NORMA DE PROCEDIMENTO – SEFAZ/STIC Nº 008.2020

Tema:	Política de Segurança da Informação		
Emitente:	Secretaria de Estado da Fazenda – SEFAZ		
Sistema:	Sistema de Tecnologia da Informação e Comunicação		**Código:** SEFAZ/STIC
Versão:	15		**Vigência: 19/06/2020**

1. OBJETIVO

Todas as informações contidas neste documento são consideradas privilegiadas e pertencentes à SEFAZ-ES para uso interno. Este material inclui método de trabalho considerado sigiloso e a sua divulgação só deverá ser praticada com a finalidade específica de avaliação de seu conteúdo para aprovação e contratação deste serviço. Sendo assim, nenhuma parte deste documento poderá ser reproduzida, por quaisquer meios, sem a permissão da GETEC/SUINT. As informações contidas neste documento representam a visão atual da GETEC/SUINT em relação aos produtos e soluções nele contidas até a data de sua divulgação e publicação. A elaboração e confecção do seu conteúdo foram realizadas com base em documentações e publicações dos próprios fabricantes.

As logomarcas utilizadas são marcas registradas de seus respectivos fabricantes.

Dessa forma, esta Política de Segurança da Informação tem como objetivo evitar que quaisquer eventos indesejados ou inesperados possam colocar em risco a CONFIDENCIALIDADE, INTEGRIDADE, DISPONIBILIDADE, AUTENTICIDADE ou LEGALIDADE dos ativos de informação da SEFAZ, afetando assim seus serviços públicos ou prejudicando os proprietários das informações e seus usuários – principalmente o cidadão.

Esta PSI contempla as principais diretrizes a serem seguidas para que se possa garantir a segurança das informações envolvidas em seus processos, procedimentos, ambientes e ativos. Esta norma está alinhada com a legislação e regulamentações vigentes como a PESI - Política Estadual de Segurança da Informação e a LGPD – Lei Geral de Proteção de Dados e ainda com as melhores práticas de mercado, em conformidade com a ISO 27001.

A preocupação com a proteção da informação é um compromisso individual e contínuo de todas as partes envolvidas – servidores, estagiários, clientes, parceiros e prestadores de serviços. Cada um de nós é corresponsável pela eficácia desse conjunto de medidas e pela disseminação da cultura de segurança da informação – não só cumprindo a PSI, como também participando pró-ativamente desse processo, através de sugestões e críticas que possam ajudar a aprimorar nossas políticas de Segurança da Informação.

2. ABRANGÊNCIA

2.1 Secretaria de Estado da Fazenda.

3. FUNDAMENTAÇÃO LEGAL

3.1 **DECRETO Nº 2.884-R, de 21 de outubro de 2011**: Institui a Política Estadual de Segurança da Informação no âmbito do Poder Executivo do Estado - PESI; cria o Comitê Estadual de Segurança da Informação do Poder Executivo do Estado- CESI, cria o Comitê Estadual de Tratamento e Resposta a Incidentes de Segurança da Informação do Poder Executivo do Estado - CETRIN e dá outras providências.

3.2 **LEI FEDERAL Nº 13.709, de 14 de agosto de 2018**: Lei Geral de Proteção de Dados Pessoais – LGPD.

3.3 **LEI FEDERAL Nº 12.527, de 18 de novembro de 2011:** Regula o acesso às informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal.

4. DEFINIÇÕES

4.1 **Informação:** Ativo e recurso fundamental para o desenvolvimento das atividades da Secretaria da Fazenda do Estado do Espírito Santo. A informação pode existir em diversas formas, podendo ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos ou falada em conversas. Seja qual for a forma apresentada ou o meio pelo qual a informação é compartilhada ou armazenada, ela precisa sempre estar protegida adequadamente [ISO/IEC 27002:2013 (adaptado)].

4.2 **Ativos da Informação:** Todo bem que se relaciona com informação e que tenha valor para a organização [ISO/IEC 27000:2018], ou seja, softwares, sistemas, aplicações, ambientes, equipamentos, redes etc. – incluindo a própria informação.

4.3 **Confidencialidade:** Garantia de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados. [ISO/IEC 27000:2018].

4.4 **Integridade:** Garantia de que o dado ou a informação está inalterado conforme seu estado original. [ISO/IEC 27000:2018].

