíncrona, dependendo do

impacto na performance vs. RPO), procedimentos de recuperação bem documentados e testados.

- **RNF010 – Correção de Defeitos Críticos**

Descrição: O tempo médio para identificar a causa raiz e corrigir um defeito classificado como crítico (que impeça funcionalidades essenciais ou cause perda de dados) deve ser inferior a 5 horas de trabalho da equipe de desenvolvimento após a sua notificação e reprodução.

Classificação ISO/IEC 25010: Manutenibilidade.

Prioridade: Média

Formulação SMART:

Específico: O Tempo Médio Para Reparo (MTTR) para defeitos críticos, desde a identificação até o deployment de uma correção no ambiente de produção, deve ser inferior a 5 horas.

Mensurável: Tempo em horas (< 5 horas), rastreado via sistema de acompanhamento de issues.

Alcançável: Viável com bom logging, monitoramento, equipe qualificada e pipeline CI/CD eficiente.

Relevante: Minimiza o impacto de problemas críticos nos usuários e na operação do sistema.

Temporizado: Medido para cada defeito crítico ocorrendo em produção.

Método de Verificação: Análise de Histórico de Defeitos, Simulação de Resposta a Incidentes.

Critérios de Aceitação: Durante um período de 6 meses, o tempo médio para resolver 90% dos defeitos críticos reportados é inferior a 5 horas.

Impacto no Plano de Testes: Manutenção de ambientes de teste que espelhem fielmente o ambiente de produção para facilitar a reprodução de defeitos. Desenvolvimento de casos de teste para verificar as correções de defeitos e garantir que não introduzam regressões.

Impacto na Arquitetura: Implementação de logging e monitoramento abrangentes e detalhados para auxiliar no diagnóstico rápido de problemas. Design modular que permita isolar falhas e facilitar a identificação da causa raiz. Pipeline de Integração Contínua/Entrega Contínua (CI/CD) para permitir o deployment rápido de correções. Uso de feature flags para desabilitar componentes defeituosos, se necessário. Procedimentos de rollback claros e testados.

- **RNF011 – Integração de Novas Funcionalidades**

Descrição: Novas funcionalidades de complexidade média devem ser integradas ao sistema existente com menos de 2 dias de esforço adicional dedicados exclusivamente à integração e testes de regressão associados.

Classificação ISO/IEC 25010: Manutenibilidade.

Prioridade: Média

Formulação SMART:

Específico: Integrar novas funcionalidades de complexidade média no sistema existente, incluindo desenvolvimento, teste e deployment, deve requerer menos de 2 pessoa-dias de esforço.

Mensurável: Esforço em pessoa-dias (< 2). Nível de complexidade claramente definido.

Alcançável: Viável com design modular, padrões de codificação claros e testes automatizados.

Relevante: Garante que o sistema possa evoluir e se adaptar a novos requisitos eficientemente.

Temporizado: Avaliado durante cada ciclo de desenvolvimento envolvendo funcionalidades de complexidade média.

Método de Verificação: Revisão de Código, Análise de Esforço de Desenvolvimento (de ferramentas de gerenciamento de projetos).

Critérios de Aceitação: Pelo menos 3 novas funcionalidades de complexidade média são integradas com um esforço documentado de menos de 2 pessoa-dias cada.

Impacto no Plano de Testes: Foco em testes automatizados (unitários, de integração, de regressão) para garantir que novas funcionalidades não quebrem o comportamento existente. Avaliação da testabilidade dos novos componentes desde o início do desenvolvimento.

Impacto na Arquitetura: Arquitetura modular (microsserviços, módulos bem definidos com baixo acoplamento e alta coesão). Contratos de API claros e estáveis entre os componentes. Adoção de padrões de codificação e design consistentes em toda a aplicação. Documentação técnica abrangente para desenvolvedores. Pipeline de CI/CD eficiente para agilizar a integração e o deployment de novas funcionalidades.

- **RNF012 – Implantação em Diferentes Ambientes**

Descrição: O sistema deve ser capaz de ser implantado em ambientes operacionais Windows (Server 2019 ou superior), Linux (distribuições baseadas em RHEL 8/9 ou Ubuntu 20.04/22.04 LTS) e macOS (para fins de desenvolvimento/teste local, versão mais recente -1), sem

necessidade de alterações no código fonte principal, utilizando scripts de implantação ou contêineres (Docker) fornecidos.

Classificação ISO/IEC 25010: Portabilidade.

Prioridade: Média

Formulação SMART:

Específico: A aplicação principal (componentes do lado do servidor e quaisquer distribuíveis do lado do cliente) deve ser implantável e totalmente funcional em ambientes Windows (Server 2019+), Linux (Ubuntu 20.04+, CentOS 7+) e macOS (as 2 últimas versões principais) sem requerer modificações no código fonte. Alterações de configuração são permitidas. (Considerando a "implementação local").

Mensurável: Implantação bem-sucedida e execução de todas as funcionalidades principais em cada SO especificado.

Alcançável: Viável usando tecnologias multiplataforma (Java, Python, Node.js, conteinerização como Docker).

Relevante: Fornece flexibilidade para implantação do cliente.

Temporizado: Verificado antes da primeira liberação que suporta implantações locais e verificado para liberações maiores.

Método de Verificação: Teste de Instalação, Teste Funcional em cada SO alvo.

Critérios de Aceitação: O sistema instala com sucesso e passa em um conjunto de testes de fumaça definido nas versões atuais do Windows Server, Linux (Ubuntu, CentOS) e macOS.

