serena

Política de Segurança da Informação

serena

Sumário

Introdução

Esta Política de Segurança da Informação ("Política") define normas e diretrizes que buscam assegurar a confidencialidade, a integridade, a disponibilidade dos dados e dos sistemas de informação utilizados pela Serena. A proteção adequada dos ativos e dos dados utilizados é fundamental para possibilitar a identificação, a proteção, a detecção, a resposta e a recuperação de eventos em caso de eventual falha da segurança da informação.

Além disso, a Política complementa a Seção 13 do Código de Conduta da Companhia, no que diz respeito às diretrizes e às condutas esperadas dos co-empreendedores, terceiros, parceiros, fornecedores e prestadores de serviços, quanto à proteção dos ativos e dados com intuito de assegurar a confidencialidade, a integridade, a autenticidade e disponibilidade das informações.

Esta Política será disponibilizada no website e plataforma de rede social interna para todos do Time Serena.

A área de Tecnologia da Informação manterá em atividade um programa de revisão/atualização, que assegure que os requisitos de segurança técnicos e legais implementados estão sendo cumpridos e em conformidade com a legislação vigente, incluindo também a revisão periódica dos planos de ação e sua adesão a iniciativas de compartilhamento de informações sobre incidentes cibernéticos.

A adesão a essa Política e eventuais desvios de conduta serão endereçados pela Diretoria de Tecnologia da Serena e, sempre que necessário, reportados ao Comitê de Auditoria e Riscos.

Os termos usados em letra maiúscula possuem os significados definidos no glossário do Código de Conduta ou nesta Política de Segurança da Informação.

Público-alvo

Esta Política se aplica a todos os conselheiros, administradores, diretores e integrantes do time da Serena Energia S.A. e todas as empresas que fazem parte do Grupo Serena. Esta Política também é estendida a todos nossos parceiros de negócios, incluindo fornecedores, prestadores de serviço e quaisquer outros terceiros que mantenham relações ou atuem em benefício ou representem a Serena.

Regras básicas de segurança da informação

1.1. Princípios da segurança da informação

Nosso compromisso com o tratamento adequado das informações da Serena, de clientes e do público em geral está fundamentado nos seguintes princípios:

a) **Confidencialidade**: propriedade pela qual se assegura que a informação não será divulgada a pessoas, sistemas órgãos ou entidades sem autorização prévia dos seus titulares ou da Serena.
b) **Integridade**: propriedade pela qual se assegura que o conteúdo da informação não tenha sido alterado ou destruído de maneira não autorizada ou acidental e, portanto, seja íntegro e autêntico.
c) **Disponibilidade**: propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados.

1.2. Ciclo de vida da informação

Para efeito dessa Política, considera-se como ciclo de vida da informação:

a) **Manuseio:** é a etapa onde a informação é criada e manipulada.
b) **Armazenamento:** é a guarda da informação, seja em um banco de dados, em um papel, em mídia eletrônica externa, entre outros.
c) **Transporte:** ocorre quando a informação é transportada para algum local, não importando o meio onde ela está armazenada.
d) **Descarte:** é a eliminação de documento impresso (depositado na lixeira e/ou mantido em empresa de armazenagem), eletrônico ou destruição de

mídias de armazenamento (por exemplo, CDs, DVDs, disquetes, pen-drives) por completo.

1.3. Classifica da informação

A classificação das informações deve ser avaliada de acordo com seu conteúdo, relevância do conhecimento externo e pelos elementos específicos do documento. O acesso, divulgação e tratamento de documento (físico ou digitalizado), dado ou informação são restritos aos co-empreendedores que tenham necessidade de conhecê-los em razão de suas atividades dentro da Serena, sendo esse acesso pautado pelas regras previstas nessa Política e demais normas da empresa.

Toda informação de uso corporativo deve ser classificada de acordo com o grau de sigilo para o negócio da empresa, considerando-se três níveis:

a) **Confidencial**: É o mais alto grau de sigilo, aplicadas às informações de caráter estratégico e que devem ser manuseadas por um grupo restrito de usuários. O acesso não autorizado a essas informações pode ter consequências críticas para o negócio, causando, inclusive, danos estratégicos à imagem da empresa.
b) **Interno**: São informações específicas para uso interno, com circulação exclusiva dentro da empresa. Essas informações podem estar disponíveis a todos os funcionários e prestadores de serviço e devem ser utilizadas somente para atividades da Serena. Esse conteúdo, mesmo sendo de circulação livre dentro da empresa, não deve ser divulgado para externos sem os devidos cuidados, incluindo, quando necessário, a assinatura de acordos de confidencialidade ou de autorização formal previamente avaliada pela área responsável.
c) **Externo**: São informações de circulação livre e domínio público. Esse tipo de informação não exige controles ou restrições de segurança para seu acesso ou guarda.

