



Educação, Pesquisa
e Inovação em Rede.

CAPA –
Digitar título do
documento

Digitar subtítulo
do documento



APRESENTAÇÃO

A **REDE NACIONAL DE ENSINO E PESQUISA (RNP)** é uma associação civil, sem fins lucrativos, qualificada como organização social, vinculada ao MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÕES (MCTI) e mantida por esse, em conjunto com os MINISTÉRIOS DA EDUCAÇÃO (MEC), das COMUNICAÇÕES (MCOM), TURISMO, SAÚDE (MS) E DEFESA (MD), que participam do programa interministerial **RNP (PRO-RNP)**.

Perfis Solicitados

APRESENTAÇÃO	2
AT – Analista de Atendimento JR	5
AT – Analista de Atendimento PL	5
AT – Analista de Atendimento SR	6
AT – Analista de Atendimento Especializado JR.....	7
AT – Analista de Atendimento Especializado PL	7
AT – Analista de Atendimento Especializado SR	7
ACX - Analista de Experiência JR.....	8
ACX - Analista de Experiência PL	8
ACX - Analista de Experiência SR	9
ASV - Analista de Serviços JR	9
ASV - Analista de Serviços PL.....	10
ASV - Analista de Serviços SR	10
LID-02 – Supervisor de Atendimento e Experiência (CX) Júnior	11
LID-03 – Supervisor de Atendimento e Experiência (CX) Pleno	12
LID-04 – Supervisor de Atendimento e Experiência (CX) Sênior	12
AGP - Analista de Projetos JR	13
AGP - Analista de Projetos PL	13
AGP - Analista de Projetos SR.....	14
SEG-01.1 – Analista de Segurança da informação Nível 1 - JÚNIOR	15
SEG-02.1 - Analista de Segurança da Informação Nível 2 - JÚNIOR	16
SEG-03.1 - Analista de Segurança da Informação Nível 3 - JÚNIOR	17
SEG-01.2 - Analista de Segurança da informação Nível 1 - PLENO.....	18
SEG-02.2 - Analista de Segurança da Informação Nível 2 - PLENO.....	19
SEG-03.2 - Analista de Segurança da Informação Nível 3 - PLENO.....	21
SEG-01.3 - Analista de Segurança da informação Nível 1 - SENIOR	22
SEG-02.3 - Analista de Segurança da Informação Nível 2 - SENIOR	23
SEG-03.3 - Analista de Segurança da Informação Nível 3 - SENIOR	24
SEG-03.4 - Analista de Segurança da Informação Nível 1 - ESPECIALISTA.....	26
SEG-03.5 - Analista de Segurança da Informação Nível 2 - ESPECIALISTA.....	27
SEG-03.5 - Analista de Segurança da Informação Nível 3 - ESPECIALISTA.....	29
SEG-03.6 - Líder Técnico de Segurança – Nível 1 - OPERAÇÃO	30
SEG-03.6 - Líder Técnico de Segurança – Nível 2 - OPERAÇÃO	31
SEG-03.6 - Líder Técnico de Segurança – Nível 3 - OPERAÇÃO	32

SEG-03.6 - Líder Técnico de Segurança – Nível 1 - CORE.....	34
SEG-03.6 - Líder Técnico de Segurança – Nível 2 - CORE.....	35
SEG-03.6 - Líder Técnico de Segurança – Nível 3 - CORE.....	36
ESP-01 – Especialista 1	37
ESP-02 – Especialista 2	38
ESP-03 – Especialista 3	38
ANC – Analista de Negócios JR	39
ANC– Analista de Negócios PL	39
ANC – Analista de Negócios SR.....	40
APC – Analista de Processos JR.....	40
APC-02 – Analista de Processos PL.....	41
APC – Analista de Processos SR	41
ATC – Analista de Telecomunicações JR.....	42
ATC – Analista de Telecomunicações PL	42
1.1 AN1 - Analista de Operações NOC – N1 (24x7) Júnior / Pleno / Sênior	43
1.2 AN2 - Analista de Operações NOC – N2 (24x7) Júnior / Pleno / Sênior	44
1.3 AN3 - Analista de Operações NOC – N3 Pleno / Sênior.....	45
2.1 SNOC-02 – Supervisor de Turno NOC Pleno / Sênior	46
2.2 SNOC-03 – Supervisor de Turno NOC	47
3.1 AOSS - Analista OSS & Automação (OSS/Zabbix/Integrações) Júnior / Pleno / Sênior	47
3.2 ADOC – Assistente de Cadastro & Documentação de Rede (Netbox/CMDB) Júnior / Pleno / Sênior.....	48
3.4 AQ - Analista de Qualidade & Garantia de Serviço Júnior / Pleno / Sênior	49

A Diretoria de Engenharia e Operações (DEO) da RNP é responsável, de forma central, pelo planejamento, arquitetura, implantação, operação, monitoramento e evolução contínua da infraestrutura de redes, assegurando elevados níveis de disponibilidade, desempenho, capacidade, resiliência e continuidade operacional. Compete-lhe conduzir a engenharia da infraestrutura de conectividade, incluindo o desenho de soluções, a expansão e modernização da rede, a gestão da capacidade e a sustentação dos ativos tecnológicos, bem como garantir a operação ininterrupta dos ambientes sob sua responsabilidade por meio de práticas estruturadas de monitoramento, gestão de incidentes e gestão de mudanças em TIC. Integram ainda suas atribuições a coordenação do atendimento técnico aos usuários, a execução das estratégias de segurança cibernética aplicadas à infraestrutura e aos serviços operados, com ações de prevenção, detecção e resposta a incidentes, e a condução de projetos estratégicos de engenharia e conectividade, alinhados ao planejamento institucional e voltados ao fortalecimento da infraestrutura nacional de ensino, pesquisa e inovação.

Dos Perfis:

AT – Analista de Atendimento JR

O papel desse profissional consiste nas seguintes atividades:

- Atendimento e registro das demandas que sejam feitas por telefone, e-mail ou chat através das ferramentas adotadas na operação, além do acompanhamento dos chamados registrados pelo cliente na ferramenta de tratativa de chamados;
- Análise da demanda em base de conhecimento e execução de testes junto ao usuário;
- Registro de todo atendimento realizado na ferramenta de chamados;
- Escalonamento dos chamados quando necessário;
- Encerramento do chamado junto ao cliente;
- Atendimento de demandas específicas sempre que indicadas pela coordenação.

Formação necessária para o profissional nesta função: cursando nível superior;

Horário de trabalho: Horário de trabalho: 36 horas semanais em formato de escala 24x7 ou horário comercial;

AT – Analista de Atendimento PL

O papel desse profissional consiste nas seguintes atividades:

- Atender e registrar as demandas que sejam feitas por telefone, e-mail ou chat através das ferramentas adotadas na operação, além do acompanhamento dos chamados registrados pelo cliente na ferramenta de tratativa de chamados;
- Analisar a demanda em base de conhecimento e execução de testes junto ao usuário;
- Registrar todo o atendimento realizado na ferramenta de chamados;
- Escalonar os chamados quando necessário;
- Fazer as tratativas de chamados pendentes na fila de atendimento do Service Desk;
- Fazer o encerramento do chamado junto ao cliente;
- Indicar e auxiliar na melhoria da base de conhecimento;

- Executar o Plano de Comunicação para Incidentes Críticos;
- Atender as demandas específicas sempre que indicadas pela coordenação.

Formação necessária para o profissional nesta função:

- Cursando nível superior;
- Certificação HDI – SCA;

Horário de trabalho: Horário de trabalho: 36 horas semanais em formato de escala 24x7 ou horário comercial;

AT – Analista de Atendimento SR

Responsável por manter os processos atualizados e fluindo em parceria com as equipes responsáveis pelos Serviços da RNP. É responsabilidade principal desse analista a manutenção (gestão, administração) da base de conhecimento do Service Desk, a passagem de conhecimento para toda a equipe de forma que esta esteja sempre atualizada em relação a possíveis alterações efetuadas e manter a Base de Conhecimento alinhada aos interesses dos donos (ou demandantes) dos Serviços. As atividades desse papel são:

- Auxiliar no atendimento de chamados sempre que requisitado;
- Atender as demandas escalonadas pelos Atendentes Genéricos ou Especializados;
- Acompanhar ou executar o Plano de Comunicação para Incidentes Críticos;
- Criar, atualizar, revisar e publicar itens na base de conhecimento;
- Programar ações preventivas e orientações periódicas aos técnicos da operação para eliminar falhas no atendimento;
- Identificar melhorias nos sistemas de gerenciamento e abertura de chamados;

Para cumprir essas atividades, os analistas serão alocados de acordo com a demanda mediante análise da coordenação.

Formação necessária para o profissional nesta função:

- Cursando nível superior;
- Certificação HDI – SCA;
- ITIL Foundation 4;

AT – Analista de Atendimento Especializado JR

O papel desse profissional consiste nas seguintes atividades:

- Atendimento e registro das demandas que sejam feitas por telefone, e-mail ou chat através das ferramentas adotadas na operação, além do acompanhamento dos chamados registrados pelo cliente na ferramenta de tratativa de chamados;
- Análise da demanda em base de conhecimento e execução de testes junto ao usuário;
- Registro de todo atendimento realizado na ferramenta de chamados;
- Escalonamento dos chamados quando necessário;
- Encerramento do chamado junto ao cliente;
- Atendimento de demandas específicas sempre que indicadas pela coordenação.

Formação necessária para o profissional nesta função: Nível superior;

AT – Analista de Atendimento Especializado PL

O papel desse profissional consiste nas seguintes atividades:

- Atender e registrar as demandas que sejam feitas por telefone, e-mail ou chat através das ferramentas adotadas na operação, além do acompanhamento dos chamados registrados pelo cliente na ferramenta de tratativa de chamados;
- Analisar a demanda em base de conhecimento e execução de testes junto ao usuário;
- Registrar todo o atendimento realizado na ferramenta de chamados;
- Escalonar os chamados quando necessário;
- Fazer as tratativas de chamados pendentes na fila de atendimento do Service Desk;
- Fazer o encerramento do chamado junto ao cliente;
- Indicar e auxiliar na melhoria da base de conhecimento;
- Executar o Plano de Comunicação para Incidentes Críticos;
- Atender as demandas específicas sempre que indicadas pela coordenação.

Formação necessária para o profissional nesta função:

- Nível superior;
- Certificação HDI – SCA;

Horário de trabalho: Horário de trabalho: 36 horas semanais em formato de escala 24x7 ou horário comercial;

AT – Analista de Atendimento Especializado SR

Responsável por manter os processos atualizados e fluindo em parceria com as equipes responsáveis pelos Serviços da RNP. É responsabilidade principal desse analista a manutenção (gestão, administração) da base de conhecimento do Service Desk, a passagem de conhecimento para toda a equipe de forma

que esta esteja sempre atualizada em relação a possíveis alterações efetuadas e manter a Base de Conhecimento alinhada aos interesses dos donos (ou demandantes) dos Serviços. As atividades desse papel são:

- Auxiliar no atendimento de chamados sempre que requisitado;
- Atender as demandas escalonadas pelos Atendentes Genéricos ou Especializados;
- Acompanhar ou executar o Plano de Comunicação para Incidentes Críticos;
- Criar, atualizar, revisar e publicar itens na base de conhecimento;
- Programar ações preventivas e orientações periódicas aos técnicos da operação para eliminar falhas no atendimento;
- Identificar melhorias nos sistemas de gerenciamento e abertura de chamados;

Para cumprir essas atividades, os analistas serão alocados de acordo com a demanda mediante análise da coordenação.

Formação necessária para o profissional nesta função:

- Nível superior;
- Certificação HDI – SCA;
- ITIL Foundation 4;

ACX – Analista de Experiência JR

O analista de Customer Experience JR é responsável por apoiar as iniciativas de melhoria da experiência do cliente na Gerência de Atendimento Integrado da RNP, auxiliando na coleta, organização e análise inicial de dados relacionados à satisfação e percepção dos usuários. Atua de forma operacional no suporte às ações de acompanhamento da jornada do cliente, sempre com o intuito de elevar o nível de satisfação de parceiros, equipe e clientes. São atividades dessa função:

- Apoiar o mapeamento da jornada do cliente (Customer Journey);
- Apoiar a consolidação de indicadores de experiência (NPS, CSAT, CES);
- Auxiliar na análise de pesquisas de satisfação respondidas;
- Apoiar a elaboração de relatórios periódicos de experiência;
- Identificar oportunidades de melhoria nos fluxos de atendimento;
- Apoiar ações de melhoria contínua relacionadas à experiência do usuário;
- Organizar e atualizar registros e bases de dados relacionadas à experiência do cliente.