Impacto no Plano de Testes: Criação e manutenção de ambientes de teste dedicados para cada sistema operacional alvo (Windows, Linux, macOS), execução completa da suíte de testes funcionais em cada um dos sistemas operacionais suportados, testes de instalação, configuração e desinstalação em cada SO.

Impacto na Arquitetura: Uso de linguagens de programação e frameworks multiplataforma (Java, Python, Node.js, Go), utilização de conteinerização (Docker) para abstrair diferenças entre os sistemas operacionais e simplificar o deployment, evitar o uso de APIs específicas do sistema operacional ou, se necessário, fornecer camadas de abstração ou compilação condicional, scripts de build e ferramentas de deployment que suportem todos os sistemas operacionais alvo.

- **RNF013 – Configuração de Alerta Padrão**

Descrição: A interface do sistema deve permitir que analista de segurança (nível 1, 2 e 3) ou especialista forense ou analista de risco e DPO, configurem um alerta padrão (baseado em templates predefinidos para eventos comuns como múltiplas falhas de login) em no máximo 5 passos (cliques ou preenchimento de campos essenciais) a partir da tela de gerenciamento de alertas.

Classificação ISO/IEC 25010: Usabilidade.

Prioridade: Baixa

Formulação SMART:

Específico: Usuários com os papéis “analista de segurança (nível 1, 2 e 3) ou especialista forense ou analista de risco e DPO”, devem ser capazes de configurar um alerta padrão do sistema (baseado em um template predefinido) através da interface do usuário.

Mensurável: Número de passos contados para tarefas específicas de configuração de alerta (≤ 5).

Alcançável: Viável com um fluxo de UI bem desenhado.

Relevante: Melhora a facilidade de uso e reduz o tempo para tarefas comuns de configuração.

Temporizado: Validado durante a fase de testes de usabilidade antes da liberação.

Método de Verificação: Teste de Usabilidade (análise de conclusão de tarefa).

Critérios de Aceitação: 90% dos usuários de teste (analista de segurança (nível 1, 2 e 3) ou especialista forense ou analista de risco e DPO) conseguem configurar com sucesso um alerta padrão em 5 passos sem assistência.

Impacto no Plano de Testes: Testes de usabilidade focados no fluxo de configuração de alertas padrão. Análise de conclusão de tarefa: usuários (representando os papéis Analista/Diretor) tentam configurar alertas, e o número de passos é contado e avaliado.

Impacto na Arquitetura: Design de UI/UX com fluxos de trabalho otimizados para tarefas comuns, como a configuração de alertas. Uso de interfaces estilo "wizard" ou templates predefinidos para configuração simplificada de alertas padrão.

- **RNF014 – Integridade dos Dados de Log e Análises**

Descrição: O sistema deve garantir a integridade dos dados de log brutos armazenados e das análises geradas, implementando mecanismos para detectar e alertar sobre quaisquer alterações

não autorizadas nos dados armazenados (hashing, checksums, logs de acesso imutáveis), com verificação periódica (diária).

Classificação ISO/IEC 25010: Segurança.

Prioridade: Média

Formulação SMART:

Específico: O sistema deve implementar mecanismos (hashing, assinaturas digitais, armazenamento append-only) para assegurar a integridade dos dados de log armazenados e das análises geradas. Deve detectar quaisquer modificações não autorizadas nesses conjuntos de dados e disparar um alerta para os administradores em até 10 minutos após a detecção.

Mensurável: Detecção de tentativas de adulteração. Geração de alerta em até 10 minutos.

Alcançável: Viável com checksums, algoritmos de hashing e ferramentas de monitoramento de integridade.

Relevante: Crítico para a confiabilidade da análise forense e trilhas de auditoria.

Temporizado: Implementado até a primeira versão de produção e monitorado continuamente.

Método de Verificação: Teste de Segurança (tentativa de adulterar dados), Auditoria de Código.

Critérios de Aceitação: Todas as tentativas de modificar dados de log armazenados ou resultados de análises sem autorização são detectadas. Um alerta é gerado e entregue ao canal administrativo designado em até 10 minutos após a modificação não autorizada detectada.

Impacto no Plano de Testes: Testes de segurança com tentativas de adulteração (tampering) dos dados de log e resultados de análises armazenados. Verificação de que os alertas de violação de integridade são gerados corretamente e dentro do tempo especificado (10 minutos). Testes dos mecanismos de verificação de integridade (validação de checksums/hashes).

Impacto na Arquitetura: Uso de algoritmos de hashing (SHA-256) para gerar e verificar a integridade de logs e análises. Consideração de assinaturas digitais para garantir autenticidade e integridade. Uso de armazenamento append-only para logs brutos. Ferramentas de monitoramento e verificação periódica da integridade dos dados. Trilha de auditoria segura para quaisquer acessos ou modificações nos próprios mecanismos de integridade.

- **RNF015 – Armazenamento de Dados Históricos**

Descrição: O sistema deve ser capaz de armazenar dados históricos de logs pelo período mínimo de 1 ano, considerando um volume máximo anual de até 10 Terabytes de dados brutos, sem

degradação significativa.

Classificação ISO/IEC 25010: Confiabilidade.

Prioridade: Média

Formulação SMART:

Específico: O sistema deve ser capaz de armazenar um mínimo de 1 ano de dados de log brutos históricos, acomodando até 10 Terabytes de volume total de dados brutos anualmente, mantendo a recuperabilidade dos dados.

Mensurável: Capacidade de armazenamento (até 10TB/ano). Período de retenção (mínimo de 1 ano). Recuperação bem-sucedida de dados de vários pontos na janela de 1 ano.

Alcançável: Viável com soluções de armazenamento apropriadas e políticas de gerenciamento de dados (armazenamento em camadas, compressão).