1.4. Incidentes de segurança da informação

Para efeito dessa Política, um incidente de segurança é definido como qualquer evento adverso, decorrente da ação ou omissão de co-empreendedores e de terceiros, ainda que intencional, ou, ainda, de uma ameaça que ataque os princípios da Segurança da Informação.

Sistema de gestão da segurança da informação

O Sistema de Gestão da Segurança da Informação é o conjunto de processos e boas práticas para estabelecer, implementar, operar, monitorar, revisar, manter e aprimorar a segurança da informação com ações em quatro grandes frentes de atuação:

- Governança das políticas e procedimentos de segurança da informação;
- Recursos e componentes de segurança da informação;
- Monitoramento contínuo do ambiente de tecnologia da informação; e
- Gestão de crises e continuidade de negócios.

Diretrizes internas sobre segurança da informação e *cyber security*

3.1. Comportamento seguro

Co-empreendedores e parceiros devem assumir atitude proativa e engajada no que diz respeito à segurança da informação, bem como à privacidade e à proteção de dados.

É vetado comentários sobre assuntos relacionados à Serena e suas operações fora do ambiente de trabalho ou na presença de pessoas que não estejam ligadas a eles.

Informações internas e/ou confidenciais devem ser armazenadas nos servidores e sistemas corporativos. Informações salvas localmente nos equipamentos não são consideradas adequadamente protegidas e não estão contempladas em processos corporativos de cópia de segurança (backup). Informações contendo dados pessoais de clientes, co-empreendedores e parceiros não devem ser salvas localmente no equipamento.

Co-empreendedores e parceiros da Serena não devem trocar, publicar ou armazenar informações estratégicas, de segredo industrial e confidenciais, sobre a Serena, inclusive parceiros e clientes, salvo ocasiões formalmente definidas (como por exemplo, em caso de divulgação de resultados de promoções, publicidades etc.), em redes sociais, e-mail pessoal, sistemas e equipamentos externos.

O correio eletrônico (e-mail) é uma ferramenta disponibilizada exclusivamente para uso profissional, sendo, portanto, passível de análise/consulta pela companhia. Não deve ser utilizado para enviar spam, correntes, pirâmides, boatos, comentários difamatórios, ofensivos, racistas, obscenos, material ilegal, entre outros, conforme disposto na [Norma de Uso Aceitável de Ativos de TI] e no Código de Ética e Conduta da empresa.

O uso de mensagens instantâneas (chat) é restrito para uso profissional e deve ser utilizado de forma ética e responsável, conforme Norma de Uso Aceitável de Ativos de TI. É proibido o uso de aplicativos de comunicação instantânea não homologados para enviar documentos, fotos PDFs, arquivos de Word, Excel, Power Point (e plataformas análogas), os quais devem ser enviados pelo e-mail corporativo ou por aplicativo homologado pela Companhia.

Os co-empreendedores e, quando aplicável, parceiros devem adotar a política de mesas e telas limpas. Tais medidas objetivam a mitigação do risco de acesso não autorizado, perda e dano da informação durante e fora do horário de trabalho. Informações de negócio (sensíveis ou críticas, por exemplo, em papel ou mídia de armazenamento removível) não devem permanecer de forma desprotegida (por exemplo, sobre as mesas ou em quadros), bem como os computadores devem ser bloqueados com senha durante a ausência do usuário. Idealmente, o armazenamento destas informações deve ser feito em cofre, armário ou outra mobília de segurança, especialmente quando o escritório estiver desocupado.

O uso de equipamentos corporativos deve ser feito unicamente pelo profissional. Ceder seu uso a um terceiro indivíduo para qualquer atividade alheia ao propósito profissional caracteriza infração sujeita às sanções administrativas cabíveis.

3.2. Security & privacy by design

A segurança da informação e a proteção de dados devem ser seguidos e implantados de forma proativa desde o início do desenho, desenvolvimento e arquitetura de novos produtos e processos, incorporando boas práticas de segurança da informação, privacidade e proteção de dados ao longo de todo o ciclo.