4.5 **Disponibilidade:** Garantia de usuários ou processos devidamente autorizados tenham acesso à informação e aos recursos a ela associados, sempre que forem requisitados. [ISO/IEC 27000:2018].

4.6 **Segurança da informação:** É definida como a proteção contra a perda da confidencialidade, integridade e disponibilidade da informação, adicionalmente, outras propriedades tais como autenticidade, responsabilidade, não repúdio e confiabilidade. [ISO/IEC 27002:2013].

4.7 **Incidente de segurança:** Um simples ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as atividades da Secretaria da Fazenda do Estado do Espírito Santo. [ISO/IEC 27000:2018 (adaptado)].

5. PREMISSAS DA POLÍTICA ESTADUAL DE SEGURANÇA DA INFORMAÇÃO

5.1 **Segurança Lógica:** de forma a assegurar o controle de acesso adequado à rede corporativa, aos sistemas e às informações do Poder Executivo, dos agentes públicos e cidadãos, prevenindo e detectando acessos não autorizados e adulterações de informações.

5.2 **Segurança de Pessoas:** de forma a minimizar erros humanos, fraudes, furtos, processos judiciais ou uso inadequado das informações e demais ativos da informação do Poder Executivo.

5.3 **Segurança Física:** de forma a assegurar o controle de acesso adequado de entrada e saída de ativos da informação nos diversos ambientes críticos e/ou restritos do Poder Executivo, para prevenir perda (s), dano (s) ou comprometimento das informações de seus órgãos.

5.4 **Gestão de Riscos, Incidentes e Continuidade de Serviços:** de forma a prevenir, controlar e tratar riscos, incidentes ou interrupções dos processos, serviços e ativos da informação do Poder Executivo, provendo a continuidade de processos-chave.

5.5 **Capacitação e treinamento:** de forma a capacitar e conscientizar o agente público nos aspectos relacionados aos fundamentos da segurança da informação, possibilitando criar uma cultura preventiva no uso da tecnologia da informação no ambiente profissional, e reduzir o impacto quando na ocorrência de um incidente de segurança dentro do respectivo órgão.

6. DIRETRIZES DA POLÍTICA ESTADUAL DA SEGURANÇA DA INFORMAÇÃO (PESI)

6.1 Propriedade:

Toda informação gerada, transmitida, adquirida ou custodiada pelo Poder Executivo do Estado do Espírito Santo, por meio de quaisquer de suas secretarias, órgãos, autarquias, empresas públicas e fundações de direito público é considerada um ativo e assim sendo, propriedade e patrimônio do Poder Executivo constituído (PESI).

6.1.1 Os ativos da informação da SEFAZ e seu ambiente informatizado devem estar de acordo com esta PSI e suas normas internas relacionadas à segurança da informação.

6.1.2 Os ativos da informação devem ter um responsável pela sua criação, aquisição, manutenção, atualização e segurança.

6.1.3 Todos os ativos da informação, quando hardware, devem ter um número de patrimônio para controle da SEFAZ.

6.1.4 Os ativos de informação da SEFAZ devem ser protegidos contra ações indevidas, intencionais ou acidentais que impliquem perda, destruição, inserção, cópia, extração, alteração, uso ou exposição indevida, em conformidade com os princípios da confidencialidade, integridade, disponibilidade e também com a LGPD.

6.2 Responsabilidade

É dever de todo agente público cumprir a Política Estadual de Segurança da Informação do Poder Executivo do Estado do Espírito Santo e assumir a responsabilidade pelos ativos e informações que estejam sob sua custódia, não podendo, em qualquer tempo ou sob qualquer propósito, apropriar-se deles, limitando-se aos direitos, privilégios e permissões concedidos formalmente para execução de suas atividades - PESI.

6.2.1 Todos os agentes públicos devem conhecer e cumprir as determinações desta Política de Segurança da Informação.

6.2.2 Todos os agentes públicos devem zelar pela INTEGRIDADE, DISPONIBILIDADE, AUTENTICIDADE, LEGALIDADE e CONFIDENCIALIDADE dos ativos de informação, não as utilizando para benefício próprio ou para fins que possam trazer prejuízos de qualquer natureza à SEFAZ, a terceiros ou ao Governo do Estado do Espírito Santo.