Relevante: Suporta análise de longo prazo, conformidade e investigação histórica.

Temporizado: Planejamento de capacidade a ser revisado anualmente; políticas de retenção de dados aplicadas continuamente.

Método de Verificação: Teste de Capacidade de Armazenamento, Teste de Recuperação de Dados Históricos.

Critérios de Aceitação: O sistema demonstra capacidade de ingerir e armazenar dados até o volume especificado (10TB/ano) e retê-los por pelo menos 1 ano.

Impacto no Plano de Testes: Uso de ferramentas de geração de dados para simular a ingestão de logs até o volume de 10TB ao longo de um ano. Testes de desempenho na recuperação de dados históricos (logs de 6, 9, 11 meses atrás). Verificação da aplicação correta das políticas de retenção de dados (expurgo ou arquivamento de dados após o período definido).

Impacto na Arquitetura: Sistemas de arquivos distribuídos, object storage, bancos de dados time-series com boa compressão. Implementação de políticas de gerenciamento do ciclo de vida dos dados (tiers de armazenamento hot, warm, cold). Estratégias eficientes de indexação para dados históricos. Uso de técnicas de compressão para os logs armazenados. Planejamento e monitoramento contínuo da capacidade de armazenamento.

- **RNF016 – Escalabilidade Horizontal**

Descrição: O sistema deve ser projetado para escalar horizontalmente para suportar um aumento de 50% no volume de logs ingeridos por hora e um aumento de 40% no número de usuários

concorrentes dentro de 7 meses após o lançamento, mantendo os tempos de resposta definidos nos requisitos de desempenho (RNF 001, RNF 002, RNF 006).

Classificação ISO/IEC 25010: Eficiência de desempenho

Prioridade: Baixa

Formulação SMART:

Específico: Em até 7 meses após o deployment inicial, a arquitetura do sistema deve ser capaz de escalar horizontalmente para suportar um aumento de 50% no volume de logs e 40% no número de usuários concorrentes, mantendo os tempos de resposta definidos nos requisitos de desempenho (RNF 001, RNF 002).

Mensurável: Aumento percentual no volume de logs (50%) e usuários concorrentes (40%). As métricas de desempenho (RNF 001, RNF 002) devem permanecer dentro dos limites estabelecidos.

Alcançável: Viável com arquitetura baseada em microsserviços, balanceamento de carga e bancos de dados distribuídos.

Relevante: Garante que o sistema possa crescer com as necessidades do cliente sem degradação de performance.

Temporizado: A capacidade de escalabilidade deve ser demonstrada dentro de 7 meses a partir de um ponto de medição de linha de base definido.

Método de Verificação: Teste de Escalabilidade, Teste de Carga Prolongado.

Critérios de Aceitação: Quando submetido a um aumento de 50% no volume de logs e 40% mais usuários concorrentes em relação à linha de base, todos os requisitos não funcionais críticos de desempenho (RNF 001, RNF 002, RNF 006) ainda são atendidos. A escalabilidade horizontal melhora demonstravelmente a capacidade.

Impacto no Plano de Testes: Testes de escalabilidade, aumentando gradualmente a carga de logs e usuários e adicionando recursos (nós) para verificar se o desempenho se mantém. Benchmarking de performance em diferentes pontos de escala. Monitoramento do uso de recursos (CPU, memória, rede, I/O) em cada nó da arquitetura distribuída.

Impacto na Arquitetura: Design de componentes de aplicação preferencialmente stateless. Uso de balanceadores de carga para distribuir o tráfego. Bancos de dados e sistemas de armazenamento que suportem escalabilidade horizontal. Capacidade de auto-scaling. Filas de mensagens para desacoplar serviços e gerenciar picos de carga.

- **RNF017 – Documentação de Implementação**

Descrição: O sistema deve fornecer uma documentação clara e abrangente que explique como instalar, configurar e iniciar o uso básico do sistema Argos (ingestão de logs e visualização de dashboards padrão) em cada um dos ambientes suportados (definidos no RNF 012). A documentação deve permitir que um administrador de sistemas com 2 anos de experiência realize a instalação em até 4 horas.

Classificação ISO/IEC 25010: Usabilidade.

Prioridade: Média

Formulação SMART:

Específico: Uma documentação de deployment abrangente deve ser fornecida com o sistema, detalhando procedimentos passo a passo para instalar, configurar e verificar o sistema Argos em ambientes suportados (Windows, Linux, macOS conforme RNF 0012).

Mensurável: Completude da documentação contra uma checklist de tarefas de deployment. Sucesso no deployment por um novo usuário seguindo a documentação.

Alcançável: Prática padrão para produtos de software.

Relevante: Facilita a configuração e adoção do sistema por usuários/administradores.

Temporizado: Disponível com a primeira liberação do software.

Método de Verificação: Revisão de Documentação, Teste de Instalação por Terceiros (seguindo o guia).

Critérios de Aceitação: Um redator técnico ou um novo membro da equipe consegue realizar o deployment do sistema Argos com sucesso em um ambiente limpo suportado, usando apenas a documentação fornecida, dentro de um prazo definido (4 horas). A documentação cobre todos os passos, desde pré-requisitos até verificações operacionais básicas.

Impacto no Plano de Testes: Testes de "caixa-preta" da documentação: membros da equipe e testadores externos não familiarizados com o sistema tentam realizar a instalação e configuração usando apenas o manual. Verificação da clareza, correção e completude de todos os passos da documentação. Teste do processo de instalação documentado em todos os sistemas operacionais suportados (conforme RNF 0012).