3.3. Proteção de dados

O trato com o dado, em todo o seu ciclo de vida, deve seguir os requisitos da Política de Proteção de Dados.

Toda a informação contendo dados pessoal que seja tratada pela Serena deve ser classificada conforme o grau de sigilo do seu conteúdo e pensadas de acordo com seu valor, requisitos legais, sensibilidade e confidencialidade, conforme disposto nas políticas e normas internas aplicáveis.

Todos os co-empreendedores e parceiros são responsáveis por manter a privacidade e garantir a proteção dos dados tratados, bem como garantir o sigilo das informações da Serena classificadas como confidenciais e internas.

Os contratos com parceiros devem possuir um acordo formal de confidencialidade estabelecido antes do início da prestação do serviço, bem como o parceiro deve dar o aceite da Política de Segurança da Informação da Companhia, respeitando suas diretrizes e controles.

3.4. Identificação/avaliação de ameaças e vulnerabilidades

Caberá à área de Segurança da Informação da Serena a identificação, avaliação, registro e reporte dos riscos a que os processos e ativos estejam sujeitos e possíveis cenários de ameaça.

As vulnerabilidades e riscos identificados devem ser mitigados e monitorados, considerando as legislações vigentes e obrigações com reguladores.

Deve-se suportar o correto tratamento e encaminhamento dos eventos, sua documentação formal, classificação e comunicação aos times responsáveis pelas correções, utilizando modelos e procedimentos de melhores práticas adequadas às respectivas ameaças.

A Serena revisou ou irá revisaras cláusulas contratuais obrigatórias para a contratação de fornecedores e prestadores de serviços com intuito de adequar todos às políticas vigentes. Para contratações estratégicas e/ou que envolva o tratamento de dados pessoais, a Serena, previamente à assinatura do contrato, irá avaliar a necessidade de se proceder com a avaliação prévia do fornecedor

e/ou prestador (*vendor assessment*), para validar os controles aplicáveis às informações e/ou dados por eles tratados.

3.5. Gestão de continuidade de negócios (GCN)

A Serena envidará os esforços necessários para garantir a continuidade dos processos críticos de negócios, conforme normas e políticas internas aplicáveis.

As áreas de negócio e área de apoio são responsáveis pelo estabelecimento dos planos de continuidade operacionais de sua área e de testar regulamente dentro dos cronogramas estabelecidos esses planos.

3.6. Ações de prevenção e proteção

Serão adotadas rotinas padronizadas de prevenção e proteção dos processos e ativo, conforme previstas na norma interna, realizando análises de vulnerabilidade, testes de intrusão e outras avaliações específicas que certifiquem o cumprimento dos requisitos de segurança e as responsabilidades previamente estabelecidas.

Destacando a execução periódica de testes de ataque e invasão, visando monitorar a eficiência de seu sistema de proteção a vulnerabilidades cibernéticas, a Serena realiza testes, tanto em ambiente interno (na modalidade Gray Box) como o externo (na modalidade Black Box).

3.7. Controle de registros

Os registros (logs) de sistemas e aplicações serão gerados de acordo com as exigências legais, regulamentares, comerciais ou de negócio e protegidos contra cópia não autorizada, perda, destruição e falsificação que busquem garantir a rastreabilidade e segurança das informações sensíveis.

Não é permitido apagar, esconder ou modificar qualquer trilha de auditoria nos servidores e sistemas. Caso isso ocorra, o responsável estará sujeito às sanções internas aplicáveis.

3.8. Dispositivos móveis pessoais (BYOD)

Para ter acesso a aplicações e sistemas corporativos da Serena por meio de dispositivos móveis pessoais (Bring Your Own Device – BYOD), o colaborador e/ou

parceiro devem dar aceite ao "Termo de Responsabilidade" no qual formaliza que tal escolha é de sua exclusiva iniciativa, assumindo seu conhecimento e concordância com a Política de Segurança da Informação, o Código de Conduta e demais normas eventualmente aplicáveis.

O colaborador e/ou parceiro devem zelar pela segurança das informações da Serena, praticando comportamento seguro, não trafegando ou armazenando informações da empresa em canais ou locais não seguros.

O colaborador e/ou parceiro devem garantir conformidade do seu dispositivo pessoal aos itens da Norma de Uso de Dispositivos Móveis Pessoais (uso de rede, atualização do sistema operacional, configurações de bloqueio do dispositivo).

A companhia poderá fazer restrições de uso para equipamentos antigos ou que não ofereçam controle mínimo de segurança e gestão.