6.2.3 Todas as informações obtidas ou extraídas por empresa CONTRATADA quando da execução dos serviços deverão ser tratadas como confidenciais, sendo vedada qualquer reprodução, utilização ou divulgação a terceiros, mantendo sigilo absoluto sobre os dados, informações, documentos, especificações técnicas e comerciais que tenham conhecimento ou acesso em razão dos serviços executados.

6.2.4 Os usuários não devem compartilhar senhas, códigos, tokens, crachás, cartões de acesso, credenciais ou dispositivos de autenticação que lhes sejam de uso pessoal, fornecidos para seu uso exclusivo de serviços na SEFAZ, esta utilização será monitorada e sua utilização está sob total responsabilidade do usuário cadastrado.

6.2.5 Senhas de acesso a recursos e ambientes da SEFAZ-ES que precisem ser compartilhadas entre seus administradores ou equipes devem ser armazenadas criptografadas em sistemas seguros, específicos para este propósito. Exemplo: Kee Pass 2, Passbolt, etc.

6.2.6 Os usuários cadastrados são responsáveis pelos atos, danos e incidentes provocados pelo mau uso que fizerem das informações e recursos sob suas responsabilidades, sendo aos mesmos imputados as punições cabíveis.

6.3 Acesso Controlado

Os Órgãos e Entidades do Poder Executivo Estadual terão suas áreas físicas divididas em perímetros de segurança, conforme as necessidades de proteção dos ativos da informação mantidos, sendo o seu acesso controlado e quando pertinente sujeito a registro, monitoração e auditoria. A identificação de cada agente público, seja para acesso físico ou lógico, é pessoal e intransferível, não devendo ser compartilhado (PESI).

6.3.1 Acesso de Pessoas

- As regras de Acesso de Pessoas às unidades da SEFAZ estão descritas na Norma SEFAZ/SADM Nº 02 - Utilização do Prédio SEDE.

6.3.2 Acesso Lógico

- Os equipamentos da SEFAZ disponibilizados aos usuários (estações de trabalho, notebooks, tablets, smartphones etc.) devem ser e permanecer configurados de forma a minimizar a probabilidade de incidentes de segurança.
- Não é permitida a conexão de equipamentos pessoais nas redes locais cabeadas.
- Autorizações de acesso a sistemas, ambientes e demais recursos devem ser concedidas mediante necessidade e sob o princípio dos privilégios mínimos.
- Todo prestador de serviço contratado pela SEFAZ deve ter um usuário e senha para acesso a qualquer solução dentro das dependências da Instituição, estando sujeitos às mesmas regras de sigilo, proteção e conformidade desta PSI e sob o princípio de privilégios de acesso mínimos.
- Todo agente público deve ter seu usuário e senha cadastrados no sistema de acordo com a Norma SEFAZ STIC nº 005-2020 – Acesso às Redes da SEFAZ

6.4 Classificação da Informação

As informações serão classificadas quanto ao seu grau de sigilo, conforme seu valor, importância estratégica, criticidade e base legal que a proteja para os objetivos dos serviços do Poder Executivo do Estado do Espírito Santo (PESI).

6.4.1 Toda informação, quando necessário, deve ser classificada quanto ao seu grau de sigilo no momento de sua geração ou obtenção. Essa classificação deve ser preservada (incluindo eventuais alterações) durante todo o seu ciclo de vida, de acordo com a Lei Federal Nº 12.527, de 18 de novembro de 2011, que regula o acesso às informações.

6.4.2 O Governo do Estado, atendendo à solicitação da Secretaria de Controle e Transparência do Estado – SECONT, criou a plataforma e-Docs, onde toda informação neste sistema tramitada, deve ser tratada de acordo com o módulo de Gestão da Informação e Classificação (GIC) que prevê os seguintes níveis de acesso:

i. **Público** - O documento pode ser acessado por qualquer usuário que tenha efetuado login no sistema e-Docs.

ii. **Organizacional** - O documento pode ser acessado por qualquer servidor lotado em qualquer um dos órgãos por onde este documento transitar.

iii. **Sigiloso** - O documento só pode ser acessado por quem o captura, quem o assina, ou quem o recebe (via tramitação avulsa ou processo administrativo).

iv. **Classificado** - O documento só pode ser acessado por quem tiver permissão para visualizar documentos classificados de acordo com a lei de acesso à informação, pode ser classificado como reservado, secreto ou ultrassecreto.