Formação necessária para o profissional nesta função:

- Cursando nível superior;

ACX – Analista de Experiência PL

O analista de Customer Experience PL é responsável por identificar pontos de melhoria na jornada do cliente e na percepção dos serviços ofertados pela RNP, analisando indicadores de experiência e propondo ações estruturadas para aprimoramento dos processos de atendimento e operação. Atua de forma analítica e colaborativa junto às equipes técnicas e operacionais, sempre com o intuito de elevar o nível de satisfação de parceiros, equipe e clientes. São atividades dessa função:

- Mapear e revisar a jornada do cliente;
- Analisar indicadores de experiência (NPS, CSAT, CES e correlatos);
- Elaborar relatórios gerenciais e dashboards de acompanhamento;
- Identificar causas de insatisfação e propor planos de ação;
- Conduzir análises de causa-raiz relacionadas à experiência do cliente;
- Facilitar reuniões com áreas envolvidas para alinhamento de melhorias;
- Acompanhar a execução de planos de melhoria;

Formação necessária para o profissional nesta função:

- Graduação completa;

ACX – Analista de Experiência SR

O analista de Customer Experience SR é responsável por estruturar, conduzir e evoluir a estratégia de experiência do cliente na Gerência de Atendimento Integrado da RNP, promovendo integração entre áreas, consolidando indicadores estratégicos e propondo melhorias estruturantes nos serviços e processos. Atua de forma estratégica, garantindo visão integrada da jornada do cliente e apoiando a tomada de decisão institucional, sempre com o intuito de elevar o nível de satisfação de parceiros, equipe e clientes. São atividades dessa função:

- Liderar iniciativas estratégicas de melhoria da experiência do cliente;
- Estruturar e evoluir o modelo de governança de Customer Experience;
- Consolidar e analisar indicadores estratégicos de experiência;
- Conduzir análises aprofundadas de causa-raiz;
- Propor melhorias estruturantes em processos e serviços;
- Facilitar workshops e apresentações executivas;
- Apoiar a definição de metas institucionais relacionadas à experiência do cliente;
- Atuar como referência técnica em práticas de CX, Service Design e melhoria contínua.

Formação necessária para o profissional nesta função:

- Graduação completa;

ASV – Analista de Serviços JR

Responsável por manter os processos atualizados e fluindo em parceria com as equipes responsáveis pelos Serviços da RNP.

- É responsabilidade desse profissional agir para diminuição contínua do backlog de chamados abertos no Service Desk, que se encontrem em outros grupos solucionadores.
- Realiza a interface com grupos solucionadores para melhoria e evolução de processos e procedimentos utilizados para atendimento ao cliente da RNP.
- Apoia na estruturação da entrada de novos serviços para o atendimento.
- Auxiliar no atendimento aos tickets da Gestão de Mudanças de TIC da RNP, analisar datas e horários, verificar se formulário técnico se encontra de acordo, comunicar partes interessadas a respeito da manutenção, agendar comunicações internas e externas para clientes que utilizam os serviços fornecidos pela RNP.

Formação necessária para o profissional nesta função:

- Cursando nível superior;

ASV – Analista de Serviços PL

Responsável por apoiar a área em evoluções tecnológicas, automações e integrações.

Tem como atribuições elaborar melhorias para os sistemas utilizados internamente, propor formas de automação nas rotinas gerais e desenvolvimento de dashboards que deem visibilidade ao trabalho exercido pela área, seja utilizando de insumo as ferramentas de atendimento, de telefonia, de conhecimento, etc.

- Apoiar no desenvolvimento de tecnologias que auxiliem o dia a dia da operação;
- Construção e manutenção de chatbot;
- Integrações tecnológicas entre os sistemas utilizados na área;

Formação necessária para o profissional nesta função:

- Cursando nível superior;
- Certificação ITIL Foundation 4;

ASV – Analista de Serviços SR

Responsável por atuar na melhoria contínua das diversas frentes de processos e tecnologia dentro da Gerencia de Atendimento Integrado da RNP.

- Responsável por apoiar a área em evoluções tecnológicas.

- Tem como atribuições elaborar melhorias para os sistemas utilizados internamente, propor formas de automação nas rotinas gerais e desenvolvimento de dashboards que deem visibilidade ao trabalho exercido pela área, seja utilizando de insumo as ferramentas de atendimento, de telefonia, de conhecimento, etc.
- Responsável por manter os processos atualizados e fluindo em parceria com as equipes responsáveis pelos Serviços da RNP.
- Apoiar no desenvolvimento de tecnologias que auxiliem o dia a dia da operação sustentando a transformação digital dos processos e atividades;
- Integrações tecnológicas entre os sistemas utilizados na área;

Formação necessária para o profissional nesta função:

- Graduação completa;
- Certificação ITIL Foundation 4;
- Uma das seguintes certificações: Scrum (Exin/Alliance/Org), Lean IT, DevOps (Exin LPI Linux Essentials, LPIC-1 – Linux Administrator, LPIC-2 – Linux Engineer, CompTIA Linux+, Microsoft Certified Solutions Associate (MCSA), Microsoft Certified Solutions Expert (MCSE) e Microsoft Certified Solutions Developer (MCSD));

LID-02 – Supervisor de Atendimento e Experiência (CX) Júnior

Objetivo do cargo

Apoiar a liderança das frentes de Atendimento e de Experiência do Cliente (CX), acompanhando a operação diária e os indicadores para assegurar a qualidade do atendimento e a satisfação dos clientes, sob orientação da coordenação.

Responsabilidades

- Apoiar a supervisão da operação diária das equipes de Atendimento e de Experiência, acompanhando cobertura e aderência aos procedimentos.
- Acompanhar as filas e a distribuição de demandas, sinalizando desvios à coordenação.
- Acompanhar os indicadores de atendimento e de experiência.
- Atuar no primeiro nível de escalonamento e na comunicação de incidentes.
- Conduzir os rituais da equipe e apoiar a capacitação dos profissionais.
- Apoiar ações de melhoria dos fluxos de atendimento.

Requisitos

- Vivência em operação de atendimento.
- Noções de gestão de filas, SLA e indicadores de experiência do cliente.
- Boa comunicação, organização e foco na satisfação do cliente.

Formação

- Superior completo em áreas correlatas.
- Desejável pós-graduação em áreas correlatas.

LID-03 – Supervisor de Atendimento e Experiência (CX) Pleno

Objetivo do cargo

Liderar de forma autônoma as frentes de Atendimento e de Experiência do Cliente (CX), garantindo o cumprimento dos níveis de serviço, a qualidade do atendimento, a gestão da equipe e a evolução contínua da satisfação dos clientes.

Responsabilidades

- Supervisionar a operação diária das equipes de Atendimento e de Experiência, garantindo cobertura, cumprimento de SLA e aderência aos procedimentos.
- Gerir a escala, a distribuição de demandas e a priorização dos atendimentos.
- Atuar como ponto focal na condução e comunicação de incidentes críticos.
- Monitorar os indicadores de atendimento e de experiência e conduzir planos de ação para tratar desvios.
- Conduzir os rituais da equipe e apoiar a capacitação e o desenvolvimento dos profissionais.
- Apoiar a melhoria da jornada do cliente, transformando análises em melhorias nos fluxos de atendimento.
- Reportar periodicamente o desempenho das frentes, os riscos e as oportunidades de melhoria.

Requisitos

- Experiência em operação de atendimento e em liderança de equipes.
- Conhecimento de gestão de filas, SLA e indicadores de experiência do cliente.
- Boa capacidade de comunicação, organização, tomada de decisão e resolução de conflitos.
- Perfil de liderança e foco em resultados e na satisfação do cliente.

Formação

- Superior completo em áreas correlatas.
- Pós-graduação em áreas correlatas.

LID-04 – Supervisor de Atendimento e Experiência (CX) Sênior

Objetivo do cargo

Responder pela liderança e pela estratégia das frentes de Atendimento e de Experiência do Cliente (CX), conduzindo situações de maior complexidade e a evolução dos indicadores de satisfação, com autonomia e visão de resultado.

Responsabilidades

- Responder pela operação das frentes de Atendimento e de Experiência, garantindo cumprimento de SLA e qualidade do atendimento.
- Definir e conduzir a estratégia de experiência do cliente e os planos de melhoria contínua.
- Gerir a escala, a priorização e a alocação da equipe conforme volume e criticidade.
- Conduzir incidentes críticos e crises de maior impacto, atuando como principal ponto focal.
- Negociar alinhamentos complexos com diferentes áreas e parceiros.
- Responder pela evolução dos indicadores de atendimento e de satisfação, reportando desempenho, riscos e oportunidades.
- Desenvolver e orientar a equipe, atuando como referência de liderança.

Requisitos

- Experiência consolidada em operação de atendimento e em liderança de equipes.
- Domínio de gestão de filas, SLA e indicadores de experiência do cliente.
- Excelente comunicação, negociação, tomada de decisão sob pressão e resolução de conflitos.
- Perfil de liderança, mentoria e visão estratégica orientada a resultados.

Formação

- Superior completo em áreas correlatas.
- Pós-graduação completa em áreas correlatas.

AGP – Analista de Projetos JR

Tem como objetivo apoiar a GAI em termos de gestão de processos e projetos tanto internos quanto externos. Deve acompanhar o planejamento dos projetos, verificando escopo da proposta e monitorando os cronogramas, visando assegurar performance superior dos mesmos. Em conjunto com a equipe, deve efetuar planos de ação, através de observação e análise de problemas recorrentes, visando maximizar resultados de curto, médio e longo prazo, bem como:

- Acompanhar os planos de ação para melhoria de processos
- Apoiar a elaboração de modelos de dashboards utilizados para o controle e o acompanhamento da execução
- Conhecimento em gerenciamento de processos de negócio (BPM)
- Identificar e desenvolver metodologia, melhores práticas e padrões de gerenciamento de projetos;
- Direcionar os gerentes de projeto na utilização das melhores práticas de gerenciamento de projetos;
- Desenvolver e gerenciar políticas, procedimentos, formulários e outras documentações compartilhadas dos projetos (ativos de processos organizacionais);
- Esclarecer questionamentos e comunicar problemas de qualquer natureza que possam impactar na execução dos projetos;
- Manter-se atualizado sobre as inovações tecnológicas do segmento, buscando aperfeiçoamento dos recursos existentes, tendo em vista constante otimização e qualidade na realização do trabalho.
- Disponibilizar informações sobre atividades desenvolvidas, através de relatórios de status, visando fornecer informações sobre o andamento das rotinas dos projetos e subsídios para análise e tomada de decisões;

Formação necessária para o profissional nesta função:

- Cursando nível superior;

AGP – Analista de Projetos PL

Tem como objetivo apoiar a GAI em termos de gestão de processos e projetos tanto internos quanto externos. Deve acompanhar o planejamento dos projetos, verificando escopo da proposta e monitorando os cronogramas, visando assegurar performance superior dos mesmos.

Em conjunto com a equipe, deve efetuar planos de ação, através de observação e análise de problemas recorrentes, visando maximizar resultados de curto, médio e longo prazo, bem como:

- Acompanhar os planos de ação para melhoria de processos
- Apoiar a elaboração de modelos de dashboards utilizados para o controle e o acompanhamento da execução
- Conhecimento em gerenciamento de processos de negócio (BPM)

- Prover visibilidade sobre o desempenho dos projetos para a organização;
- Elaborar planejamentos e monitorar entregas, prazos, custos, riscos e qualidade;
- Direcionar os gerentes de projeto na utilização das melhores práticas de gerenciamento de projetos;
- Desenvolver e gerenciar políticas, procedimentos, formulários e outras documentações compartilhadas dos projetos (ativos de processos organizacionais);
- Apoiar o planejamento de atividades de implantação de projetos: analisar e definir escopo do projeto e serviço, prevendo seus impactos; analisar escopo do negócio; definir estratégia de desenvolvimento e necessidades de recursos humanos, materiais (infraestrutura) e recursos tecnológicos (software e hardware); estabelecer prioridades, prazos e custos de execução; elaborar propostas de projetos e serviços, estabelecendo acordo de nível de serviço, metas, política de segurança e pontos de controle; definir matriz de responsabilidades e padrões de desempenho e qualidade; elaborar orçamento;
- Esclarecer questionamentos e comunicar problemas de qualquer natureza que possam impactar na execução dos projetos;
- Manter-se atualizado sobre as inovações tecnológicas do segmento, buscando aperfeiçoamento dos recursos existentes, tendo em vista constante otimização e qualidade na realização do trabalho.
- Disponibilizar informações sobre atividades desenvolvidas, através de relatórios de status, visando fornecer informações sobre o andamento das rotinas dos projetos e subsídios para análise e tomada de decisões;

Formação necessária para o profissional nesta função:

- Graduação completa.

AGP – Analista de Projetos SR

Tem como objetivo apoiar a GAI em termos de gestão de processos e projetos tanto internos quanto externos. Deve acompanhar o planejamento dos projetos, verificando escopo da proposta e monitorando os cronogramas, visando assegurar performance superior dos mesmos.