3.9. Monitoramento e testes

Objetivando avaliar a segurança dos controles adotados em cada um dos procedimentos operacionais, podem ser realizadas auditorias internas e externas regularmente.

Devem ser implementados controles internos efetivos para proteção dos RTICs (Recursos de Tecnologia da Informação e Comunicação) da Serena, garantindo a sua confidencialidade, integridade, autenticidade e disponibilidade sempre observando as melhores práticas de mercado e regulamentações vigentes.

A área de Segurança da Informação pode monitorar ou inspecionar os RTICs que estiverem em suas dependências ou que interajam com os ambientes da Serena sempre que considerar necessário.

As atividades realizadas nas estações de trabalho e servidores, bem como os acessos e utilização realizados no e-mail corporativo, internet e dados armazenados nas pastas de rede e sistemas da Serena como um todo são monitorados, registrados e podem ser utilizadas em caso de exigência legal, de regulador ou demanda da Companhia.

Os aplicativos críticos devem implementar a geração/manutenção de trilhas de auditoria, controle de versionamento do código fonte e segregação entre ambientes de produção e homologação. As ameaças cibernéticas devem ser analisadas em conjunto com as vulnerabilidades detectadas pela Segurança da

Informação nos ativos de informação e devem possuir monitoramento proativo da área de Segurança da Informação.

3.10. Plano de ação e de resposta a incidentes

O ambiente tecnológico deve ser monitorado continuamente para detectar eventos, anormalidades e Incidentes de Segurança da Informação.

A gestão, resposta, tratamento e redução de incidentes de segurança, estabelece e prevê condições em que eventos podem ser analisados, correlacionados, classificados, sinalizados e encaminhados para o correto atendimento dentro de uma estrutura gerenciada e padronizada para tratamento de tais incidentes.

Ações, rotinas, registros, definição de responsáveis e times, canais de comunicação, compartilhamento de informação com agentes externos e emissão de relatórios devem ser definidos de acordo com políticas internas, exigências regulatórias e/ou outros controles complementares que venham a ser exigidos.

Sem prejuízo das disposições constantes em normas internas específicas, os Incidentes de Segurança da Informação devem ser identificados e registrados para acompanhamento dos planos de ação e análise das vulnerabilidades respeitando o nível de exposição ao risco definido pela Serena.

a) **Comunicação de incidentes**: Os usuários devem comunicar imediatamente os casos de incidentes ao responsável por Segurança da Informação e ao DPO, por meio do seguinte canal: dpo@srna.co. Os incidentes deverão ser avaliados e investigados de forma a construir uma análise consistente de causa, riscos, partes envolvidas e planos de respostas. A avaliação deverá ser direcionada ao Diretor responsável pela Segurança Cibernética, bem como ao DPO da empresa, para que juntos deliberem sobre ações iniciais a serem tomadas. Classificada a relevância do incidente, a Serena deverá emitir comunicação aos envolvidos, informando a situação ocorrida e ações definidas, ao menos, de forma preliminar, informando/notificando sobre as atividades que serão tomadas posteriormente. Além disso, o responsável pela Segurança da Informação deve elaborar e divulgar ao Conselho de Administração o relatório anual sobre os planos de ação e resposta aos incidentes.
b) **Tentativa de burlar**: A mera tentativa de burlar às diretrizes e controles estabelecidos pela Serena, quando constatada, deve ser tratada como uma violação/incidente.

c) **Tratamento de vulnerabilidade identificadas**: O tratamento e as correções proativas das principais fragilidades ou fraquezas dos ativos de informação a serem utilizados devem estar registradas, sendo necessário avaliar o risco.
d) **Conflitos de interesse**: A Serena deve possuir um processo de concessão de acessos que utiliza critérios claros e objetivos para identificar conflitos de interesse que decorrem de limitações técnicas ou de situações devidamente autorizadas. Deverá haver monitoramento das atividades dos acessos e das ameaças cibernéticas.
e) **Registro do Incidente e elaboração de plano de ação**: Identificado um Incidente de Segurança da Informação, e com a devida comunicação ao responsável por Segurança da Informação e ao DPO, deve-se proceder com o registro formal de tal incidente, com todas as informações necessárias e disponíveis sobre o ocorrido, sem prejuízo de atualizações a medida em que novas informações forem surgindo. O plano de ação deverá ser elaborado pelos responsáveis de Segurança da Informação e pelo DPO, podendo ser envolvidos outros departamentos caso necessários para implementação das soluções e para administração de eventuais problemas. Tal plano deve conter definição expressa dos papéis e responsabilidades na solução do impasse, prevendo acionamento dos funcionários chave e contatos externos relevantes, caso aplicáveis. Deverão ser levados em consideração os cenários de ameaças previstos na avaliação de risco, havendo critérios para classificação dos incidentes, dependendo da gravidade. O plano de ação deverá prever os casos de necessidade de utilização das instalações de contingências nos casos mais severos, assim como o processo de retorno às instalações originais após o término do incidente. A documentação relacionada ao gerenciamento dos incidentes deverá ser arquivada para fins de auditoria.
f) **Comunicado aos Órgãos Externos**: A Serena comunicará os incidentes relevantes e interrupções de serviços relevantes que configurem uma situação de crise, bem como providências adotadas para o reinício dessas atividades para os órgãos externos, quando necessário, por meio do Departamento Jurídico e Departamento de Comunicação.