6.5 Auditoria e Conformidade

O cumprimento da Política Estadual de Segurança da Informação e de outros dispositivos legais será acompanhado e auditado pelo Poder Executivo do Estado do Espírito Santo e apoiado pelo Instituto de Tecnologia da Informação e Comunicação do Espírito Santo - PRODEST, que se reserva o direito de monitorar o uso de ativos da informação e serviços providos, assim como o tráfego através das suas redes de comunicação, incluindo o acesso à internet e o uso do correio eletrônico. Tais ações serão realizadas para identificar a efetividade dos controles implementados e aferir a conformidade com a Política Estadual de Segurança da Informação, estatutos, regulamentos e leis (PESI).

6.5.1 Acesso à Internet

i. É proibido acessar a Internet através das redes da SEFAZ para praticar, incitar, induzir ou promover qualquer ideia, ato ou atividade ilegal que violem esta PSI.

ii. A SEFAZ registra todos os acessos à Internet efetuados através de suas redes ou dispositivos e os relaciona com o usuário, para garantir a segurança de suas informações ou a utilização adequada dos recursos de sua propriedade e sob sua responsabilidade.

iii. A SEFAZ se reserva no direito de bloquear, temporária ou permanentemente, o acesso a determinados websites e serviços de Internet.

iv. Caso o agente público necessite de acesso a um ou mais recursos que esteja bloqueado, o mesmo deverá abrir uma requisição no sistema de suporte (CSS) da SEFAZ e solicitar à chefia imediata a liberação de tal acesso.

v. Agentes públicos que desejem acesso à Internet através de seus dispositivos móveis pessoais nas dependências da SEFAZ devem utilizar apenas a rede sem fio WFBYOD ou WF_ACESSO_VISITANTE.

vi. Visitantes que desejem acesso à Internet através de seus dispositivos móveis pessoais nas dependências da SEFAZ devem utilizar apenas a rede sem fio WF_ACESSO_VISITANTE, onde o visitante será direcionado para um portal de cadastro no sistema da SEFAZ.

vii. O acesso para visualização de vídeos pela WEB de sites permitidos, como YouTube ou qualquer tipo de streaming podem ser acessados no horário de almoço, de 12h as 13h30min, desde que não viole nenhum ponto desta PSI.

viii. Os acessos a websites que são categorizados como “Shopping” são liberados através de uma cota de utilização de 30 minutos por dia e devem ser utilizados moderadamente.

ix. Não é permitida a utilização de softwares ou Proxys externos que burlem o sistema de utilização de internet da SEFAZ.

6.5.2 Uso do Correio Eletrônico

i. As normas do uso do correio eletrônico estão descritas na Norma SEFAZ STIC nº 006-2020 - Uso do Correio Eletrônico.

6.5.3 Tráfego nas Redes de Comunicação da SEFAZ

i. Os agentes públicos devem aceitar que as atividades por eles executadas utilizando recursos da SEFAZ poderão por ela ser monitoradas, fiscalizadas e auditadas a qualquer tempo, mesmo sem aviso prévio ou anuência dos mesmos.

ii. Sempre que possível, as comunicações entre ativos da informação devem ser criptografadas.

iii. Todos os ativos da informação devem gerar logs e se possível enviar esses logs para um sistema que seja específico para este fim.

iv. Os logs críticos gerados e enviados para um sistema de armazenamento de logs devem ser mantidos por pelo menos 1 (um) ano.

6.6 Gestão de Riscos

O Poder Executivo do Estado do Espírito Santo, por meio de seus Órgãos e entidades, garantirá a aplicação de controles eficazes de proteção as suas informações, baseado em um processo periódico de análise e avaliação de riscos dos seus ativos de informação nos termos das características dos serviços público, com o apoio de fontes adicionais, como relatórios de auditorias e análises críticas de incidentes de segurança da informação (PESI).

i. Deve ser realizada, trimestralmente, uma análise de riscos de segurança nos ativos de informação envolvidos nos processos e sistemas mais críticos da SEFAZ, seguida da execução dos planos de tratamento necessários.

ii. Mudanças em processos, serviços, equipamentos, sistemas ou ambientes, sejam tecnológicos ou não, devem sempre que possível, ser precedidas de análises de riscos que identifiquem possíveis impactos relacionados à segurança da informação, visando garantir a aplicação das medidas que se fizerem necessários.

iii. Todos os ativos de informação da SEFAZ devem estar com seus patches críticos atualizados, desde que este não impacte no pleno funcionamento da aplicação, sistema ou recurso final.