Impacto na Arquitetura: Design que vise um processo de implantação o mais simples possível. Listagem clara de todas as dependências e pré-requisitos de software e hardware. Parâmetros de configuração bem documentados, com exemplos. Fornecimento de scripts ou instaladores para automatizar partes do processo de setup.

- **RNF018 – Validação de Entrada de Dados**

Descrição: O sistema deve incluir validação rigorosa na entrada de todos os dados provenientes de fontes externas ou de interação do usuário (configurações, filtros de busca, uploads de arquivos de log), para mitigar riscos de ataques comuns, como injeção de código (SQL Injection, XSS) e scripts maliciosos, conforme as top 10 vulnerabilidades do OWASP.

Classificação ISO/IEC 25010: Segurança.

Prioridade: Média

Formulação SMART:

Específico: Todos os campos de entrada fornecidos pelo usuário e interfaces de ingestão de dados devem implementar validação de entrada rigorosa (verificação de tipo, sanitização, limites de comprimento, validação de formato) para prevenir ataques de injeção comuns (SQLi, XSS, command injection) conforme as recomendações do OWASP Top 10.

Mensurável: Percentual de vetores de entrada validados. Número de vulnerabilidades encontradas em testes de penetração relacionados à validação de entrada.

Alcançável: Prática padrão de codificação segura.

Relevante: Protege o sistema contra vulnerabilidades web comuns e corrupção de dados.

Temporizado: Implementado e verificado antes de cada liberação.

Método de Verificação: Auditoria de Código (foco em segurança), Teste de Penetração, Teste de Segurança de Aplicação Dinâmica (DAST).

Critérios de Aceitação: Nenhuma vulnerabilidade crítica ou de alta severidade relacionada à validação de entrada (SQLi, XSS) é encontrada durante os testes de segurança. A revisão de código confirma que mecanismos de validação de entrada são aplicados a todos os pontos de entrada de dados externos.

Impacto no Plano de Testes: Uso de ferramentas de Teste de Segurança de Aplicação Dinâmica (DAST). Testes de penetração manuais com foco em vulnerabilidades de injeção (SQLi, XSS, Command Injection, etc.). Fuzz testing em todos os campos de entrada. Casos de teste específicos com entradas malformadas e maliciosas. Revisão de código focada em validação de entrada.

Impacto na Arquitetura: Utilização consistente de bibliotecas ou frameworks de validação de entrada robustos. Abordagem de defesa em profundidade: validação no lado do cliente (para UX) e, crucialmente, no lado do servidor. Uso de consultas parametrizadas ou ORMs para interações

com banco de dados, prevenindo SQLi. Codificação de saída (output encoding) para dados exibidos na UI, prevenindo XSS.

- **RNF019 – Atualização de Software**

Descrição: O processo de atualização para novas versões do software do sistema Argos (aplicação de patches ou novas releases) deve ser realizado com um tempo de inatividade planejado máximo de 30 minutos por atualização.

Classificação ISO/IEC 25010: Manutenibilidade.

Prioridade: Média

Formulação SMART:

Específico: O processo padrão para atualizar o sistema para uma nova versão de software deve ser realizável com um tempo de inatividade planejado máximo de 30 minutos.

Mensurável: Tempo de inatividade em minutos (≤ 30).

Alcançável: Viável com scripts de atualização eficientes, estratégias de deployment blue/green ou rolling updates para componentes críticos.

Relevante: Minimiza a interrupção para os usuários durante a manutenção do software.

Temporizador: Para todas as atualizações de versão planejadas no ambiente de produção.

Método de Verificação: Teste de Processo de Atualização (em ambiente de homologação).

Critérios de Aceitação: O procedimento de atualização documentado, quando executado em um ambiente similar ao de produção, resulta em um tempo de inatividade do sistema não superior a 30 minutos por 3 atualizações de teste consecutivas.

Impacto no Plano de Testes: Testes repetidos e rigorosos do processo de atualização em um ambiente de homologação que simula o ambiente de produção. Medição precisa do tempo real de inatividade durante as atualizações de teste. Teste dos procedimentos de rollback caso uma atualização falhe ou cause problemas.

Impacto na Arquitetura: Suporte a estratégias de deployment como Blue-Green ou Rolling Updates para minimizar o tempo de inatividade. Estratégias de migração de esquema de banco de dados que permitam mínima interrupção do serviço. Scripts eficientes e automatizados para backup, atualização e verificação pós-atualização. Gerenciamento de sessão que possa lidar com breves interrupções ou reinícios de componentes durante a atualização.

- **RNF020 – Navegadores Web**

Descrição: A interface web do sistema deve ser totalmente funcional e apresentar um layout consistente (sem quebras visuais significativas) nas duas últimas versões estáveis dos navegadores web mais utilizados: Google Chrome, Mozilla Firefox, Microsoft Edge e Apple Safari, no momento do lançamento da versão.

Classificação ISO/IEC 25010: Compatibilidade

Prioridade: Média

Formulação SMART:

Específico: A interface do usuário baseada na web do sistema Argos deve ser totalmente funcional (todas as funcionalidades operam como esperado) e manter um layout consistente (sem elementos quebrados ou discrepâncias visuais significativas) nas versões estáveis mais recentes dos navegadores Google Chrome, Mozilla Firefox, Microsoft Edge e Apple Safari no momento de cada liberação.

Mensurável: Lista de navegadores e versões suportadas. Percentual de casos de teste aprovados em cada navegador. Número de inconsistências de layout.

Alcançável: Viável com desenvolvimento web compatível com padrões e testes cross-browser.

Relevante: Garante uma boa experiência do usuário para a maioria dos usuários, independentemente da escolha do navegador.