Em conjunto com a equipe, deve efetuar planos de ação, através de observação e análise de problemas recorrentes, visando maximizar resultados de curto, médio e longo prazo, bem como:

- Acompanhar os planos de ação para melhoria de processos
- Apoiar a elaboração de modelos de dashboards utilizados para o controle e o acompanhamento da execução
- Conhecimento em gerenciamento de processos de negócio (BPM)
- Apoiar a gestão dos programas e projetos da Diretoria de Engenharia e Operações;
- Prover visibilidade sobre o desempenho dos projetos para a organização;

- Elaborar planejamentos e monitorar entregas, prazos, custos, riscos e qualidade;
- Identificar e desenvolver metodologia, melhores práticas e padrões de gerenciamento de projetos;
- Coordenar o desenvolvimento dos projetos de modo que os mesmos atendam os objetivos da empresa;
- Responsabilizar-se diretamente por tarefas que auxiliem a atingir metas acordadas;
- Direcionar os gerentes de projeto na utilização das melhores práticas de gerenciamento de projetos;
- Desenvolver e gerenciar políticas, procedimentos, formulários e outras documentações compartilhadas dos projetos (ativos de processos organizacionais);
- Apoiar o planejamento de atividades de implantação de projetos: analisar e definir escopo do projeto e serviço, prevendo seus impactos; analisar escopo do negócio; definir estratégia de desenvolvimento e necessidades de recursos humanos, materiais (infraestrutura) e recursos tecnológicos (software e hardware); estabelecer prioridades, prazos e custos de execução; elaborar propostas de projetos e serviços, estabelecendo acordo de nível de serviço, metas, política de segurança e pontos de controle; definir matriz de responsabilidades e padrões de desempenho e qualidade; elaborar orçamento;
- Elaborar níveis de serviços e de qualidade;
- Esclarecer questionamentos e comunicar problemas de qualquer natureza que possam impactar na execução dos projetos;
- Manter-se atualizado sobre as inovações tecnológicas do segmento, buscando aperfeiçoamento dos recursos existentes, tendo em vista constante otimização e qualidade na realização do trabalho.
- Planejar processos da área, verificando prazos e alinhando as atividades com a equipe, tendo em vista a garantia da organização e eficiência no direcionamento do trabalho;
- Disponibilizar informações sobre atividades desenvolvidas, através de relatórios de status, visando fornecer informações sobre o andamento das rotinas dos projetos e subsídios para análise e tomada de decisões;

Formação necessária para o profissional nesta função:

- Graduação completa;
- Cursando pós-graduação.

SEG-01.1 – Analista de Segurança da informação Nível 1 - JUNIOR

Resumo do Cargo:

Atuar no monitoramento e na operação de ferramentas de segurança, realizando triagem, análise e tratamento inicial de incidentes conforme playbooks e SLAs. É responsável pelo atendimento a clientes, registro e documentação de ocorrências, além da comunicação e escalonamento quando necessário. Também contribui para a melhoria contínua dos processos, geração de relatórios e apoio na

administração das soluções de segurança.

Requisitos de Formação:

- Estar cursando graduação em TI, Redes, Segurança da Informação ou áreas correlatas;
- Conhecimentos básicos em sistemas operacionais (Windows/Linux);
- Noções de redes e protocolos TCP/IP;
- Boa comunicação escrita e oral;

Responsabilidades:

- Monitoramento de ferramentas de segurança, com triagem inicial, classificação por severidade/impacto e priorização conforme regras de negócio
- Tratativa de incidentes disparados por alertas: validação, categorização, contenção inicial, comunicação ao cliente e escalonamento conforme playbook e SLA
- Tratativa de incidentes reportados por clientes: registro, qualificação do cenário, verificação técnica, orientação imediata e abertura de investigação formal
- Abertura de chamados multicanal (telefone/mensagens/e-mail) com coleta dos dados mínimos (quem, quando, o quê, impacto), categorização e definição do SLA
- Execução do atendimento: diagnóstico, ações acordadas, atualização contínua do status, registro de evidências e alinhamento com o solicitante
- Encerramento com validação da solução, documentação sucinta (causa/ação/resultado), lições aprendidas quando cabível e notificação formal ao cliente
- Engenharia/operacionalização de ferramentas de segurança: configuração, hardening, atualização, health checks, tuning contínuo e gestão de capacidade
- Execução conforme processo definido, registro de desvios e proposta de melhorias contínuas com atualização controlada
- Elaboração de relatórios periódicos (operacionais e executivos) com tendências, principais incidentes e recomendações
- Coleta, saneamento e automação de métricas nas plataformas, assegurando integridade e consistência dos dados que abastecem painéis e relatório

SEG-02.1 – Analista de Segurança da Informação Nível 2 – JUNIOR**Resumo do Cargo:**

Atuar na operação de segurança com foco em padronização e qualidade dos processos, executando o monitoramento e a tratativa de incidentes conforme SLAs e boas práticas de ITIL. Além da atuação técnica, é responsável pela elaboração, atualização e versionamento de playbooks, garantindo organização, rastreabilidade e melhoria contínua da operação. Contribui para a eficiência do SOC por

meio de relatórios, métricas e suporte na evolução das ferramentas de segurança.

Requisitos de Formação:

- Graduação em andamento em TI, Redes, Segurança da Informação ou áreas correlatas;
- Experiência prévia em SOC, suporte ou operação de ferramentas de segurança;
- Conhecimento de ITIL Foundation;
- Capacidade de elaboração e manutenção de playbooks;

Responsabilidades:

- Monitoramento de ferramentas de segurança, com triagem inicial, classificação por severidade/impacto e priorização conforme regras de negócio
- Tratativa de incidentes disparados por alertas: validação, categorização, contenção inicial, comunicação ao cliente e escalonamento conforme playbook e SLA
- Tratativa de incidentes reportados por clientes: registro, qualificação do cenário, verificação técnica, orientação imediata e abertura de investigação formal
- Abertura de chamados multicanal (telefone/mensagens/e-mail) com coleta dos dados mínimos (quem, quando, o quê, impacto), categorização e definição do SLA
- Execução do atendimento: diagnóstico, ações acordadas, atualização contínua do status, registro de evidências e alinhamento com o solicitante
- Encerramento com validação da solução, documentação sucinta (causa/ação/resultado), lições aprendidas quando cabível e notificação formal ao cliente
- Engenharia/operacionalização de ferramentas de segurança: configuração, hardening, atualização, health checks, tuning contínuo e gestão de capacidade
- Execução conforme processo definido, registro de desvios e proposta de melhorias contínuas com atualização controlada
- Elaboração de relatórios periódicos (operacionais e executivos) com tendências, principais incidentes e recomendações
- Coleta, saneamento e automação de métricas nas plataformas, assegurando integridade e consistência dos dados que abastecem painéis e relatório
- Criação e versionamento de playbooks/runbooks por tipo de incidente, com pré-requisitos, passos, responsáveis, critérios de saída e comunicação

SEG-03.1 – Analista de Segurança da Informação Nível 3 – JUNIOR**Resumo do Cargo:**

Analista responsável por apoiar a operação de segurança no monitoramento e na tratativa de incidentes, seguindo processos e SLAs definidos. Atua na documentação técnica, atualização de playbooks e geração de relatórios, contribuindo para a organização e padronização da operação. Tem papel fundamental na

sustentação das ferramentas de segurança e na qualidade dos registros e evidências.

Requisitos de Formação:

- Graduação em andamento ou concluída em TI, Redes, Segurança da Informação ou áreas afins;
- Experiência em monitoramento e tratativa de incidentes de segurança;
- Conhecimento em elaboração de documentação técnica;

Responsabilidades:

- Monitoramento de ferramentas de segurança, com triagem inicial, classificação por severidade/impacto e priorização conforme regras de negócio
- Tratativa de incidentes disparados por alertas: validação, categorização, contenção inicial, comunicação ao cliente e escalonamento conforme playbook e SLA
- Tratativa de incidentes reportados por clientes: registro, qualificação do cenário, verificação técnica, orientação imediata e abertura de investigação formal
- Abertura de chamados multicanal (telefone/mensagens/e-mail) com coleta dos dados mínimos (quem, quando, o quê, impacto), categorização e definição do SLA
- Execução do atendimento: diagnóstico, ações acordadas, atualização contínua do status, registro de evidências e alinhamento com o solicitante
- Encerramento com validação da solução, documentação sucinta (causa/ação/resultado), lições aprendidas quando cabível e notificação formal ao cliente
- Engenharia/operacionalização de ferramentas de segurança: configuração, hardening, atualização, health checks, tuning contínuo e gestão de capacidade
- Execução conforme processo definido, registro de desvios e proposta de melhorias contínuas com atualização controlada
- Elaboração de relatórios periódicos (operacionais e executivos) com tendências, principais incidentes e recomendações
- Coleta, saneamento e automação de métricas nas plataformas, assegurando integridade e consistência dos dados que abastecem painéis e relatório
- Criação e versionamento de playbooks/runbooks por tipo de incidente, com pré-requisitos, passos, responsáveis, critérios de saída e comunicação
- Documentação de arquitetura e procedimentos para clientes, com controle de versão, repositório central e revisão periódica

SEG-01.2 – Analista de Segurança da informação Nível 1 – PLENO**Resumo do Cargo:**

Atuar no monitoramento e na gestão de incidentes de segurança em ambiente de SOC, conduzindo análises, tratativas técnicas e escalonamentos conforme SLA. É responsável também pela gestão de tickets junto a fabricantes, documentação de processos (playbooks e arquitetura) e elaboração de relatórios executivos. Contribui para a melhoria contínua das operações, assegurando qualidade, rastreabilidade e evolução dos controles de segurança.

Requisitos de Formação:

- Graduação completa em TI, Redes, Segurança da Informação ou áreas relacionadas;
- Experiência comprovada em SOC ou gestão de incidentes de segurança;
- Conhecimento em abertura e acompanhamento de tickets junto a fabricantes/provedores;

Responsabilidades:

- Monitoramento de ferramentas de segurança, com triagem inicial, classificação por severidade/impacto e priorização conforme regras de negócio
- Tratativa de incidentes disparados por alertas: validação, categorização, contenção inicial, comunicação ao cliente e escalonamento conforme playbook e SLA
- Tratativa de incidentes reportados por clientes: registro, qualificação do cenário, verificação técnica, orientação imediata e abertura de investigação formal
- Abertura de chamados multicanal (telefone/mensagens/e-mail) com coleta dos dados mínimos (quem, quando, o quê, impacto), categorização e definição do SLA
- Execução do atendimento: diagnóstico, ações acordadas, atualização contínua do status, registro de evidências e alinhamento com o solicitante
- Encerramento com validação da solução, documentação sucinta (causa/ação/resultado), lições aprendidas quando cabível e notificação formal ao cliente
- Engenharia/operacionalização de ferramentas de segurança: configuração, hardening, atualização, health checks, tuning contínuo e gestão de capacidade
- Abertura e gestão de tickets com fabricantes/provedores: coleta de logs, acompanhamento de prazos, validação de correções e retorno consolidado ao cliente
- Execução conforme processo definido, registro de desvios e proposta de melhorias contínuas com atualização controlada
- Elaboração de relatórios periódicos (operacionais e executivos) com tendências, principais incidentes e recomendações
- Coleta, saneamento e automação de métricas nas plataformas, assegurando integridade e consistência dos dados que abastecem painéis e relatório
- Criação e versionamento de playbooks/runbooks por tipo de incidente, com pré-requisitos, passos, responsáveis, critérios de saída e comunicação

- Documentação de arquitetura e procedimentos para clientes, com controle de versão, repositório central e revisão periódica

SEG-02.2 - Analista de Segurança da Informação Nível 2 - PLENO

Resumo do Cargo:

Profissional com atuação avançada em threat hunting e resposta a incidentes, responsável por identificar ameaças de forma proativa e conduzir investigações técnicas aprofundadas. Trabalha com base em frameworks como NIST e MITRE ATT&CK para fortalecer a capacidade de detecção e resposta do SOC. Também contribui para a melhoria contínua dos processos, documentação técnica e evolução das ferramentas de segurança.

Requisitos de Formação:

- Graduação completa em áreas de TI ou Segurança;
- Experiência sólida em threat hunting, investigações e resposta a incidentes;
- Conhecimento em frameworks de segurança (NIST, MITRE ATT&CK);

Responsabilidades:

- Monitoramento de ferramentas de segurança, com triagem inicial, classificação por severidade/impacto e priorização conforme regras de negócio
- Tratativa de incidentes disparados por alertas: validação, categorização, contenção inicial, comunicação ao cliente e escalonamento conforme playbook e SLA
- Threat hunting e investigações proativas com hipóteses orientadas a TTPs/IOCs, varredura em telemetrias, identificação de anomalias e abertura de incidentes quando aplicável
- Tratativa de incidentes reportados por clientes: registro, qualificação do cenário, verificação técnica, orientação imediata e abertura de investigação formal
- Abertura de chamados multicanal (telefone/mensagens/e-mail) com coleta dos dados mínimos (quem, quando, o quê, impacto), categorização e definição do SLA
- Execução do atendimento: diagnóstico, ações acordadas, atualização contínua do status, registro de evidências e alinhamento com o solicitante
- Encerramento com validação da solução, documentação sucinta (causa/ação/resultados), lições aprendidas quando cabível e notificação formal ao cliente
- Engenharia/operacionalização de ferramentas de segurança: configuração, hardening, atualização, health checks, tuning contínuo e gestão de capacidade
- Abertura e gestão de tickets com fabricantes/provedores: coleta de logs, acompanhamento de prazos, validação de correções e retorno consolidado ao cliente
- Execução conforme processo definido, registro de desvios e proposta de melhorias contínuas com atualização controlada

- Elaboração de relatórios periódicos (operacionais e executivos) com tendências, principais incidentes e recomendações
- Coleta, saneamento e automação de métricas nas plataformas, assegurando integridade e consistência dos dados que abastecem painéis e relatório
- Criação e versionamento de playbooks/runbooks por tipo de incidente, com pré-requisitos, passos, responsáveis, critérios de saída e comunicação
- Documentação de arquitetura e procedimentos para clientes, com controle de versão, repositório central e revisão periódica

SEG-03.2 - Analista de Segurança da Informação Nível 3 - PLENO

Resumo do Cargo:

Analista pleno com atuação técnica focada na análise aprofundada de incidentes e no aprimoramento contínuo das capacidades de detecção do SOC. Responsável por desenvolver e otimizar regras em SIEM/SOAR, realizar threat hunting e reduzir falsos positivos por meio de tuning e ajustes avançados. Contribui diretamente para a eficiência operacional e para o aumento da maturidade técnica da operação de segurança.