Programa de capacitação e conscientização

Programas de capacitação e conscientização para o correto manuseio das informações serão estabelecidos, de forma a desenvolver de forma contínua a cultura e a responsabilidade em segurança da informação pelos co-empreendedores.

Através das suas plataformas internas, a Serena promove um plano de conscientização recorrente sobre a importância da Segurança da Informação voltada para todo público interno, além de um resumo de segurança divulgado nos portais da empresa.

Medidas disciplinares

As violações às determinações da presente Política podem levar a sanções disciplinares, incluindo advertência, suspensão ou término imediato de contrato de trabalho ou de serviços, segundo critérios estabelecidos.

No caso de parceiros, violações da Política e das cláusulas de segurança da informação previstas no contrato podem causar desde advertências até o cancelamento do contrato e a aplicação das penas cabíveis de acordo com a Lei.

Atualizações e histórico de versões

Esta Política será revisada sempre que necessário e, a cada atualização, seu público-alvo interno deverá manifestar expressa adesão às suas normas.

Data de aprovação:	Aprovado por:	Versão:	Vigência:	Descrição:
12/06/2024	Conselho de Administração	2ª	De 12/06/2024 a 12/06/2026 ou até a publicação de nova versão se anterior ao fim da vigência	Versão atual
19/12/2021	Conselho de Administração	1ª	19/12/2021 até 11/06/2024.	Versão anterior

Anexo I – Gestão de acessos

Objetivo: O processo de concessão de acesso aos ativos de informação da Serena visa garantir acesso apropriado aos funcionários e terceiros, de acordo com suas funções na empresa, mantendo a segurança e integridade dos dados.

Procedimentos:

1. **Solicitação automatizada de acessos**:

- Durante o processo de Onboarding, movimentação ou novas requisições de acesso, um fluxo automatizado é acionado.
- A solicitação é iniciada eletronicamente, contendo detalhes como nome completo, data de nascimento, função, e motivo da solicitação.
- O sistema encaminha a solicitação para aprovação pelos gestores responsáveis, garantindo um processo rápido e eficiente.

2. **Criação de conta de acesso**:

- Contas são criadas automaticamente após a aprovação no fluxo automatizado.
- A equipe de recrutamento/gestão acompanha o processo para garantir que as informações essenciais estejam corretas.

3. **Alteração de conta de acesso**:

- Derivada de transferências ou mudanças nas funções dos co-empreendedores.
- O gestor anterior valida pendências e o novo gestor aprova as mudanças no sistema automatizado.

4. **Bloqueio automatizado de conta de acesso**:

- Durante o processo de rescisão ou mudança de função, um fluxo automatizado é acionado.
- O acesso é bloqueado automaticamente após a validação das pendências pela equipe de gestão de pessoas e gestor.

5. **Fluxo de aprovação**:

Os pedidos de acessos são encaminhados para os gestores apropriados para aprovação, garantindo que apenas as pessoas autorizadas tenham acesso aos recursos necessários.

Anexo II – Gestão de mudanças

Objetivo: A gestão de mudanças tem como objetivo garantir a preservação dos controles relacionados à disponibilidade, integridade, confidencialidade e autenticidade dos dados durante qualquer alteração em sistemas ou infraestrutura tecnológica relevante. Todas as mudanças serão geridas pelo Departamento de Tecnologia da Informação de forma planejada, aprovada, testada e obedecendo ao processo de gerenciamento de mudanças.