Temporizado: Verificado antes de cada liberação maior e menor.

Método de Verificação: Teste de Compatibilidade de Navegador (manual e automatizado).

Critérios de Aceitação: Todas as funcionalidades principais são aprovadas nas versões estáveis mais recentes de Chrome, Firefox, Edge e Safari. Não mais do que 5 inconsistências menores de layout são reportadas em todos os navegadores suportados, sem que nenhuma funcionalidade

Impacto no Plano de Testes: Testes funcionais e de layout nas versões estáveis mais recentes de todos os navegadores especificados (Chrome, Firefox, Edge, Safari). Uso de plataformas ou serviços de teste de navegadores para cobrir diferentes versões e configurações. Execução de testes de UI automatizados em diferentes navegadores.

Impacto na Arquitetura: Aderência estrita aos padrões web (HTML, CSS, JavaScript). Uso de frameworks de front-end conhecidos por oferecer bom suporte cross-browser. Utilização de bibliotecas de CSS reset ou normalize para garantir uma base de estilo consistente. Implementação de graceful degradation ou uso de polyfills para funcionalidades não suportadas

nativamente em todos os navegadores. Preferência por feature detection em vez de browser sniffing para aplicar lógicas específicas de navegador.

5. Lista de regras de negócio

- **RN001: Identificação Única de Usuário**

Descrição: Cada usuário cadastrado no sistema Argos deve ser unicamente identificável por seu endereço de e-mail. Não será permitida a existência de dois usuários com o mesmo endereço de e-mail.

Fonte/Autoridade: "Documento_Visao.pdf" (implícito pela necessidade de cadastro e login); Práticas comuns de gerenciamento de identidade.

Impacto: Afeta a funcionalidade F1. Manter cadastro de usuário (processos de inclusão e edição de e-mail).

- **RN002: Atribuição Obrigatória de Perfil de Acesso**

Descrição: Todo usuário ativo no sistema Argos deve estar associado a um perfil de permissões. Este perfil determinará suas permissões de acesso às funcionalidades e dados do sistema.

Fonte/Autoridade: "Documento_Visao.pdf" (funcionalidades F2. Manter perfil de acesso e F3. Realizar controle lógico de acesso).

Impacto: Afeta as funcionalidades F1. Manter cadastro de usuário (inclusão/edição de usuário) e F2. Manter perfil de acesso.

- **RN003: Dados Obrigatórios para Cadastro de Usuário**

Descrição: Para o cadastro de um novo usuário no sistema Argos, o fornecimento de Nome Completo, Endereço de E-mail válido (conforme RN-001), Senha Inicial (conforme RN-004) e a atribuição de um Perfil de Acesso (conforme RN-002) são obrigatórios.

Fonte/Autoridade: "Documento_Visao.pdf" (F1. Manter cadastro de usuário); Necessidades de autenticação e autorização.

Impacto: Afeta a funcionalidade F1. Manter cadastro de usuário (processo de inclusão).

- **RN004: Política de Complexidade de Senha**

Descrição: A senha do usuário do sistema Argos deve atender a uma política de complexidade mínima, que inclui: um comprimento mínimo de 8 caracteres, contendo pelo menos uma letra maiúscula, uma letra minúscula, um número e um caractere especial.

Fonte/Autoridade: "Documento_Visao.pdf" (RNF 003 de Segurança: "O sistema deve proteger dados sensíveis, como credenciais de acesso"); Boas práticas de segurança da informação.

Impacto: Afeta a funcionalidade F1. Manter cadastro de usuário (processos de inclusão e definição/alteração de senha).

- **RN005: Armazenamento Seguro de Credenciais**

Descrição: A senha do usuário deve ser armazenada no sistema de forma segura, utilizando algoritmos de hashing robustos com a adição de salt, para impedir sua recuperação em formato de texto claro.

Fonte/Autoridade: "Documento_Visao.pdf" (RNF 003 de Segurança: "O sistema deve proteger dados sensíveis, como credenciais de acesso."); Boas práticas de segurança da informação.

Impacto: Afeta a funcionalidade F1. Manter cadastro de usuário (aspecto de segurança da infraestrutura de dados).

- **RN006: Controle de Acesso Baseado em Perfil**

Descrição: O acesso de um usuário às funcionalidades e dados do sistema Argos será determinado exclusivamente pelas permissões associadas ao seu perfil de acesso. Funcionalidades ou dados não explicitamente permitidos pelo perfil serão inacessíveis.

Fonte/Autoridade: "Documento_Visao.pdf" (funcionalidade F3. Realizar controle lógico de acesso).

Impacto: Afeta a funcionalidade F3. Realizar controle lógico de acesso e, indiretamente, todas as demais funcionalidades do sistema.

- **RN07: Identificação de IP fora do horário permitido**

Descrição: O sistema deve considerar como suspeito todo o acesso originado de um IP válido,

porém ocorrido fora da faixa de horário definida como permitida (ex: 08h - 18h), e gerar um alerta automaticamente.

Fonte/autoridade: Política Corporativa de Acesso Seguro v3.2. / "Documento_Visao.pdf" (funcionalidade F5. Emitir alerta para atividades suspeitas, como acesso fora de hora).

Impacto: UC-004 Analisar Logs; UC-005 Gerar Alerta. / Afeta a funcionalidade F5. Emitir alerta para atividades suspeitas.

- **RN08: Detecção de Múltiplas Tentativas de Login com Erro**

Descrição: O sistema deve gerar um alerta se um mesmo IP realizar mais de 5 tentativas consecutivas de login com erro em um intervalo inferior a 10 minutos.