Requisitos de Formação:

- Graduação completa em áreas de TI ou Segurança da Informação;
- Experiência avançada em análise de incidentes e desenvolvimento de detecções;
- Vivência em ajustes e otimização de regras de segurança em SIEM/SOAR;

Responsabilidades:

- Monitoramento de ferramentas de segurança, com triagem inicial, classificação por severidade/impacto e priorização conforme regras de negócio
- Tratativa de incidentes disparados por alertas: validação, categorização, contenção inicial, comunicação ao cliente e escalonamento conforme playbook e SLA
- Threat hunting e investigações proativas com hipóteses orientadas a TTPs/IOCs, varredura em telemetrias, identificação de anomalias e abertura de incidentes quando aplicável
- Tratativa de incidentes reportados por clientes: registro, qualificação do cenário, verificação técnica, orientação imediata e abertura de investigação formal
- Abertura de chamados multicanal (telefone/mensagens/e-mail) com coleta dos dados mínimos (quem, quando, o quê, impacto), categorização e definição do SLA
- Execução do atendimento: diagnóstico, ações acordadas, atualização contínua do status, registro de evidências e alinhamento com o solicitante
- Encerramento com validação da solução, documentação sucinta (causa/ação/resultados), lições aprendidas quando cabível e notificação formal ao cliente

- Engenharia/operacionalização de ferramentas de segurança: configuração, hardening, atualização, health checks, tuning contínuo e gestão de capacidade
- Abertura e gestão de tickets com fabricantes/provedores: coleta de logs, acompanhamento de prazos, validação de correções e retorno consolidado ao cliente
- Execução conforme processo definido, registro de desvios e proposta de melhorias contínuas com atualização controlada
- Elaboração de relatórios periódicos (operacionais e executivos) com tendências, principais incidentes e recomendações
- Coleta, saneamento e automação de métricas nas plataformas, assegurando integridade e consistência dos dados que abastecem painéis e relatório
- Desenvolvimento e tuning de detecções mapeadas ao MITRE ATT&CK, com teste, avaliação de precisão e redução de falsos positivos
- Criação e versionamento de playbooks/runbooks por tipo de incidente, com pré-requisitos, passos, responsáveis, critérios de saída e comunicação
- Documentação de arquitetura e procedimentos para clientes, com controle de versão, repositório central e revisão periódica.

SEG-01.3 – Analista de Segurança da informação Nível 1 – SENIOR

Resumo do Cargo:

Profissional responsável por atuar como referência técnica na condução de incidentes de alta complexidade, realizando investigações aprofundadas, threat hunting e aprimoramento contínuo das detecções. Atua na estruturação e governança dos processos de segurança, definindo fluxos, SLAs e boas práticas. Tem papel estratégico na elevação da maturidade do SOC e na melhoria da efetividade das respostas a incidentes.

Requisitos de Formação:

- Graduação completa em TI, Redes ou Segurança da Informação;
- Experiência avançada em gestão de incidentes complexos e processos de segurança;
- Conhecimento em definição de SLAs, fluxos de processos e governança de segurança;

Responsabilidades:

- Monitoramento de ferramentas de segurança, com triagem inicial, classificação por severidade/impacto e priorização conforme regras de negócio
- Tratativa de incidentes disparados por alertas: validação, categorização, contenção inicial, comunicação ao cliente e escalonamento conforme playbook e SLA
- Threat hunting e investigações proativas com hipóteses orientadas a TTPs/IOCs, varredura em telemetrias, identificação de anomalias e abertura de incidentes quando aplicável

- Tratativa de incidentes reportados por clientes: registro, qualificação do cenário, verificação técnica, orientação imediata e abertura de investigação formal
- Abertura de chamados multicanal (telefone/mensagens/e-mail) com coleta dos dados mínimos (quem, quando, o quê, impacto), categorização e definição do SLA
- Execução do atendimento: diagnóstico, ações acordadas, atualização contínua do status, registro de evidências e alinhamento com o solicitante
- Encerramento com validação da solução, documentação sucinta (causa/ação/resultado), lições aprendidas quando cabível e notificação formal ao cliente
- Engenharia/operacionalização de ferramentas de segurança: configuração, hardening, atualização, health checks, tuning contínuo e gestão de capacidade
- Abertura e gestão de tickets com fabricantes/provedores: coleta de logs, acompanhamento de prazos, validação de correções e retorno consolidado ao cliente
- Codificação/ajuste de processos com foco em segurança: fluxos, papéis e responsabilidades (RACI), SLAs, canais de comunicação e critérios de severidade
- Execução conforme processo definido, registro de desvios e proposta de melhorias contínuas com atualização controlada
- Elaboração de relatórios periódicos (operacionais e executivos) com tendências, principais incidentes e recomendações
- Coleta, saneamento e automação de métricas nas plataformas, assegurando integridade e consistência dos dados que abastecem painéis e relatório
- Desenvolvimento e tuning de detecções mapeadas ao MITRE ATT&CK, com teste, avaliação de precisão e redução de falsos positivos
- Criação e versionamento de playbooks/runbooks por tipo de incidente, com pré-requisitos, passos, responsáveis, critérios de saída e comunicação
- Documentação de arquitetura e procedimentos para clientes, com controle de versão, repositório central e revisão periódica

SEG-02.3 – Analista de Segurança da Informação Nível 2 – SENIOR

Resumo do Cargo:

Analista Sênior com atuação estratégica e técnica na implantação e evolução de soluções de segurança, incluindo desenho de arquitetura, integrações e migrações. Conduz investigações avançadas, threat hunting e desenvolvimento de detecções, além de apoiar a gestão de projetos e times. Tem papel relevante na estruturação de processos, governança e amadurecimento contínuo da operação de segurança.

Requisitos de Formação:

- Graduação completa em TI ou Segurança da Informação;

- Experiência consolidada em implantação de ferramentas de segurança (arquitetura, integração, migração);
- Atuação prévia em gestão de equipes ou projetos de segurança;

Responsabilidades:

- Monitoramento de ferramentas de segurança, com triagem inicial, classificação por severidade/impacto e priorização conforme regras de negócio
- Tratativa de incidentes disparados por alertas: validação, categorização, contenção inicial, comunicação ao cliente e escalonamento conforme playbook e SLA
- Threat hunting e investigações proativas com hipóteses orientadas a TTPs/IOCs, varredura em telemetrias, identificação de anomalias e abertura de incidentes quando aplicável
- Tratativa de incidentes reportados por clientes: registro, qualificação do cenário, verificação técnica, orientação imediata e abertura de investigação formal
- Abertura de chamados multicanal (telefone/mensagens/e-mail) com coleta dos dados mínimos (quem, quando, o quê, impacto), categorização e definição do SLA
- Execução do atendimento: diagnóstico, ações acordadas, atualização contínua do status, registro de evidências e alinhamento com o solicitante
- Encerramento com validação da solução, documentação sucinta (causa/ação/resultado), lições aprendidas quando cabível e notificação formal ao cliente
- Engenharia/operacionalização de ferramentas de segurança: configuração, hardening, atualização, health checks, tuning contínuo e gestão de capacidade
- Abertura e gestão de tickets com fabricantes/provedores: coleta de logs, acompanhamento de prazos, validação de correções e retorno consolidado ao cliente
- Planejamento e execução de implantação de ferramentas: desenho de arquitetura, integrações, migrações, testes, aceitação (UAT) e handover para operação.
- Codificação/ajuste de processos com foco em segurança: fluxos, papéis e responsabilidades (RACI), SLAs, canais de comunicação e critérios de severidade
- Execução conforme processo definido, registro de desvios e proposta de melhorias contínuas com atualização controlada
- Elaboração de relatórios periódicos (operacionais e executivos) com tendências, principais incidentes e recomendações
- Coleta, saneamento e automação de métricas nas plataformas, assegurando integridade e consistência dos dados que abastecem painéis e relatório
- Desenvolvimento e tuning de detecções mapeadas ao MITRE ATT&CK, com teste, avaliação de precisão e redução de falsos positivos
- Criação e versionamento de playbooks/runbooks por tipo de incidente, com pré-requisitos, passos, responsáveis, critérios de saída e comunicação

- Documentação de arquitetura e procedimentos para clientes, com controle de versão, repositório central e revisão periódica

SEG-03.3 – Analista de Segurança da Informação Nível 3 – SENIOR

Resumo do Cargo:

Analista sênior com atuação estratégica na condução e liderança de projetos de segurança, incluindo avaliação e implantação de novas soluções com foco em riscos, compliance e integração. Atua na gestão de incidentes complexos, desenvolvimento de detecções e estruturação de processos, apoiando a governança e a tomada de decisão. Tem papel central no planejamento técnico, na evolução da arquitetura de segurança e no amadurecimento da operação.

Requisitos de Formação:

- Graduação completa em TI, Segurança da Informação ou áreas afins;
- Experiência estratégica em avaliação de soluções de segurança, compliance e gestão de riscos;
- Forte atuação em planejamento e liderança de projetos de segurança;

Responsabilidades:

- Monitoramento de ferramentas de segurança, com triagem inicial, classificação por severidade/impacto e priorização conforme regras de negócio
- Tratativa de incidentes disparados por alertas: validação, categorização, contenção inicial, comunicação ao cliente e escalonamento conforme playbook e SLA
- Threat hunting e investigações proativas com hipóteses orientadas a TTPs/IOCs, varredura em telemetrias, identificação de anomalias e abertura de incidentes quando aplicável
- Tratativa de incidentes reportados por clientes: registro, qualificação do cenário, verificação técnica, orientação imediata e abertura de investigação formal
- Abertura de chamados multicanal (telefone/mensagens/e-mail) com coleta dos dados mínimos (quem, quando, o quê, impacto), categorização e definição do SLA
- Execução do atendimento: diagnóstico, ações acordadas, atualização contínua do status, registro de evidências e alinhamento com o solicitante
- Encerramento com validação da solução, documentação sucinta (causa/ação/resultado), lições aprendidas quando cabível e notificação formal ao cliente
- Engenharia/operacionalização de ferramentas de segurança: configuração, hardening, atualização, health checks, tuning contínuo e gestão de capacidade
- Abertura e gestão de tickets com fabricantes/provedores: coleta de logs, acompanhamento de prazos, validação de correções e retorno consolidado ao cliente

- Avaliação técnica de novas soluções com critérios de sucesso, riscos, custos, integração e compliance
- Planejamento e execução de implantação de ferramentas: desenho de arquitetura, integrações, migrações, testes, aceitação (UAT) e handover para operação.
- Codificação/ajuste de processos com foco em segurança: fluxos, papéis e responsabilidades (RACI), SLAs, canais de comunicação e critérios de severidade
- Execução conforme processo definido, registro de desvios e proposta de melhorias contínuas com atualização controlada
- Elaboração de relatórios periódicos (operacionais e executivos) com tendências, principais incidentes e recomendações
- Coleta, saneamento e automação de métricas nas plataformas, assegurando integridade e consistência dos dados que abastecem painéis e relatório
- Desenvolvimento e tuning de detecções mapeadas ao MITRE ATT&CK, com teste, avaliação de precisão e redução de falsos positivos
- Criação e versionamento de playbooks/runbooks por tipo de incidente, com pré-requisitos, passos, responsáveis, critérios de saída e comunicação
- Documentação de arquitetura e procedimentos para clientes, com controle de versão, repositório central e revisão periódica.

SEG-03.4 - Analista de Segurança da Informação Nível 1 - ESPECIALISTA

Resumo do Cargo:

Profissional com atuação estratégica e forte profundidade técnica, responsável por avaliar, implantar e evoluir soluções de segurança com foco em risco e compliance. Atua como referência técnica para o time, apoiando decisões arquiteturais e o desenvolvimento de capacidades avançadas de detecção e resposta. Contribui diretamente para a padronização, governança e amadurecimento da operação.