6.7 Gestão da Continuidade

A Gestão de Continuidade de Serviços tem por objetivo "não permitir a interrupção das atividades dos negócios e proteger os processos críticos contra efeitos de falhas ou desastres significativos e assegurando a sua retomada em tempo hábil, se for o caso". (ISO/IEC 17799, 2005). A Gestão de Continuidade de Serviços deve criar, manter e incorporar um plano de ação à organização, composto por uma série de procedimentos e medidas que devem ser executados perante um incidente considerado extremamente crítico.

Os Órgãos e Entidades do Poder Executivo do Estado do Espírito Santo devem, então, dispor de planejamento e de mecanismos adequados à pronta recuperação de suas operações, no menor tempo possível, como forma de precaver-se dos efeitos desastrosos de eventos que causem interrupções significativas em parte, ou mesmo em todos os seus serviços (PESI).

i. Planos de contingência, recuperação de desastres e respostas a incidentes de segurança da informação devem ser elaborados, testados e atualizados periodicamente, visando garantir a continuidade dos serviços mais críticos quando da ocorrência de eventos que afetem sua disponibilidade.

ii. Toda alteração em ativo que for considerado crítico deve ser aprovada pela GETEC, através de uma reunião de mudanças.

iii. A gestão da cópia de segurança e recuperação de dados está descrita na Norma SEFAZ STIC nº 007-2020 Gestão de Cópia de Segurança e Recuperação de Dados.

6.8 Conscientização do Agente Público, Capacitação e Treinamento

A Política Estadual de Segurança da Informação deve ser cumprida por todo agente público pertencente ao Poder Executivo do Estado do Espírito Santo, independente do vínculo contratual ou jurídico a que estejam submetidos ou do nível hierárquico, cargo ou função em que estejam inseridos.

O Poder Executivo do Estado do Espírito Santo, compromete-se a capacitar e conscientizar o agente público quanto à importância das ações preconizadas pela Política Estadual de Segurança da Informação em suas atividades, buscando o comprometimento para com a proteção dos recursos oferecidos pelo Governo (PESI). Nesse sentido, recomenda-se:

i. À SEFAZ, a promoção de pelo menos 1 (uma) palestra ao longo do ano sobre a conscientização da segurança da informação, como também acesso ao material disponibilizado na plataforma EAD da SEFAZ;

ii. A Todos os agentes públicos, assim que possível, que façam a leitura para ~~e~~ tomar ciência das mais variadas ameaças na internet, para esta ciência sugerimos a leitura da “Cartilha de Segurança para Internet” fornecida pelo “Núcleo de Informação e Coordenação do Ponto BR Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil”. Com esta leitura conseguimos aumentar a própria segurança tecnológica dos usuários e fortalecer a cultura de segurança da informação da SEFAZ.

6.9 Comprometimento, Violação, Sanções, Fiscalização e Controle

As leis, normas e contratos regulamentadores referentes à proteção adequada do sigilo profissional, assim como da propriedade intelectual e legal relacionados às atividades executadas dentro da estrutura do Poder Executivo do Estado do Espírito Santo, deverão ser rigorosamente cumpridos.

Quaisquer eventos ou incidentes, de Segurança da Informação, sejam supostos ou evidenciados, devem ser comunicados imediatamente ao Comitê Estadual de Tratamento e Resposta a Incidentes de Segurança da Informação do Poder Executivo do Estado do Espírito Santo - CETRIN.

O agente público que deixar de atender ao disposto na Política Estadual de Segurança da Informação, injustificadamente, responderá solidariamente pelos prejuízos que a Administração vier a sofrer, se apurada sua culpa ou dolo, em sindicância ou processo administrativo disciplinar. É importante ressaltar que a conivência ou omissão por parte dos agentes públicos perante as violações de segurança efetuadas por outros usuários serão consideradas como faltas graves (PESI).