Fonte/autoridade: Manual de Boas Práticas de Segurança – Item 2.6. / "Documento_Visao.pdf" (funcionalidade F5. Emitir alerta para atividades suspeitas).

Impacto: UC-004 Analisar Logs; UC-005 Gerar Alerta; UC-007 Notificar SOC. / Afeta a funcionalidade F5. Emitir alerta para atividades suspeitas e F13. Relatório de Tentativas de Login Falhadas.

- **RN09: Verificação de IP em Lista de Blacklist**

Descrição: O sistema deve manter um script que consulte blacklist públicas usando APIs de fontes de Threat Intelligence como “AbusellPDB” e blacklist privadas que leem um arquivo de texto ou CSV mantidos pela empresa, assim que um IP for identificado deve ser marcado como suspeito e um alerta deve ser disparado automaticamente.

Fonte/autoridade: Repositório Central de Ameaças – ThreatIntel v5.0. / "Documento_Visao.pdf" (funcionalidade F5. Emitir alerta para atividades suspeitas, ... ou IP suspeito).

Impacto: UC-002: Monitoramento e Alerta de Atividades Suspeitas;UC-004: Visualização Hierárquica de Ameaças;UC-006: Análise Temporal e Histórico de Incidentes. / Afeta a funcionalidade F5. Emitir alerta para atividades suspeitas.

- **RN10: Retenção de Trilhas de Auditoria de Usuário**

Descrição: As principais atividades dos usuários, como logins (sucesso e falha), acessos a dados sensíveis e alterações de configuração, incluindo gerenciamento de usuários e perfis, devem ser registradas em uma trilha de auditoria. Esses registros de auditoria devem ser retidos por um período mínimo de 1 (um) ano.

Fonte/Autoridade: "Documento_Visao.pdf" (RNF004 de Segurança: "O sistema deve registrar as principais atividades dos usuários. Retida por 1 ano.").

Impacto: Afeta F1, F2, F3 e potencialmente todas as funcionalidades que envolvem acesso a dados ou configurações.

- **RN11: Geração de Relatório Diário de Atividades Suspeitas**

Descrição: O relatório diário de atividades suspeitas (F6) deve consolidar todas as atividades classificadas como suspeitas (conforme RN 007, RN 008, RN 009) ocorridas nas últimas 24 horas e deverá ser enviado todos os dias às 0h, detalhando para cada uma: timestamp, tipo de suspeita, criticidade, origem (IP, usuário) e sistema/recurso alvo.

Fonte/autoridade: Política de Auditoria de Segurança – Seção 4.1. / "Documento_Visao.pdf" (funcionalidade F6. Gerar relatório diário de atividades suspeitas).

Impacto: UC-003: Geração de Relatórios; UC-006: Análise Temporal e Histórico de Incidentes. / Afeta a funcionalidade F6. Gerar relatório diário de atividades suspeitas.

- **RN12: Classificação Automática da Gravidade de Incidentes**

Descrição: O sistema deve classificar automaticamente a gravidade de cada incidente combinando a sensibilidade do ativo com o contexto e o impacto usando a matriz.

Fator 1: O Ativo Comprometido (Onde ocorreu o acesso?)
Sensibilidade Baixa: Um servidor de desenvolvimento isolado, uma máquina de teste sem dados reais.
Sensibilidade Média: Um servidor web de produção (sem dados pessoais), um servidor de arquivos de um departamento.
Sensibilidade Alta: Um servidor de aplicação que processa dados de clientes.
Sensibilidade Crítica: Um controlador de domínio, um banco de dados com dados pessoais sensíveis, um sistema financeiro, a infraestrutura do próprio Argos.

Fator 2: A Conta Envolvida (Quem realizou o acesso?)
Privilégio Baixo: Uma conta de convidado, um estagiário.
Privilégio Médio: Uma conta de usuário padrão.
Privilégio Alto: Uma conta de administrador de sistema.

Fator 3: O Impacto Potencial (Qual o dano possível?)
Impacto Baixo: Nenhuma exposição de dados, nenhuma interrupção de serviço. O acesso foi contido em um sistema não crítico.

Impacto Médio: Possível exposição de dados internos não sensíveis, degradação de performance de um serviço secundário.
Impacto Alto: Exposição de dados pessoais não sensíveis (nomes, e-mails), interrupção de um serviço de produção.
Impacto Crítico: Exposição de dados pessoais sensíveis (CPF, dados financeiros), alteração ou destruição de dados, interrupção de serviços críticos, perda de controle sobre a infraestrutura.

MATRIZ DE CLASSIFICAÇÃO DE GRAVIDADE:

Sensibilidade do Ativo / Conta	Impacto Baixo	Impacto Médio	Impacto Alto	Impacto Crítico
Baixa	BAIXO	BAIXO	MÉDIO	ALTO
Média	BAIXO	MÉDIO	ALTO	ALTO
Alta	MÉDIO	ALTO	ALTO	CRÍTICO
Crítica	MÉDIO	ALTO	CRÍTICO	CRÍTICO

Fonte/autoridade: "Documento_Visao.pdf" / funcionalidade F7. Visualizar ameaças por níveis de severidade.

Impacto: UC-004: Visualização Hierárquica de Ameaças; UC-003: Geração de Relatórios. / Afeta as funcionalidades F5. Emitir alerta para atividades suspeitas e F7. Visualizar ameaças por níveis de severidade.

- **RN13: Retenção de Logs por 6 Meses para Auditoria**

Descrição: Todos os logs de acesso e eventos suspeitos devem ser armazenados por, no mínimo, 6 meses para fins de auditoria e conformidade com normas de segurança.