Requisitos de Formação:

- Graduação completa em TI, Segurança da Informação ou áreas afins;
- Pós-graduação ou especialização em Segurança da Informação, Gestão de Riscos ou áreas correlatas;
- Desejável Certificação de segurança reconhecida (ex: ISO 27001, Security+, CySA+, ou equivalente);
- Experiência estratégica em avaliação de soluções de segurança, compliance e gestão de riscos;
- Forte atuação em planejamento e liderança de projetos de segurança;

Responsabilidades:

- Monitoramento de ferramentas de segurança, com triagem inicial, classificação por severidade/impacto e priorização conforme regras de negócio
- Tratativa de incidentes disparados por alertas: validação, categorização, contenção inicial, comunicação ao cliente e escalonamento conforme playbook e SLA
- Threat hunting e investigações proativas com hipóteses orientadas a TTPs/IOCs, varredura em telemetrias, identificação de anomalias e abertura de incidentes quando aplicável
- Tratativa de incidentes reportados por clientes: registro, qualificação do cenário, verificação técnica, orientação imediata e abertura de investigação formal
- Abertura de chamados multicanal (telefone/mensagens/e-mail) com coleta dos dados mínimos (quem, quando, o quê, impacto), categorização e definição do SLA
- Execução do atendimento: diagnóstico, ações acordadas, atualização contínua do status, registro de evidências e alinhamento com o solicitante
- Encerramento com validação da solução, documentação sucinta (causa/ação/resultado), lições aprendidas quando cabível e notificação formal ao cliente
- Engenharia/operacionalização de ferramentas de segurança: configuração, hardening, atualização, health checks, tuning contínuo e gestão de capacidade
- Abertura e gestão de tickets com fabricantes/provedores: coleta de logs, acompanhamento de prazos, validação de correções e retorno consolidado ao cliente
- Avaliação técnica de novas soluções com critérios de sucesso, riscos, custos, integração e compliance
- Planejamento e execução de implantação de ferramentas: desenho de arquitetura, integrações, migrações, testes, aceitação (UAT) e handover para operação.
- Codificação/ajuste de processos com foco em segurança: fluxos, papéis e responsabilidades (RACI), SLAs, canais de comunicação e critérios de severidade
- Execução conforme processo definido, registro de desvios e proposta de melhorias contínuas com atualização controlada
- Elaboração de relatórios periódicos (operacionais e executivos) com tendências, principais incidentes e recomendações
- Coleta, saneamento e automação de métricas nas plataformas, assegurando integridade e consistência dos dados que abastecem painéis e relatório
- Desenvolvimento e tuning de detecções mapeadas ao MITRE ATT&CK, com teste, avaliação de precisão e redução de falsos positivos
- Criação e versionamento de playbooks/runbooks por tipo de incidente, com pré-requisitos, passos, responsáveis, critérios de saída e comunicação
- Documentação de arquitetura e procedimentos para clientes, com controle de versão, repositório central e revisão periódica.

- Atuação como referência técnica para analistas seniores em temas específicos de segurança;

SEG-03.5 - Analista de Segurança da Informação Nível 2 - ESPECIALISTA

Resumo do Cargo:

Especialista com liderança técnica consolidada, responsável por conduzir projetos estratégicos de grande porte e orientar tecnicamente equipes em iniciativas críticas de segurança. Atua na avaliação de soluções complexas, definição de diretrizes e fortalecimento da governança. Tem papel decisivo na evolução da arquitetura de segurança e na mitigação de riscos institucionais.

Requisitos de Formação:

- Graduação completa em TI, Segurança da Informação ou áreas afins;
- Pós-graduação ou especialização em Segurança da Informação, Gestão de Riscos ou áreas correlatas;
- Desejável Certificação avançada (ex: CISSP, CISM, CISA, CCSP ou equivalente);
- Experiência estratégica em avaliação de soluções de segurança, compliance e gestão de riscos;
- Forte atuação em planejamento e liderança de projetos de segurança;

Responsabilidades:

- Monitoramento de ferramentas de segurança, com triagem inicial, classificação por severidade/impacto e priorização conforme regras de negócio
- Tratativa de incidentes disparados por alertas: validação, categorização, contenção inicial, comunicação ao cliente e escalonamento conforme playbook e SLA
- Threat hunting e investigações proativas com hipóteses orientadas a TTPs/IOCs, varredura em telemetrias, identificação de anomalias e abertura de incidentes quando aplicável
- Tratativa de incidentes reportados por clientes: registro, qualificação do cenário, verificação técnica, orientação imediata e abertura de investigação formal
- Abertura de chamados multicanal (telefone/mensagens/e-mail) com coleta dos dados mínimos (quem, quando, o quê, impacto), categorização e definição do SLA
- Execução do atendimento: diagnóstico, ações acordadas, atualização contínua do status, registro de evidências e alinhamento com o solicitante
- Encerramento com validação da solução, documentação sucinta (causa/ação/resultado), lições aprendidas quando cabível e notificação formal ao cliente
- Engenharia/operacionalização de ferramentas de segurança: configuração, hardening, atualização, health checks, tuning contínuo e gestão de capacidade

- Abertura e gestão de tickets com fabricantes/provedores: coleta de logs, acompanhamento de prazos, validação de correções e retorno consolidado ao cliente
- Avaliação técnica de novas soluções com critérios de sucesso, riscos, custos, integração e compliance
- Planejamento e execução de implantação de ferramentas: desenho de arquitetura, integrações, migrações, testes, aceitação (UAT) e handover para operação.
- Codificação/ajuste de processos com foco em segurança: fluxos, papéis e responsabilidades (RACI), SLAs, canais de comunicação e critérios de severidade
- Execução conforme processo definido, registro de desvios e proposta de melhorias contínuas com atualização controlada
- Elaboração de relatórios periódicos (operacionais e executivos) com tendências, principais incidentes e recomendações
- Coleta, saneamento e automação de métricas nas plataformas, assegurando integridade e consistência dos dados que abastecem painéis e relatório
- Desenvolvimento e tuning de detecções mapeadas ao MITRE ATT&CK, com teste, avaliação de precisão e redução de falsos positivos
- Criação e versionamento de playbooks/runbooks por tipo de incidente, com pré-requisitos, passos, responsáveis, critérios de saída e comunicação
- Documentação de arquitetura e procedimentos para clientes, com controle de versão, repositório central e revisão periódica.
- Atuação como referência técnica para analistas seniores em temas específicos de segurança;
- Liderança técnica de projetos estratégicos de grande porte;

SEG-03.5 - Analista de Segurança da Informação Nível 3 - ESPECIALISTA

Resumo do Cargo:

Autoridade técnica máxima na área de segurança, responsável por decisões estratégicas críticas, direcionamento arquitetural e definição de padrões corporativos. Lidera iniciativas estruturantes de alto impacto, alinhando segurança ao negócio e à gestão de riscos. Atua como principal referência institucional em temas avançados de segurança da informação.

Requisitos de Formação:

- Graduação completa em TI, Segurança da Informação ou áreas afins;
- Pós-graduação ou especialização em Segurança da Informação, Gestão de Riscos ou áreas correlatas;
- Desejável Certificação (ex: CISSP, CISM, CISA, CCSP ou equivalente);

- Experiência estratégica em avaliação de soluções de segurança, compliance e gestão de riscos;
- Forte atuação em planejamento e liderança de projetos de segurança;

Responsabilidades:

- Monitoramento de ferramentas de segurança, com triagem inicial, classificação por severidade/impacto e priorização conforme regras de negócio
- Tratativa de incidentes disparados por alertas: validação, categorização, contenção inicial, comunicação ao cliente e escalonamento conforme playbook e SLA
- Threat hunting e investigações proativas com hipóteses orientadas a TTPs/IOCs, varredura em telemetrias, identificação de anomalias e abertura de incidentes quando aplicável
- Tratativa de incidentes reportados por clientes: registro, qualificação do cenário, verificação técnica, orientação imediata e abertura de investigação formal
- Abertura de chamados multicanal (telefone/mensagens/e-mail) com coleta dos dados mínimos (quem, quando, o quê, impacto), categorização e definição do SLA
- Execução do atendimento: diagnóstico, ações acordadas, atualização contínua do status, registro de evidências e alinhamento com o solicitante
- Encerramento com validação da solução, documentação sucinta (causa/ação/resultados), lições aprendidas quando cabível e notificação formal ao cliente
- Engenharia/operacionalização de ferramentas de segurança: configuração, hardening, atualização, health checks, tuning contínuo e gestão de capacidade
- Abertura e gestão de tickets com fabricantes/provedores: coleta de logs, acompanhamento de prazos, validação de correções e retorno consolidado ao cliente
- Avaliação técnica de novas soluções com critérios de sucesso, riscos, custos, integração e compliance
- Planejamento e execução de implantação de ferramentas: desenho de arquitetura, integrações, migrações, testes, aceitação (UAT) e handover para operação.
- Codificação/ajuste de processos com foco em segurança: fluxos, papéis e responsabilidades (RACI), SLAs, canais de comunicação e critérios de severidade
- Execução conforme processo definido, registro de desvios e proposta de melhorias contínuas com atualização controlada
- Elaboração de relatórios periódicos (operacionais e executivos) com tendências, principais incidentes e recomendações
- Coleta, saneamento e automação de métricas nas plataformas, assegurando integridade e consistência dos dados que abastecem painéis e relatório
- Desenvolvimento e tuning de detecções mapeadas ao MITRE ATT&CK, com teste, avaliação de precisão e redução de falsos positivos

- Criação e versionamento de playbooks/runbooks por tipo de incidente, com pré-requisitos, passos, responsáveis, critérios de saída e comunicação
- Documentação de arquitetura e procedimentos para clientes, com controle de versão, repositório central e revisão periódica.
- Atuação como autoridade técnica máxima em decisões críticas de segurança;
- Liderança técnica de projetos estratégicos de grande porte;

SEG-03.6 - Líder Técnico de Segurança – Nível 1 - OPERAÇÃO

Resumo do Cargo:

Responsável por coordenar tecnicamente a rotina operacional do SOC, garantindo qualidade nas análises, aderência a SLAs e padronização dos processos. Atua como ponto focal técnico da equipe, apoiando investigações e promovendo melhorias contínuas na operação. Tem foco direto na estabilidade, eficiência e organização do dia a dia operacional.

Requisitos de Formação:

- Ensino superior completo em Redes de Computadores, Segurança da Informação, Ciência da Computação, Sistemas de Informação ou áreas correlatas;
- Pós-graduação em Gestão ou Segurança da Informação será considerada um diferencial;
- Experiência sólida em operações de SOC (Security Operations Center) e resposta a incidentes de segurança da informação;
- Conhecimentos avançados em redes, segurança, monitoramento e arquitetura de sistemas de segurança;
- Vivência prática com ferramentas como SIEM (Google SecOps, QRadar, entre outras), Anti-DDoS, WAF, XDR, IDS/IPS;
- Familiaridade com frameworks e boas práticas de segurança da informação, como MITRE ATT&CK, NIST, CIS Controls, entre outros;
- Habilidade na elaboração de relatórios técnicos e documentação especializada;
- Desejável experiência prévia em liderança técnica.

Responsabilidades:

- Liderar tecnicamente a equipe de analistas de segurança, assegurando qualidade, padronização e aderência aos SLAs na identificação, análise e resposta a incidentes;
- Orquestrar e supervisionar as operações do SOC, garantindo disponibilidade, eficiência operacional e cumprimento de processos;
- Elaborar, revisar e evoluir playbooks, runbooks, procedimentos operacionais e casos de uso de detecção;

- Apoiar tecnicamente na mitigação de ataques cibernéticos e na coleta e preservação de evidências para auditorias, clientes e certificações;
- Atuar com frameworks e boas práticas como MITRE ATT&CK, NIST, CIS Controls;
- Atuar como referência técnica da operação, promovendo capacitação e desenvolvimento contínuo da equipe;
- Identificar e implementar melhorias em dashboards, fluxos operacionais e integrações do SOC;
- Monitorar métricas e KPIs do SOC, garantindo eficiência, qualidade e evolução dos indicadores.

SEG-03.6 - Líder Técnico de Segurança – Nível 2 - OPERAÇÃO

Resumo do Cargo:

Lidera tecnicamente a operação do SOC com foco em evolução de processos, maturidade de detecção e melhoria contínua da resposta a incidentes. Atua no desenvolvimento de casos de uso, otimização de fluxos e fortalecimento das práticas baseadas em frameworks de segurança. Possui papel ativo na consolidação de indicadores e na performance da equipe.

Requisitos de Formação:

- Ensino superior completo em Redes de Computadores, Segurança da Informação, Ciência da Computação, Sistemas de Informação ou áreas correlatas;
- Pós-graduação em Gestão ou Segurança da Informação será considerada um diferencial;
- Experiência sólida em operações de SOC (Security Operations Center) e resposta a incidentes de segurança da informação;
- Conhecimentos avançados em redes, segurança, monitoramento e arquitetura de sistemas de segurança;
- Vivência prática com ferramentas como SIEM (Google SecOps, QRadar, entre outras), Anti-DDoS, WAF, XDR, IDS/IPS;
- Familiaridade com frameworks e boas práticas de segurança da informação, como MITRE ATT&CK, NIST, CIS Controls, entre outros;
- Habilidade na elaboração de relatórios técnicos e documentação especializada;
- Desejável experiência prévia em liderança técnica.

Responsabilidades:

- Liderar tecnicamente a equipe de analistas de segurança, assegurando qualidade, padronização e aderência aos SLAs na identificação, análise e resposta a incidentes;
- Orquestrar e supervisionar as operações do SOC, garantindo disponibilidade, eficiência operacional e cumprimento de processos;

- Elaborar, revisar e evoluir playbooks, runbooks, procedimentos operacionais e casos de uso de detecção;
- Desenvolver e aprimorar processos de detecção, resposta e contenção de incidentes, promovendo melhoria contínua;
- Apoiar tecnicamente na mitigação de ataques cibernéticos e na coleta e preservação de evidências para auditorias, clientes e certificações;
- Atuar com frameworks e boas práticas como MITRE ATT&CK, NIST, CIS Controls;
- Atuar como referência técnica da operação, promovendo capacitação e desenvolvimento contínuo da equipe;
- Identificar e implementar melhorias em dashboards, fluxos operacionais e integrações do SOC;
- Monitorar métricas e KPIs do SOC, garantindo eficiência, qualidade e evolução dos indicadores.

SEG-03.6 - Líder Técnico de Segurança – Nível 3 - OPERAÇÃO

Resumo do Cargo:

Profissional com forte atuação estratégica na condução técnica da operação, combinando liderança de equipe com visão analítica e executiva. Responsável por direcionar melhorias estruturais, consolidar indicadores para tomada de decisão e elevar o nível de maturidade do SOC. Atua como elo entre a operação técnica e a gestão estratégica.