Processo de gestão de mudanças: Temos processos diferenciados para ambientes Cloud e ambientes On Premise.

Ambientes *On Premise* e *IaaS*: Para ambientes físicos e internos da Serena, Nuvem IaaS e Sistemas Corporativos, seguiremos o processo de Gestão de Mudança. Isso inclui o registro de mudança, execução de testes, métodos de rollback e aprovação ou reprovação da mudança. O registro também permite solicitações de mudanças emergenciais, que exigem intervenção imediata e são sujeitas à aprovação da liderança. Todos os casos são registrados para futuras auditorias e lições aprendidas.

Software Engineering – Cloud: Em ambientes DevOps, seguimos o processo CI/CD (Continuous Integration/Continuous Deployment). Isso envolve automação no agendamento da release, revisão das alterações em ambiente DEV por um desenvolvedor diferente do criador do código, merge do ambiente DEV para ambiente STAGING, homologação pelo time de QA em ambiente STAGING e, finalmente, merge do ambiente STAGING para ambiente PROD. Em casos não planejados, o Tech Lead é responsável por executar o processo de rollback, utilizando o merge da release anterior no ambiente PROD. Todas as etapas são registradas com logs de auditoria para futuras análises e lições aprendidas.

Ambientes SaaS: Para ambientes SaaS, seguimos os procedimentos determinados pelos parceiros contratados. Somos notificados sobre releases, geralmente trimestrais para todo o ambiente, com antecedência para testes e validações. A equipe Tech é responsável por gerenciar as validações prévias com os usuários-chave quando necessário e comunicar a empresa sobre essas atualizações.

Monitoramento e Relatórios: Mensalmente, durante as reuniões do Comitê GMUD, será apresentado um relatório detalhado que inclui a quantidade de mudanças normais, mudanças emergenciais, mudanças canceladas e mudanças executadas sem devido processo e aprovação. Esses relatórios visam garantir a transparência e responsabilidade em nossos processos de gestão de mudanças.

Anexo III – Gestão de operação

Objetivo: Realizar a gestão do ciclo de vida (aquisição, manutenção, atualização, suporte e descarte) dos recursos de tecnologia e telecomunicações da empresa e garantir aos usuários da empresa o pleno uso dos referidos recursos, levando em consideração as boas práticas do mercado, as práticas de segurança da informação e, quando aplicáveis, práticas de privacidade e proteção de dados definidas nessa Política.

Processo:

- **Suporte e gestão de crises**:

A área de tecnologia atende às solicitações dos usuários, considerando que estes devem fazer uso adequado dos recursos de tecnologia, através do registro de incidentes, dúvidas, dificuldades ou problemas no uso dos recursos e tecnologia.

A área de tecnologia disponibiliza e organiza canais de comunicação para organização da operação diária:

- Grupos em plataformas de comunicação: Há grupos fixos para o acompanhamento da operação e grupos específicos criados para gestões de crises pontuais.
- Sistema para reporte de chamados: Há o sistema da própria empresa, gerido pela área de tecnologia, e os sistemas de chamados dos fornecedores de serviços, como NOC e SOC.

- **Monitoramento:**

A empresa possui monitoramento 24 x 7 em duas frentes:

- **NOC** (Network Operations Center): Equipe que monitora a disponibilidade e performance do ambiente de tecnologia. Ao ocorrerem alarmes e eventos, o NOC notifica a equipe técnica da área de tecnologia da empresa e, imediatamente, inicia a atuação (junto à provedores de telecomunicações, fornecedores de tecnologia e demais provedores de serviços). O NOC também atua reativamente, quando usuários relatam

problemas ou dúvidas na utilização de recursos de comunicação da empresa.

- **SOC** (Security Operations Center): Essa equipe monitora, através de ferramentas como SIEM e CAS, o ambiente de tecnologia com foco em segurança da informação, acompanhando constantemente os eventos gerados no ambiente (alertas, alarmes e outros dados provenientes das diversas plataformas utilizadas pela empresa, seja em cloud e on premise). Cada alarme ou alerta é devidamente analisado e tratado. De acordo com os níveis de criticidade de cada evento, ações mais ou menos enérgicas podem ser tomadas. Os eventos relevantes são notificados por e-mail. Os eventos críticos requerem contato telefônico com a área de tecnologia da empresa, em geral após as medidas de mitigação e contenção do risco, ameaça ou incidente terem sido tomadas.

É realizada uma reunião semanal de acompanhamento dos indicadores relacionados à segurança da informação.