	<b>NEXA</b>  <b>Padrão Gerencial</b>	<b>Código</b>	PG-CTI-GTI-001-PT
		<b>Revisão</b>	1.0
	<b>Título:</b>  Controle de Acesso Lógico	<b>Área</b>	TI
		<b>Páginas</b>	1 / 13

## 1. OBJETIVO

O Controle de Acesso Lógico tem o objetivo de descrever as diretrizes necessárias à aplicação de melhores práticas e fluxo no processo de concessão e exclusão de acessos na admissão e demissão de funcionários.

Este documento detalha todo o processo de inserção de um novo funcionário na base do SAP até o processo de concessão de acesso à rede e revogação. Este documento e os processos que nele estão detalhados serão revisados e atualizados conforme necessário.

O gerente responsável pela área de Tecnologia da Informação da companhia é a autoridade responsável para aprovação desses procedimentos, em consulta com o responsável pela área do DHO.

A área de Tecnologia da Informação deve prover padrões para que os envolvidos neste processo como um todo consigam realizar suas atividades de maneira transparente e simplificada, garantido assim efetividade deste controle no âmbito dos recursos de tecnologia.

## 2. ABRANGÊNCIA

Este procedimento se aplica as Unidades Nexa e suas subsidiárias.

## 3. DEFINIÇÕES

Para os efeitos deste Controle de Acesso Lógico, aplicam-se as seguintes definições.


### 3.1 Acesso Lógico

Acesso a redes de computadores, sistemas e estações de trabalho por meio de autenticação.

### 3.2 Autenticação

É o ato de confirmar que algo ou alguém é autêntico, ou seja, uma garantia de que qualquer alegação de ou sobre um objeto é verdadeira.

<b>Elaborador:</b> Fabiano Alves	<b>Classificação:</b> Uso Interno	<b>Aprovador:</b> José Furtado
-------------------------------------	--------------------------------------	-----------------------------------

	<b>NEXA</b>	<b>Código</b>	PG-CTI-GTI-001-PT
		<b>Revisão</b>	1.0
	<b>Padrão Gerencial</b>	<b>Área</b>	TI
		<b>Páginas</b>	2 / 13
	<b>Título:</b>		
	Controle de Acesso Lógico		

### 3.3 Bloqueio de Acesso

Processo que tem por finalidade suspender temporariamente o acesso.

### 3.4 Controle de Acesso

Conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso.

### 3.5 Credenciais ou Contas de Acesso

Permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física como crachá, cartão e selo ou lógica como identificação de usuário e senha.

### 3.6 Usuário

Empregados, terceiros, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos ativos de informação de uma área.

### 3.7 Empregado

Pessoas contratadas no regime empregatício da legislação local vigente.

### 3.8 GQI-Nexa


Sistemas onde os documentos são disponibilizados em meio eletrônico.

## 4. PAPÉIS E RESPONSABILIDADES

Todos os empregados e terceiros da companhia devem agir de acordo com os princípios estabelecidos nesta política.

Existem vários riscos envolvidos, portanto é de responsabilidade das áreas de Tecnologia da Informação e DHO que os processos aqui descritos sejam seguidos, incluindo o conhecimento da Política de Segurança da Informação.

<b>Elaborador:</b> Fabiano Alves	<b>Classificação:</b> Uso Interno	<b>Aprovador:</b> José Furtado
-------------------------------------	--------------------------------------	-----------------------------------

	<b>NEXA</b>	<b>Código</b>	PG-CTI-GTI-001-PT
		<b>Revisão</b>	1.0
	<b>Padrão Gerencial</b>	<b>Área</b>	TI
		<b>Páginas</b>	3 / 13
	<b>Título:</b>		
	Controle de Acesso Lógico		

Para ser efetiva, esta política deve ter um esforço em conjunto que envolve as áreas de DHO e Tecnologia da Informação. É fundamental que exista um reconhecimento da necessidade do trabalho em equipe. Esta documentação esclarece as responsabilidades dos envolvidos como os passos que eles devem seguir para que os processos sejam realizados de uma maneira transparente e com segurança.

Os papéis e responsabilidades estão definidos na Matriz RACI disponível na Intranet.

#### **4.1 Comunicação entre as Partes**

A área de DHO deve comunicar a área de Tecnologia da Informação e GRC através de e-mail, para que os mesmos tenham ciência da entrada e saída dos empregados, e façam uma revisão periódica para as exclusões. Cabe frisar que o processo de bloqueio e exclusão são automáticos, portanto esta atividade ocorre apenas como uma checagem adicional.