Requisitos de Formação:

- Ensino superior completo em Redes de Computadores, Segurança da Informação, Ciência da Computação, Sistemas de Informação ou áreas correlatas;
- Pós-graduação em Gestão ou Segurança da Informação será considerada um diferencial;
- Experiência sólida em operações de SOC (Security Operations Center) e resposta a incidentes de segurança da informação;
- Conhecimentos avançados em redes, segurança, monitoramento e arquitetura de sistemas de segurança;
- Vivência prática com ferramentas como SIEM (Google SecOps, QRadar, entre outras), Anti-DDoS, WAF, XDR, IDS/IPS;
- Familiaridade com frameworks e boas práticas de segurança da informação, como MITRE ATT&CK, NIST, CIS Controls, entre outros;
- Habilidade na elaboração de relatórios técnicos e documentação especializada;
- Desejável experiência prévia em liderança técnica.

Responsabilidades:

- Liderar tecnicamente a equipe de analistas de segurança, assegurando qualidade, padronização e aderência aos SLAs na identificação, análise e resposta a incidentes;
- Orquestrar e supervisionar as operações do SOC, garantindo disponibilidade, eficiência operacional e cumprimento de processos;
- Elaborar, revisar e evoluir playbooks, runbooks, procedimentos operacionais e casos de uso de detecção;
- Desenvolver e aprimorar processos de detecção, resposta e contenção de incidentes, promovendo melhoria contínua;
- Elaborar relatórios técnicos e executivos com indicadores operacionais, riscos e recomendações;
- Apoiar tecnicamente na mitigação de ataques cibernéticos e na coleta e preservação de evidências para auditorias, clientes e certificações;
- Atuar com frameworks e boas práticas como MITRE ATT&CK, NIST, CIS Controls;
- Atuar como referência técnica da operação, promovendo capacitação e desenvolvimento contínuo da equipe;
- Identificar e implementar melhorias em dashboards, fluxos operacionais e integrações do SOC;
- Monitorar métricas e KPIs do SOC, garantindo eficiência, qualidade e evolução dos indicadores.

SEG-03.6 - Líder Técnico de Segurança – Nível 1 – CORE

Resumo do Cargo:

Responsável pela sustentação técnica das tecnologias centrais de segurança, com foco em regras de detecção, ajustes finos e estabilidade das plataformas. Atua na evolução de playbooks, melhoria de integrações e qualidade técnica das ferramentas do SOC. Tem perfil técnico aprofundado com foco em engenharia e eficiência operacional.

Requisitos de Formação:

- Ensino superior completo em Redes de Computadores, Segurança da Informação, Ciência da Computação, Sistemas de Informação ou áreas correlatas;
- Pós-graduação em Gestão ou Segurança da Informação será considerada um diferencial;
- Experiência sólida em operações de SOC (Security Operations Center) e resposta a incidentes de segurança da informação;
- Conhecimentos avançados em redes, segurança, monitoramento e arquitetura de sistemas de segurança;

- Vivência prática com ferramentas como SIEM (Google SecOps, QRadar, entre outras), Anti-DDoS, WAF, XDR, IDS/IPS;
- Conhecimento em linguagens de script, com ênfase em Python;
- Familiaridade com frameworks e boas práticas de segurança da informação, como MITRE ATT&CK, NIST, CIS Controls, entre outros;
- Habilidade na elaboração de relatórios técnicos e documentação especializada;
- Capacidade de analisar e ajustar regras de detecção e alertas de segurança;
- Desejável experiência prévia em liderança técnica.

Responsabilidades:

- Liderar tecnicamente a equipe de analistas de segurança;
- Elaborar, revisar e evoluir playbooks, runbooks, procedimentos operacionais e casos de uso de detecção;
- Desenvolver e aprimorar processos de detecção, resposta e contenção de incidentes, promovendo melhoria contínua;
- Elaborar relatórios técnicos e executivos com indicadores operacionais, riscos e recomendações;
- Apoiar tecnicamente na mitigação de ataques cibernéticos e na coleta e preservação de evidências para auditorias, clientes e certificações;
- Configurar, revisar e manter regras de detecção em plataformas como SIEM, WAF, XDR, IDS/IPS e Anti-DDoS;
- Atuar com frameworks e boas práticas como MITRE ATT&CK, NIST, CIS Controls;
- Identificar e implementar melhorias em dashboards, fluxos operacionais e integrações do SOC;
- Monitorar métricas e KPIs do SOC, garantindo eficiência, qualidade e evolução dos indicadores.

SEG-03.6 - Líder Técnico de Segurança – Nível 2 - CORE**Resumo do Cargo:**

Líder técnico com forte perfil de engenharia e automação, responsável por evoluir regras, integrações e processos por meio de scripts e otimizações avançadas. Atua diretamente na redução de ruído, aumento de precisão das detecções e ganho de escala operacional. Contribui para modernização e eficiência técnica do ecossistema de segurança.

Requisitos de Formação:

- Ensino superior completo em Redes de Computadores, Segurança da Informação, Ciência da Computação, Sistemas de Informação ou áreas correlatas;

- Pós-graduação em Gestão ou Segurança da Informação será considerada um diferencial;
- Experiência sólida em operações de SOC (Security Operations Center) e resposta a incidentes de segurança da informação;
- Conhecimentos avançados em redes, segurança, monitoramento e arquitetura de sistemas de segurança;
- Vivência prática com ferramentas como SIEM (Google SecOps, QRadar, entre outras), Anti-DDoS, WAF, XDR, IDS/IPS;
- Conhecimento em linguagens de script, com ênfase em Python;
- Familiaridade com frameworks e boas práticas de segurança da informação, como MITRE ATT&CK, NIST, CIS Controls, entre outros;
- Habilidade na elaboração de relatórios técnicos e documentação especializada;
- Capacidade de analisar e ajustar regras de detecção e alertas de segurança;
- Experiência prévia em liderança técnica.

Responsabilidades:

- Liderar tecnicamente a equipe de analistas de segurança;
- Elaborar, revisar e evoluir playbooks, runbooks, procedimentos operacionais e casos de uso de detecção;
- Desenvolver e aprimorar processos de detecção, resposta e contenção de incidentes, promovendo melhoria contínua;
- Elaborar relatórios técnicos e executivos com indicadores operacionais, riscos e recomendações;
- Apoiar tecnicamente na mitigação de ataques cibernéticos e na coleta e preservação de evidências para auditorias, clientes e certificações;
- Configurar, revisar e manter regras de detecção em plataformas como SIEM, WAF, XDR, IDS/IPS e Anti-DDoS;
- Atuar com frameworks e boas práticas como MITRE ATT&CK, NIST, CIS Controls;
- Identificar e implementar melhorias em dashboards, fluxos operacionais e integrações do SOC;
- Desenvolver scripts (preferencialmente em Python) para automação de processos e integrações;
- Monitorar métricas e KPIs do SOC, garantindo eficiência, qualidade e evolução dos indicadores.

SEG-03.6 - Líder Técnico de Segurança – Nível 3 - CORE

Resumo do Cargo:

Referência técnica da vertical Core, responsável por decisões arquiteturais, automação avançada e direcionamento técnico das soluções de segurança. Atua na evolução da arquitetura, implantação de novas tecnologias e capacitação da equipe. Tem papel estratégico na sustentação técnica de alto nível e no futuro tecnológico do SOC.

Requisitos de Formação:

- Graduação completa em TI, Segurança da Informação ou áreas afins;
- Ensino superior completo em Redes de Computadores, Segurança da Informação, Ciência da Computação, Sistemas de Informação ou áreas correlatas;
- Pós-graduação em Gestão ou Segurança da Informação será considerada um diferencial;
- Experiência sólida em operações de SOC (Security Operations Center) e resposta a incidentes de segurança da informação;
- Conhecimentos avançados em redes, segurança, monitoramento e arquitetura de sistemas de segurança;
- Vivência prática com ferramentas como SIEM (Google SecOps, QRadar, entre outras), Anti-DDoS, WAF, XDR, IDS/IPS;
- Conhecimento em linguagens de script, com ênfase em Python;
- Familiaridade com frameworks e boas práticas de segurança da informação, como MITRE ATT&CK, NIST, CIS Controls, entre outros;
- Habilidade na elaboração de relatórios técnicos e documentação especializada;
- Capacidade de analisar e ajustar regras de detecção e alertas de segurança;
- Experiência prévia em liderança técnica.

Responsabilidades:

- Liderar tecnicamente a equipe de analistas de segurança;
- Elaborar, revisar e evoluir playbooks, runbooks, procedimentos operacionais e casos de uso de detecção;
- Desenvolver e aprimorar processos de detecção, resposta e contenção de incidentes, promovendo melhoria contínua;
- Elaborar relatórios técnicos e executivos com indicadores operacionais, riscos e recomendações;
- Apoiar tecnicamente na mitigação de ataques cibernéticos e na coleta e preservação de evidências para auditorias, clientes e certificações;
- Configurar, revisar e manter regras de detecção em plataformas como SIEM, WAF, XDR, IDS/IPS e Anti-DDoS;

- Atuar com frameworks e boas práticas como MITRE ATT&CK, NIST, CIS Controls;
- Atuar como referência técnica da operação, promovendo capacitação e desenvolvimento contínuo da equipe;
- Identificar e implementar melhorias em dashboards, fluxos operacionais e integrações do SOC;
- Apoiar na implantação de novas soluções de segurança e revisões de arquitetura;
- Desenvolver scripts (preferencialmente em Python) para automação de processos e integrações;
- Monitorar métricas e KPIs do SOC, garantindo eficiência, qualidade e evolução dos indicadores.

ESP-01 – Especialista 1

Resumo do Cargo:

Profissional que atua em projetos e processos estratégicos com foco em aplicação técnica especializada, contribuindo com soluções e orientações de média a alta complexidade, sob supervisão parcial. Atua como suporte técnico para a equipe em temas da sua área de domínio.

Requisitos de Formação:

- Graduação completa em área correlata;
- Desejável certificação técnica reconhecida no mercado;
- Experiência consistente na área de especialidade.

Responsabilidades:

- Propor e implementar soluções técnicas e processuais;
- Liderar iniciativas que envolvam múltiplas áreas;
- Propor soluções técnicas dentro de sua área de atuação;
- Apoiar a execução de projetos relevantes para a área;

ESP-02 – Especialista 2

Resumo do Cargo:

Atuação em projetos e processos estratégicos com foco em aplicação técnica especializada, contribuindo com soluções e orientações de média a alta complexidade, sob supervisão parcial. Atua como suporte técnico para a equipe em temas da sua área de domínio.

Profissional com sólida experiência técnica, responsável por liderar tecnicamente projetos estratégicos e propor soluções.

Requisitos de Formação:

- Graduação completa em área correlata;

- Pós-graduação em andamento e/ou certificações técnicas reconhecidas no mercado;
- Experiência sólida e comprovada na área de especialidade.

Responsabilidades:

- Propor e implementar soluções técnicas e processuais;
- Participar de decisões críticas em projetos de alto impacto;
- Liderar iniciativas que envolvam múltiplas áreas;
- Documentar boas práticas e padrões operacionais;
- Contribuir com orientações técnicas para a equipe.

ESP-03 – Especialista 3**Resumo do Cargo:**

Atuação em projetos e processos estratégicos com foco em aplicação técnica especializada, contribuindo com soluções e orientações de média a alta complexidade, sob supervisão parcial. Atua como suporte técnico para a equipe em temas da sua área de domínio.

Profissional com sólida experiência técnica, responsável por liderar tecnicamente projetos estratégicos e propor soluções.

Requisitos de Formação:

- Graduação completa em área correlata;
- Pós-graduação e/ou certificações técnicas reconhecidas no mercado;
- Experiência ampla, comprovada e estratégica na área de especialidade.

Responsabilidades:

- Propor e implementar soluções técnicas e processuais;
- Participar de decisões críticas em projetos de alto impacto;
- Liderar iniciativas que envolvam múltiplas áreas;
- Garantir a disseminação de boas práticas e padrões avançados;
- Ser referência técnica para profissionais de diferentes níveis.

ANC – Analista de Negócios JR

Tem como objetivo **apoiar** na análise, estruturação e acompanhamento de demandas relacionadas a **serviços, produtos e negócios**, tanto internos quanto externos.

Atua sob orientação, contribuindo para a compreensão das necessidades do negócio, apoio à tomada de decisão e melhoria contínua, bem como:

- Apoiar o levantamento e a documentação de requisitos de negócio, funcionais e não funcionais;
- Preparar minutas de relatórios, atas, apresentações e insumos para reuniões;
- Apoiar o mapeamento de processos de negócio, identificando pontos de melhoria, gargalos e oportunidades;
- Acompanhar planos de ação voltados à melhoria de produtos, serviços e negócios;

- Apoiar a elaboração de modelos de dashboards, indicadores e relatórios de acompanhamento;
- Auxiliar na organização e manutenção de documentos, artefatos e bases de conhecimento da área;
- Interagir com áreas técnicas, operacionais e administrativas, apoiando o alinhamento entre negócio e execução;
- Contribuir com o fluxo de ciclo de vida de serviços executando tarefas definidas nas etapas sob supervisão.