Fonte/autoridade: Norma Interna de Compliance e Retenção de Dados – NTI-RD-2023./ "Documento_Visao.pdf" (RNF015 de Confiabilidade: "O sistema deve ser capaz de armazenar dados históricos de logs pelo período mínimo de 1 ano").

Impacto: UC-006: Análise Temporal e Histórico de Incidentes;UC-003: Geração de Relatórios./

Afeta F8. Consultar histórico de incidentes; F9. Gerar insights de tendências sobre incidentes; F10. Gerar relatório de tendências sobre incidentes, e outras funcionalidades de relatório que dependem de dados históricos.

- **RN15: Backup Automático Diário dos Logs**

Descrição:O sistema deve realizar automaticamente o backup diário dos logs, armazenando cópias em locais redundantes e seguros.

Fonte/autoridade: Política de Continuidade de Negócios – Seção 3.4.

Impacto:UC-007: Backup de Segurança; UC-006: Análise Temporal e Histórico de Incidentes.

- **RN16: Multicliente e Segregação de Dados**

Descrição: O sistema Argos é uma solução multicliente. Os dados de cada empresa contratante (incluindo seus logs, configurações, usuários, relatórios) devem ser logicamente segregados e inacessíveis a outras empresas contratantes.

Fonte/Autoridade: "Documento_Visao.pdf"

Impacto: Afeta a arquitetura geral do sistema, o armazenamento de dados e todas as funcionalidades que manipulam dados de clientes..

- **RN17: Atualização de Lista de Perfis na Edição de Usuário**

Descrição: Ao editar um usuário (F1), a lista de perfis disponíveis para atribuição (F2) deve ser apresentada de forma atualizada, contendo apenas os perfis ativos e existentes no sistema no momento da edição.

Fonte/Autoridade: Implícito pela interação entre F1. Manter cadastro de usuários e F2. Manter perfil de acessos.

Impacto: Afeta a F1. Manter cadastro de usuários (processo de edição).

- **RN18: Definição de "Acessos Constantes" como Atividade Suspeita**

Descrição: O sistema deve ser capaz de identificar e alertar sobre "acessos constantes" que

fogem de um padrão comportamental esperado para um usuário ou sistema, como um volume anormalmente alto de acessos a um recurso em um curto período. Os limiares para definir "acessos constantes" devem ser configuráveis ou baseados em análise heurística/IA.

Fonte/Autoridade: "Documento_Visao.pdf" (Declaração da visão do software).

Impacto: Afeta a funcionalidade F5. Emitir alerta para atividades suspeitas.

- **RN19: Detecção Heurística de Eventos Suspeitos**

Descrição: A identificação de eventos suspeitos deve ser realizada por meio de regras baseadas em análise heurística, além de regras explícitas (como as de acesso fora de hora, IP suspeito). Essas heurísticas visam detectar padrões incomuns ou anômalos nos logs.

Fonte/Autoridade: "Documento_Visao.pdf" (Introdução; Declaração da visão do software, seção "Nosso produto").

Impacto: Afeta as funcionalidades F4. Monitoramento em tempo real de logs de acesso e F5. Emitir alerta para atividades suspeitas.

- **RN20: Conteúdo Mínimo para Consulta de Histórico de Incidentes**

Descrição: A consulta ao histórico de incidentes (F8) deve permitir a busca e visualização de incidentes passados, apresentando para cada incidente, no mínimo: data/hora de ocorrência, tipo de incidente/alerta, severidade atribuída, status (se aplicável), e um identificador único. Detalhes adicionais, como logs associados, devem estar acessíveis.

Fonte/Autoridade: "Documento_Visao.pdf" (funcionalidade F8. Consultar histórico de incidentes).

Impacto: Afeta a funcionalidade F8. Consultar histórico de incidentes.

- **RN21: Tipos de Insights de Tendências sobre Incidentes**

Descrição: O sistema deve ser capaz de gerar insights de tendências sobre incidentes (F9) que incluam, no mínimo: a evolução do volume de incidentes ao longo do tempo e a distribuição dos tipos de incidentes mais frequentes em um período selecionado.

Fonte/Autoridade: "Documento_Visao.pdf" (funcionalidade F9. Gerar insights de tendências sobre incidentes).

Impacto: Afeta a funcionalidade F9. Gerar insights de tendências sobre incidentes.

- **RN22: Conteúdo do Relatório de Tendências sobre Incidentes**

Descrição: O relatório de tendências sobre incidentes (F10) deve apresentar de forma consolidada e exportável os insights gerados (conforme RN-020), incluindo gráficos e sumários sobre volume, tipos e, opcionalmente, severidade dos incidentes ao longo do tempo.

Fonte/Autoridade: "Documento_Visao.pdf" (funcionalidade F10. Gerar relatório de tendências sobre incidentes).

Impacto: Afeta a funcionalidade F10. Gerar relatório de tendências sobre incidentes.

- **RN23: Identificação de Incidentes com Dados Pessoais (PII)**

Descrição: O sistema deve possuir mecanismos (e.g., através de tags, configuração de fontes de dados, ou análise de conteúdo baseada em padrões/IA) para identificar incidentes de segurança que potencialmente envolvem o acesso, exposição ou vazamento de Informações Pessoais Identificáveis (PII).

Fonte/Autoridade: "Documento_Visao.pdf" (funcionalidade F11. Gerar relatório sobre incidentes com dados pessoais).

Impacto: Afeta as funcionalidades F5. Emitir alerta para atividades suspeitas e F11. Gerar relatório sobre incidentes com dados pessoais.