6.9.1 Todos os agentes públicos devem comunicar quaisquer incidentes de segurança da informação ocorridos ou prováveis de ocorrerem, enviando um e-mail para sgi@sefaz.es.gov.br e, quando possível, anexando as provas ou evidências do fato.

6.9.2 São considerados incidentes de segurança da informação quaisquer eventos que violem ou coloque em risco a CONFIDENCIALIDADE, INTEGRIDADE, DISPONIBILIDADE, AUTENTICIDADE ou LEGALIDADE de informações pertencentes, processadas ou custodiadas pela SEFAZ, bem como o não cumprimento dos termos desta PSI. São alguns exemplos de incidentes de segurança da informação:

i. Indisponibilidade total ou parcial de serviços, sistemas, sites, aplicações, equipamentos ou recursos;
ii. Uso impróprio, indevido ou não autorizado de ativos de informação (incluindo a própria informação);
iii. Violações ou falhas de controles ou recursos de segurança;
iv. Roubo, furto ou perda de dados (incluindo em mídias ou documentos em papel), equipamentos ou credenciais;
v. Falhas nas rotinas de segurança patrimonial ou de controle de acesso aos setores;

vi. Entrada e saída não controlada de ativos de informação (equipamentos, documentos confidenciais etc.)
vii. Vazamento ou divulgação não autorizada de informações sigilosas;
viii. Existência de ameaça ou iminência de ocorrência de incidente (mesmo que ainda não tenha ocorrido);

6.9.3 A fiscalização deve se projetar por sistemas de correlação de eventos de segurança da informação.

6.9.4 Todo agente público tem o dever de manter esta PSI e notificar nos sistemas já conhecidos todo incidente de segurança que presenciar.

6.10 Divulgação e Atualização

O Comitê Estadual de Segurança da Informação é responsável por definir, atualizar, publicar, viabilizar a divulgação e fazer cumprir esta Política e os demais documentos que a compõe, assim como angariar comprometimento de áreas e pessoas e criar formas de determinar o seu cumprimento junto aos Órgãos e Entidades do Poder Executivo Estadual (PESI).

6.10.1 Compete à GETEC definir, conceber, elaborar, implementar, revisar e efetuar a análise crítica da governança, diretrizes, políticas, normas, auditorias, ambientes, processos, procedimentos, contratações, produtos e serviços que afetem a segurança das informações pertencentes, custodiadas ou processadas pela SEFAZ.

7. NÚMERO DA VERSÃO E DATA

7.1 Versão e datas:

Versão	Data	Autor / Revisor
V1	28/09/2018	Carlos Sá
V2	23/01/2019	Carlos Sá
V3	15/10/2019	Lucas Kutz
V4	29/10/2019	Moacir Bortoloso
V5	12/11/2019	Carlos Sá
V6	13/11/2019	Lucas Kutz
V7	25/11/2019	Reunião de Gestores

V8	08/01/2020	Lucas Kutz
V9	10/01/2020	Carlos Sá
V10	10/01/2020	Lucas Kutz
V11	27/04/2020	Carlos Sá (Colaboração: Bruno Dias, Andressa Pavão, Sérgio Ricardo e Fábio Aguiar
V12	05/05/2020	Reunião SUINT (Carlos, Fábio, Lucas, Mauricio e Moacir)
V13	07/05/2020	Marcelo Cornélio / Carlos Sá
V14	20/05/2020	Lucas Kutz
V15	18/06/2020	Reunião SUINT (Carlos, Fábio, Lucas, Mauricio e Moacir)

8. ASSINATURAS

EQUIPE DE ELABORAÇÃO	EQUIPE DE PADRONIZAÇÃO
Marcelo Azeredo Cornélio Gerente de Tecnologia da Informação	**Eduardo Pereira de Carvalho** Supervisor de Área Fazendária
Carlos Eduardo Meneguelli de Sá Contrato Temporário	**Eliane Canal Leite da Silva** Coordenadora de Projetos
Lucas Kutz Valverde Assessor Especial Nível I	**Marta Gonçalves Achiamé** Supervisor de Área Fazendária
	Jacqueline de Souza França Subgerente da SUDOR