Manter-se atualizado sobre práticas de análise de negócios, BPM e gestão organizacional.

Formação necessária: cursando nível superior em **Administração, Engenharia de Produção, Economia, Sistemas de Informação, Ciência da Computação, Engenharia ou áreas correlatas.**

ANC– Analista de Negócios PL

Tem como objetivo atuar de forma estruturada na análise e gestão das demandas de negócio da GER, apoiando a tomada de decisão, a melhoria de processos e a evolução de serviços, produtos e negócios. Atua com autonomia moderada, sendo responsável por análises mais complexas, bem como:

- Levantar, analisar, documentar e validar requisitos de negócio e serviços junto às partes interessadas;
- Mapear, analisar e redesenhar processos de negócio utilizando práticas de BPM;
- Prover visibilidade sobre desempenho de processos, serviços e iniciativas estratégicas;
- Elaborar e acompanhar indicadores, dashboards e relatórios gerenciais;
- Apoiar a estruturação e revisão de serviços, SLAs, catálogos e portfólios;
- Analisar impactos organizacionais, operacionais e tecnológicos das demandas;
- Apoiar o planejamento de iniciativas e projetos, considerando escopo, riscos, prazos e benefícios, associados a serviços, produtos e negócios;
- Facilitar a comunicação entre áreas de negócio, tecnologia e operação;
- Apoiar a definição de padrões, métodos e boas práticas de análise de negócios;

Apoiar a gestão de contratos e SLAs de serviços;

Manter-se atualizado sobre tendências de mercado, tecnologia e gestão.

Formação necessária:

Graduação completa em **Administração, Engenharia de Produção, Economia, Sistemas de Informação, Ciência da Computação, Engenharia ou áreas correlatas.**

ANC – Analista de Negócios SR

Tem como objetivo **atuar de forma estratégica na gestão e evolução dos negócios e serviços**, apoiando decisões de médio e longo prazo, integrando processos, serviços, produtos e negócios aos objetivos organizacionais da RNP.

Atua com elevada autonomia e responsabilidade, bem como:

- Liderar análises complexas de negócio, identificando oportunidades de melhoria e inovação;
- Coordenar o levantamento e a priorização de demandas estratégicas;
- Estruturar e contribuir na evolução dos portfólios de negócios, serviços e produtos;
- Prover visão integrada do desempenho dos negócios e serviços por meio de indicadores e análises;

- Apoiar a definição e revisão de políticas, normas, SLAs e modelos de governança;
- Apoiar a gestão de portfólio negócios e serviços;
- Facilitar workshops, reuniões críticas e apresentações executivas;
- Atuar como referência técnica em análise de negócios e BPM;
- Atuar como especialista de ciclo de vida de serviços, garantindo sua plena aplicação e melhoria contínua;
- Facilitar o alinhamento entre estratégia, operação e tecnologia;
- Mitigar riscos, conduzir análises de causa raiz e propor contramedidas estratégicas;
- Apoiar a gestão da mudança organizacional;
- Manter-se atualizado sobre tendências, metodologias e inovações relevantes.

Formação necessária:

- Graduação completa em **Administração, Engenharia de Produção, Economia, Sistemas de Informação, Ciência da Computação, Engenharia ou áreas correlatas**,
- Pós-graduação em andamento (desejável) em áreas relacionadas a Gestão de Negócios, Estratégia, Processos Organizacionais, Gestão de Serviços ou áreas afins.

APC – Analista de Processos JR

Tem como objetivo **apoiar a área de Processos** na identificação, mapeamento, documentação e melhoria de processos organizacionais.

Atua sob orientação, bem como:

- Apoiar o mapeamento e a documentação de processos de negócio e de suporte;
- Apoiar a atualização da base de processos e seus artefatos;
- Auxiliar na coleta de informações e indicadores de desempenho de processos;
- Apoiar ações de melhoria contínua e padronização;
- Apoiar a comunicação e disseminação dos processos junto às áreas envolvidas;
- Apoiar análises de conformidade e aderência aos processos definidos;
- Manter-se atualizado sobre conceitos de BPM e qualidade.

Formação necessária:

Cursando nível superior em Engenharia de Produção, Administração, Sistemas de Informação, Tecnologia da Informação, Ciência da Computação, Gestão da Qualidade ou áreas correlatas.

APC-02 – Analista de Processos PL

Tem como objetivo **atuar de forma estruturada na gestão e melhoria dos processos**, assegurando eficiência, padronização e alinhamento com os objetivos organizacionais.

Bem como:

- Mapear, analisar, redesenhar e documentar processos utilizando BPM;
- Conduzir análises de desempenho, riscos e oportunidades de melhoria;
- Definir e acompanhar indicadores e métricas de processos;
- Apoiar a padronização e governança de processos;

- Facilitar workshops e interações com áreas envolvidas;
- Apoiar iniciativas de automação e melhoria de fluxos;
- Garantir atualização e comunicação dos processos;
- Apoiar auditorias e análises de conformidade.

Formação necessária:

- Graduação completa em Engenharia de Produção, Administração, Sistemas de Informação, Tecnologia da Informação, Ciência da Computação, Gestão da Qualidade ou áreas correlatas.

APC – Analista de Processos SR

Tem como objetivo **atuar estrategicamente na governança, evolução e maturidade dos processos**, promovendo eficiência operacional, integração entre áreas e melhoria contínua.

Bem como:

- Definir e evoluir metodologias, padrões e boas práticas de BPM;
- Coordenar iniciativas de melhoria e transformação de processos;
- Prover visão integrada do desempenho dos processos organizacionais;
- Apoiar a definição de políticas, normas e governança de processos;
- Atuar como referência técnica em processos e qualidade;
- Apoiar decisões estratégicas por meio de análises estruturadas;
- Integrar processos, serviços, projetos e estratégia organizacional;
- Apoiar a gestão da mudança e a cultura de melhoria contínua.

Formação necessária:

- Graduação completa em Engenharia de Produção, Administração, Sistemas de Informação, Tecnologia da Informação, Ciência da Computação, Gestão da Qualidade ou áreas correlatas
- Pós-graduação em andamento (desejável) em áreas relacionadas a Gestão de Processos, Qualidade, Gestão Organizacional ou áreas afins.

ATC – Analista de Telecomunicações JR

(Especialidade: Conectividade de Clientes)

Tem como objetivo apoiar as atividades de provisionamento, acompanhamento e operação dos serviços de conectividade dos clientes da RNP à rede Ipê, garantindo o cumprimento dos parâmetros técnicos de qualidade, prazos acordados e padrões operacionais definidos. Atua sob orientação, contribuindo para a execução das atividades técnicas, análise inicial de problemas e apoio à melhoria contínua dos serviços de conectividade.

Atividades a serem exercidas

- Acompanhar as implantações de soluções de conectividade que interligam os clientes da RNP ao backbone IP, a rede Ipê, atuando junto a fornecedores e equipes internas para o cumprimento dos prazos acordados;
- Apoiar a análise de problemas técnicos ocorridos durante as implantações e na operação dos serviços, propondo soluções sob orientação;

- Apoiar a operação e a manutenção das soluções de conectividade, acompanhando indicadores de desempenho e qualidade;
- Auxiliar em iniciativas de melhoria contínua dos serviços e processos técnicos;
- Apoiar a aplicação de conceitos básicos de automação e análise de dados em atividades técnicas e administrativas;
- Colaborar com equipes multidisciplinares na identificação de oportunidades de uso de ferramentas analíticas e soluções baseadas em Inteligência Artificial;
- Contribuir para a elaboração e atualização de relatórios, notas técnicas e documentações, garantindo a rastreabilidade das atividades realizadas;
- Acompanhar tendências tecnológicas do setor de telecomunicações, com foco em conectividade, digitalização e inovação.

Formação necessária

Graduação completa em **Engenharia de Telecomunicações, Engenharia Elétrica, Ciência da Computação, Engenharia da Computação ou áreas correlatas.**

ATC – Analista de Telecomunicações PL

(Especialidade: Conectividade de Clientes)

Tem como objetivo atuar de forma autônoma no provisionamento, acompanhamento, operação e melhoria contínua dos serviços de conectividade dos clientes da RNP à rede Ipê, assegurando qualidade técnica, cumprimento de prazos e alinhamento com os padrões operacionais e estratégicos da organização.

Atua na análise e resolução de problemas técnicos de maior complexidade, contribuindo para a evolução dos serviços, processos e soluções de conectividade.

Atividades a serem exercidas

- Planejar, acompanhar e coordenar implantações de soluções de conectividade que interligam os clientes da RNP ao backbone IP, atuando de forma integrada com fornecedores e equipes internas;
- Analisar e tratar problemas técnicos de média complexidade nas implantações e na operação dos serviços, propondo e implementando soluções adequadas;
- Atuar no acompanhamento da operação e manutenção das soluções de conectividade, analisando indicadores de desempenho, qualidade e disponibilidade;
- Contribuir ativamente para iniciativas de melhoria contínua, automação de processos técnicos e uso de dados para apoio à tomada de decisão;
- Apoiar a definição, revisão e melhoria de fluxos, procedimentos e padrões técnicos relacionados aos serviços de conectividade;
- Colaborar com equipes multidisciplinares na identificação e aplicação de soluções baseadas em Inteligência Artificial e ferramentas analíticas para otimização de processos técnicos e administrativos;
- Elaborar e revisar relatórios técnicos, notas técnicas e documentações, garantindo clareza, padronização e rastreabilidade das ações;
- Acompanhar e avaliar tendências tecnológicas do setor de telecomunicações, propondo inovações aplicáveis ao contexto da RNP.

Formação necessária

Graduação completa em **Engenharia de Telecomunicações, Engenharia Elétrica, Ciência da Computação, Engenharia da Computação ou áreas correlatas.**

1) Cargos Operacionais – Núcleo do NOC (N1 / N2 / N3)

1.1 AN1 - Analista de Operações NOC – N1 (24x7) | Júnior / Pleno / Sênior

Objetivo do cargo

Atuar na **operação de primeiro nível** do NOC, garantindo **monitoramento contínuo, triagem, registro de incidentes e acionamento/escalonamento** conforme procedimentos, com alta disciplina de evidência e passagem de turno.

Responsabilidades

- Monitorar alarmes/eventos nas plataformas de observabilidade (ex.: Zabbix, Grafana, ELK e/ou ferramenta vigente durante transição), identificando anomalias e indisponibilidades.
- Realizar **triagem, classificação e priorização inicial** de incidentes por impacto, abrangência e domínio (Backbone, Redes Metro, Transmissão/DWDM/DCI, Últimas Milhas).
- **Abrir, atualizar e encerrar registros** em ferramenta de ITSM/Service Desk, incluindo evidências, linha do tempo e ações tomadas (manual e/ou por automação).
- Executar **acionamentos iniciais** previstos em runbooks (parceiros/provedores quando aplicável) e **escalonar para N2/N3** quando houver necessidade de diagnóstico/correção.
- **Abrir e acompanhar chamados** junto a operadoras, provedores e parceiros (ex.: telecom e peering), realizando escalonamentos até resolução.
- Acompanhar o ciclo do incidente, cobrando retorno, registrando atualizações e garantindo **passagem de turno (handover)** completa e padronizada.
- Registrar e controlar janelas/downtimes comunicados pela operação (quando definidos em procedimento), garantindo consistência do registro operacional.
- Apoiar a atualização de base de conhecimento com feedback de operação (melhorias em procedimentos e alarmística).

Requisitos

- Noções de redes TCP/IP, endereçamento, roteamento básico e troubleshooting inicial (camada 2/3 conceitual).
- Familiaridade com ferramentas de monitoramento (Zabbix ou equivalente) e leitura de dashboards/alertas.
- Vivência com ferramenta ITSM/Service Desk (abertura/atualização de tickets) e disciplina de registro.
- Boa redação técnica para registros objetivos (linha do tempo, evidências, anexos).
- Atenção a detalhes, senso de urgência, organização, comunicação clara e colaboração.
- Capacidade de trabalhar sob pressão (ambiente 24x7) e seguir procedimentos.

Formação

Tecnólogo/graduação em Redes, Telecom, TI, Engenharia ou áreas correlatas.

Diferenciação por nível (complexidade)

- **AN1-01 Júnior:** foco em monitoramento, abertura/atualização de tickets, execução estrita de runbooks, escalonamento rápido e correto.
- **AN1-02 Pleno:** triagem mais qualificada, correlação inicial de eventos, acionamentos mais complexos e handover mais robusto; apoia treinamento de júnior.
- **AN1-03 Sênior:** referência de turno; atua na melhoria de procedimentos, atua como “ponto focal” operacional do turno para alinhamento com N2/Coordenação.

1.2 AN2 – Analista de Operações NOC – N2 (24x7) | Júnior /Pleno / Sênior

Objetivo do cargo

Atuar no **segundo nível** do NOC realizando **análise, correlação, diagnóstico e correção** (definitiva ou paliativa), incluindo gestão técnica de incidentes com terceiros e escalonamento para N3/fabricante quando necessário.