- **RN24: Conteúdo do Relatório de Incidentes com Dados Pessoais**

Descrição: O relatório sobre incidentes com dados pessoais (F11) deve listar todos os incidentes identificados (conforme RN-022) em um período, detalhando, quando possível, os tipos de dados pessoais potencialmente afetados, os sistemas envolvidos, e o período do incidente, para suportar investigações.

Fonte/Autoridade: "Documento_Visao.pdf" (funcionalidade F11. Gerar relatório sobre incidentes com dados pessoais).

Impacto: Afeta a funcionalidade F11. Gerar relatório sobre incidentes com dados pessoais.

- **RN25: Conteúdo do Relatório de Atividade de Login Bem-Sucedido**

Descrição: O relatório de atividade de login bem-sucedido (F12) deve listar os logins realizados com sucesso em um período, incluindo, no mínimo, o nome do usuário, endereço IP de origem, timestamp do login e o sistema/aplicação acessada (se aplicável e disponível no log).

Fonte/Autoridade: "Documento_Visao.pdf" (funcionalidade F12. Gerar relatório de Atividade de Login Bem-Sucedido).

Impacto: Afeta a funcionalidade F12. Gerar relatório de Atividade de Login Bem-Sucedido.

- **RN26: Conteúdo do Relatório de Tentativas de Login Falhadas**

Descrição: O relatório de tentativas de login falhadas (F13) deve listar as tentativas mal sucedidas de login em um período, incluindo, no mínimo, o nome de usuário (tentado), endereço IP de origem, timestamp da tentativa e, se disponível, o motivo da falha.

Fonte/Autoridade: "Documento_Visao.pdf" (funcionalidade F13. Relatório de Tentativas de Login Falhadas).

Impacto: Afeta a funcionalidade F13. Relatório de Tentativas de Login Falhadas.

- **RN27: Integridade dos Dados de Log e Análises**

Descrição: O sistema deve implementar mecanismos para garantir a integridade dos dados de log coletados e das análises geradas. Qualquer alteração não autorizada ou corrupção detectada nos dados armazenados deve ser identificada e, se possível, alertada.

Fonte/Autoridade: "Documento_Visao.pdf" (RNF014 Segurança: "O sistema deve garantir a integridade dos dados de log e das análises geradas").

Impacto: Afeta todas as funcionalidades de coleta, armazenamento, processamento e visualização de logs e relatórios.

- **RN28: Validação de Entrada de Dados**

Descrição: Todas as entradas de dados no sistema Argos, seja via interface do usuário ou API (e.g., configurações, filtros de busca, upload de listas de IPs), devem passar por validação rigorosa para mitigar riscos de ataques comuns, como injeção de código e scripts maliciosos, e para garantir a qualidade dos dados.

Fonte/Autoridade: "Documento_Visao.pdf" (RNF018 Segurança: "O sistema deve incluir validação rigorosa na entrada de dados").

Impacto: Afeta todas as funcionalidades que permitem a entrada de dados pelo usuário ou sistemas externos.

- **RN29: Normalização de Logs (Implícita)**

Descrição: Para permitir a correlação eficaz de eventos e a aplicação consistente de regras de análise e alerta, os logs de diferentes fontes e formatos devem passar por um processo de normalização para um esquema comum ou compreensível pelo sistema Argos.

Fonte/Autoridade: Implícito pela necessidade de "correlação de eventos de diferentes fontes" e pela comparação com EventLog Analyzer que realiza "normalização de logs".

Impacto: Afeta F4. Monitoramento em tempo real de logs de acesso, F5. Emitir alerta para atividades suspeitas, e todas as funcionalidades de análise e relatório.

- **RN30: Personalização de Dashboards por Papel**

Descrição: Usuários com papéis de 'Analista' ou 'Diretor' devem ter a capacidade de personalizar a disposição de widgets e visualizações em seus dashboards e salvar essas configurações para acesso futuro.

Fonte/Autoridade: "Documento_Visao.pdf" (RNF005 Usabilidade: "O sistema deve permitir que usuários com papéis de 'Analista' ou 'Diretor' personalizem a disposição de widgets...").

Impacto: Afeta a interface principal do sistema e a experiência do usuário para os papéis especificados.

6. Declaração de uso ético e responsável de inteligência artificial

Neste documento, o grupo utilizou ferramentas de inteligência artificial generativa para auxiliar na elaboração e revisão do conteúdo, visando melhorar a clareza, a estrutura e a concisão das informações apresentadas. Reconhecemos a contribuição dessas ferramentas como um suporte ao processo de escrita e revisão. A ferramenta de IA utilizada foi o Gemini do Google. O uso ocorreu durante o período de elaboração deste Documento. O suporte automatizado foi empregado para auxiliar na organização das ideias, na redação inicial de algumas seções e na revisão gramatical e estilística do texto final. Em particular, a IA contribuiu para refinar a descrição de conceitos relacionados à análise de requisitos, a estrutura do próprio documento de visão, e a formulação de tópicos baseados nos materiais fornecidos, como as dicas para escrever melhores requisitos e a estrutura da matriz de rastreabilidade. A ferramenta também auxiliou na articulação da declaração do problema e da declaração da visão do software Argos, garantindo que os pontos essenciais fossem abordados de forma clara.

Ressaltamos que toda a saída gerada pela ferramenta de IA foi revisada criticamente por membros do grupo. A equipe permanece integralmente responsável pela exatidão, completude e conformidade acadêmica de todo o conteúdo apresentado neste documento. A supervisão humana foi fundamental para garantir que as informações estivessem alinhadas com os objetivos do projeto Argos, as necessidades das partes interessadas, e os padrões de qualidade esperados para documentos de requisitos.