Responsabilidades

- Executar **diagnóstico técnico** a partir de alarmes/eventos, logs e testes operacionais, definindo causa provável e plano de ação.
- Realizar **correções paliativas/definitivas** dentro do escopo operacional (ajustes operacionais, reconfigurações controladas, restaurações, validações pós-correção), ou coordenar correção por equipe responsável.
- Avaliar e apoiar **GMUDs** relacionadas a circuitos e operação, registrando janelas/downtimes conforme processo.
- Produzir registros técnicos completos (diagnóstico, evidências, testes, conclusão, relatórios de RFO (*reason for outage*)), suportando pós-análise e melhoria contínua.
- Escalonar para N3 quando envolver necessidade de intervenção de fabricante, manutenção/atualização, falha recorrente complexa ou risco elevado.
- Apoiar a evolução da base de conhecimento e procedimentos operacionais.

Requisitos

- Troubleshooting avançado em redes (L2/L3), roteamento dinâmico (ex.: BGP) e análise de indisponibilidade/perda de qualidade.
- Capacidade de operar e interpretar monitoramento/observabilidade (eventos, correlação, métricas).
- Experiência com gestão de incidentes envolvendo terceiros (operadoras/parceiros) e documentação técnica.
- Desejável: conhecimento de redes ópticas/transmissão (dependendo da subespecialização).
- Raciocínio analítico, autonomia, priorização, comunicação objetiva e negociação técnica com terceiros.
- Postura colaborativa e orientação a resolução.

Formação

Graduação/tecnólogo em Redes/Telecom/TI/Engenharias correlatas.

Certificações são desejáveis (ex.: redes, fabricantes, ITIL — se aplicável ao ambiente).

Diferenciação por nível (complexidade)

- **AN2-01 Júnior:** executa diagnóstico e correção na maioria dos incidentes; aciona terceiros e valida restauração.
- **AN2-02 Pleno:** conduz incidentes complexos/múltiplos domínios, define workaround, orienta N1/N2 e atua fortemente com terceiros.
- **AN2-03 Sênior:** referência por domínio (IP, DWDM, Metro etc.), define padrões técnicos de correção operacional e faz interface técnica avançada com N3/fabricantes quando necessário.

Subespecializações por domínio

A diferenciação por domínio está alinhada às camadas/ambientes de redes tais como: metro, acesso, longa distância, DWDM e backbone IP

- **AN2-0X-BK – Backbone IP:** circuitos de backbone, roteamento OSPF, BGP, peering, roteadores do *core*, out of band.
- **AN2-0X-MT – Redes Metropolitanas e Acesso:** redes metro ethernet, longa distância e acesso e interações com parceiros locais/field service.
- **AN2-0X-TX – Transmissão:** gerência dos sistemas ópticos DWDM, canais ópticos, DCI de fabricantes Huawei, Ciena e/ou Padtec.

1.3 AN3 – Analista de Operações NOC – N3 | Pleno / Sênior

Objetivo do cargo

Atuar como **terceiro nível** (engenharia de operação), responsável por **resolver problemas complexos**, conduzir **atualizações/manutenções**, interagir com **fabricantes** e governar **procedimentos, scripts e configurações avançadas** de monitoramento/observabilidade.

Responsabilidades

- Atuar em incidentes escalonados (alta complexidade), realizando troubleshooting profundo e definindo solução definitiva.
- **Acionar e conduzir tratativas com fabricantes (TAC)**, incluindo abertura, acompanhamento e validação técnica de correções.
- Planejar/executar **atualizações, manutenções preventivas** e mudanças de alto risco operacional, garantindo registro e alinhamento com janelas.
- Consolidar e manter **procedimentos, scripts e manuais** operacionais; promover compartilhamento de conhecimento e treinamento.
- Evoluir a configuração de monitoramento (cadastro de serviços/hosts, perfis de acesso, visões/correlações quando aplicável).
- Produzir relatórios técnicos periódicos e recomendações de melhoria (quando solicitado pela gestão).

Requisitos

- Sólida experiência em redes/telecom (L2/L3), troubleshooting avançado e ambientes críticos.
- Vivência em execução de mudanças (GMUD), atualizações/manutenções e gestão de risco operacional.
- Experiência com ferramentas de monitoramento, observabilidade e administração (Zabbix), incluindo modelagem de serviços e visões.
- Experiência em relacionamento técnico com fabricantes (TAC) e análise de bugs/firmware (desejável).
- Liderança técnica informal, didática, comunicação assertiva, organização e pensamento sistêmico.

Formação

Graduação em Engenharias, Redes, Telecom, Ciência da Computação ou áreas correlatas.

Diferenciação por nível (complexidade)

- **AN3-02 Pleno:** resolve incidentes complexos e conduz mudanças relevantes; mantém procedimentos e atua como referência técnica.
- **AN3-03 Sênior:** domínio profundo (IP, DWDM, Metro); elabora os scripts e automações de rede; conduz relacionamento com fabricantes, define padrões e arquitetura operacional do monitoramento/runbooks.

Subespecializações por domínio

- **AN3-0X-BK – Backbone IP:** troubleshooting avançado de BGP/roteamento, engenharia de tráfego e arquitetura operacional do backbone.
- **AN3-0X-MT – Redes Metropolitanas e Acesso:** troubleshooting avançado, Integrações de campo, padrões de O&M, runbooks de acionamento e validação fim-a-fim.
- **AN3-0X-TX – Transmissão:** troubleshooting avançado, manutenção/atualização de elementos ópticos, DWDM e interface técnica com fabricantes Huawei, Padtec e/ou Ciena.

2) Cargos de Coordenação e Liderança Técnica

2.1 SNOC-02 – Supervisor de Turno NOC | Pleno / Sênior

Objetivo do cargo

Coordenar a operação do NOC garantindo **continuidade 24x7**, governança de rotinas, qualidade da execução, gestão de escala e condução de incidentes críticos, reportando-se à **Gerência**.

Responsabilidades

- Gerir a operação 24x7 (escala, cobertura, passagem de turno, padronização de execução e aderência a procedimentos).
- Conduzir o processo de transição/integração operacional (treinamentos, padronização, rotinas de acompanhamento, comunicação interna) quando aplicável.
- Coordenar resposta a incidentes de alto impacto (mobilização de N2/N3, priorização, alinhamento operacional).
- Garantir atualização e governança de procedimentos operacionais e base de conhecimento (em conjunto com Tech Lead/N3).
- Atuar como interface administrativa-operacional do time terceirizado (alinhamento de alocação, cobertura, substituições), mantendo foco na continuidade do serviço.

Requisitos

- Experiência consolidada em operação de NOC e gestão de turno/equipes 24x7.
- Boa compreensão de processos de operação, incidentes e mudanças (GMUD/downtime).
- Liderança, tomada de decisão sob pressão, comunicação clara, organização e negociação.

Formação

Superior completo em áreas correlatas a TI/Telecom/Engenharia.

2.2 SNOC-03 – Supervisor de Turno NOC

Objetivo do cargo

Atuar como **liderança técnica transversal**, sustentando a maturidade técnica do NOC (especialmente N2/N3), padronizando runbooks, orientando resolução de alta complexidade e contribuindo para evolução de monitoramento/observabilidade. Deve possuir perfil técnico forte e habilidades de liderança, reportando-se à Coordenação.

Responsabilidades

- Ser referência técnica para diagnósticos complexos e incidentes recorrentes, orientando N2 e N3.
- Padronizar e revisar procedimentos, scripts e guias operacionais (runbooks), garantindo aplicabilidade prática para N1/N2.
- Apoiar a evolução do monitoramento (visões, correlações, melhores práticas de alarmística e integração operacional), principalmente em contexto de mudança de ferramenta.
- Apoiar a gestão na capacitação técnica do time terceirizado (trilhas por domínio, onboarding e reciclagens).
- Atuar em escalonamentos críticos e apoiar a coordenação em crises técnicas (sem assumir papel administrativo primário).

Requisitos

- Experiência sólida em operação/engenharia de redes/telecom, troubleshooting avançado.
- Vivência com ambientes multi-domínio (IP, Metro, Transmissão) e operação com parceiros.
- Domínio de ferramentas de monitoramento/observabilidade e práticas de melhoria de alarmística.
- Liderança técnica, comunicação, influência sem autoridade formal, mentoria, didática, organização.

Formação

Superior completo em Engenharias, Redes, Telecom, Computação ou correlatas.

3.1 AOSS – Analista OSS & Automação (OSS/Zabbix/Integrações) | Júnior / Pleno / Sênior

Objetivo do cargo

Sustentar e evoluir a capacidade de **OSS e automação** do NOC, administrando a plataforma de monitoramento/observabilidade e integrações operacionais (ex.: ITSM), garantindo visões, alarmística e automações alinhadas ao uso do N1/N2.

Responsabilidades

- Administrar a infraestrutura das plataformas de monitoramento (ex.: Zabbix): itens, triggers, templates, discovery, macros, manutenção/downtime e visões operacionais e outras ferramentas de suporte à operação do NOC (OSS).
- Desenvolver e manter dashboards/visões orientadas por serviço e domínio, apoiando a triagem do N1 e o diagnóstico do N2.
- Implementar e sustentar **automações** (abertura/enriquecimento de tickets, deduplicação, roteamento), reduzindo esforço manual do NOC.
- Integrar monitoramento com inventário (quando aplicável) e base de conhecimento, garantindo consistência entre “o que existe” e “o que monitora”.
- Definir padrões de onboarding de novos elementos (hosts/services) e controlar qualidade da alarmística (redução de falso positivo/ruído).
- Apoiar migrações e transições de ferramenta (quando aplicável), garantindo continuidade operacional.

Requisitos

- Administração de Zabbix (ou equivalente) e conceitos de observabilidade.
- Integração via APIs, webhooks e automação de fluxo (desejável).
- Noções sólidas de redes e infraestrutura para modelagem correta de monitoramento.

- Organização, pensamento analítico, capacidade de traduzir necessidade operacional em automação, comunicação com operação.

Formação

- Tecnólogo/Graduação em TI, Redes, Computação, Engenharias correlatas.

Diferenciação por nível (complexidade)

- **AOSS-01 Júnior:** operação assistida, manutenção de cadastros, apoio a dashboards, execução de tarefas guiadas.
- **AOSS-02 Pleno:** cria/ajusta templates, triggers e integrações simples; melhora visões para N1/N2.
- **AOSS-03 Sênior:** desenha padrões, governa alarmística e integrações complexas; atua em migração e mudanças, atua em automações.

3.2 ADOC – Assistente de Cadastro & Documentação de Rede (Netbox/CMDB) | Júnior / Pleno / Sênior

Objetivo do cargo

Manter a **documentação e inventário (Netbox/CMDB)** atualizados e confiáveis, assegurando rastreabilidade de ativos, circuitos, canais, rotas e relacionamentos, apoiando auditorias, fiscalização de uso e eficiência de diagnóstico.

Responsabilidades

- Realizar cadastro e atualização de topologia, circuitos, fibras/trechos, equipamentos, enlaces e dependências no Netbox/CMDB.
- Garantir que mudanças operacionais (GMUD, ampliações, substituições) reflitam no inventário e documentação.
- Apoiar o NOC na identificação de impacto (mapa de dependências) e na padronização de nomenclatura/atributos técnicos.
- Produzir documentação operacional de referência (diagramas, cadastros mínimos, listas de contatos técnicos por rota/parceiro).
- Apoiar **auditorias/fiscalização de uso e alocação de blocos** (quando aplicável ao escopo).

Requisitos

- Experiência com Netbox e/ou CMDB, inventário de rede e conceitos de topologia (L1/L2/L3).
- Boa capacidade de documentação técnica e padronização.
- Atenção extrema a detalhe, disciplina, comunicação e colaboração com equipes técnicas.

Formação

Técnico/Tecnólogo/Graduação - TI/Redes/Telecom/Engenharias ou correlatas.

Diferenciação por nível (complexidade)

- **ADOC-01 Júnior:** cadastro e atualização supervisionada, checagem de consistência.
- **ADOC-02 Pleno:** governa padrões de cadastro, consolida documentação e apoia auditorias.
- **ADOC-03 Sênior:** desenha modelo de dados, garante integridade e integra inventário com monitoramento/processos.

3.4 AQ – Analista de Qualidade & Garantia de Serviço | Júnior / Pleno / Sênior

Objetivo / Resumo

Sustentar a capacidade de **Qualidade e Garantia de Serviço** do NOC, organizando análises pós-incidente, padrões de registro/qualidade operacional e backlog de melhorias de confiabilidade.

Responsabilidades detalhadas

- Realizar análises qualitativas de incidentes relevantes (consistência de registros, evidências, categorização e aprendizado).
- Acompanhar incidentes e escalonamentos, reparos e garantir a priorização.
- Acompanhar a performance do serviço de conectividade prestado aos clientes, por meio dos acordos firmados (SLAs) para condução e execução de planos de melhoria.
- Conduzir e padronizar relatórios operacionais periódicos quando demandados (formato e conteúdo).
- Identificar recorrências e propor ações estruturantes (procedimentos, alarmística, documentação, automação).
- Apoiar governança de janelas/downtime e aderência ao processo de mudanças sob a ótica de qualidade.

Requisitos

- Experiência com operação/qualidade em ambientes NOC e boa capacidade de análise e documentação.
- Organização, senso crítico, comunicação escrita excelente, colaboração.

Formação

TI/Telecom/Engenharias ou correlatas (desejável).

Diferenciação por nível

- **AQ-01 Júnior:** consolidação de informações e relatórios sob orientação.
- **AQ-02 Pleno:** análises e padronizações; recomenda melhorias e acompanha execução.
- **AQ-03 Sênior:** conduz análises complexas (multi-domínio) e governa padrões de qualidade.