Qualquer problema relativo ao processo de replicação, a área de Tecnologia da Informação ficará responsável em avisar a área do DHO e aos usuários, dando um retorno até a normalização dos sistemas.

#### **4.2 Área de Tecnologia da Informação (TI)**

A área de tecnologia da informação tem a responsabilidade pela operacionalização tecnológica desta política e pela sustentação dos termos definidos neste documento, e para isso suas responsabilidades incluem:

- Revisar as questões descritas neste documento ao menos duas vezes ao ano;
- Analisar e informar aos administradores do ambiente de gestão de identidade os problemas ocorridos em casos de inoperância em algum processo ou falha dos sistemas envolvidos;
- O responsável pela área de Tecnologia da Informação terá a responsabilidade de, juntamente com sua equipe, garantir que esta política

<b>Elaborador:</b> Fabiano Alves	<b>Classificação:</b> Uso Interno	<b>Aprovador:</b> José Furtado
-------------------------------------	--------------------------------------	-----------------------------------

	<b>NEXA</b>  <b>Padrão Gerencial</b>	<b>Código</b>	PG-CTI-GTI-001-PT
		<b>Revisão</b>	1.0
	<b>Título:</b>  Controle de Acesso Lógico	<b>Área</b>	TI
		<b>Páginas</b>	4 / 13

esteja devidamente elaborada e aprovada no intuito de garantir a sua plena aplicabilidade.

#### 4.3 Área de Recursos Humanos (DHO)

É de total responsabilidade da área do DHO a inclusão dos dados do novo empregado no sistema do SAP, como também realizar a baixa no sistema uma vez que o mesmo deixe a companhia, e para isso suas responsabilidades incluem:

- Quando houver uma nova inclusão no SAP, a área de DHO deve informar através de comunicado quando a inclusão foi realizada, e informar os dados do empregado, como nome completo, área, cargo, etc.

A área do DHO também deve informar, através de comunicado sobre os empregados que estão deixando a companhia para que a área de Tecnologia da Informação e GRC possa realizar revisões esporádicas. Cabe mencionar que todo o processo de inclusão e baixa dos usuários de rede são feitos de uma maneira automática, conforme já mencionado.

#### 5. DOCUMENTOS DE REFERÊNCIA

- PC-CTI-GTI-001-PT – Política de Segurança da Informação.
- Norma ABNT NBR ISO/IEC 27001:2013.
- Norma ABNT NBR ISO/IEC 27002:2013.


#### 6. CONTROLE DE ACESSO À REDE E SISTEMAS OPERACIONAIS

Esta seção descreve os requisitos para assegurar que os direitos de acesso sejam aplicados em redes internas e sistemas operacionais.

##### 6.1 Sistemas Operacionais

- Todos os sistemas operacionais devem empregar um processo seguro de login para minimizar o vazamento de informações.

<b>Elaborador:</b> Fabiano Alves	<b>Classificação:</b> Uso Interno	<b>Aprovador:</b> José Furtado
-------------------------------------	--------------------------------------	-----------------------------------


	<b>NEXA</b>	<b>Código</b>	PG-CTI-GTI-001-PT
		<b>Revisão</b>	1.0
	<b>Padrão Gerencial</b>	<b>Área</b>	TI
		<b>Páginas</b>	5 / 13
	<b>Título:</b> Controle de Acesso Lógico		

- Os usuários devem ser autenticados nos sistemas operacionais com o mínimo de segurança, utilizando ID de usuário e senha.
- As sessões devem ser bloqueadas após um período de inatividade especificado. Os usuários devem voltar a autenticar para desbloquear a sessão.
- O acesso a sistemas sensíveis deve ser limitado ao tempo e à duração para os quais o acesso é necessário.

## 6.2 Rede

- O acesso aos serviços de rede deve ser gerenciado pela área de Operação de TI (OGS) ou através de seus parceiros.
- Os usuários só devem ser autorizados a utilizar os serviços aos quais tenham acesso.
- O acesso às portas de diagnóstico e configuração devem ser restritos e controlados.
- As portas e serviços abertos devem ser mantidos ao mínimo exigido para os requisitos de negócios da companhia.
- A rede da empresa deve ser logicamente segregada, zonificada e classificada em domínios, com base em seus requisitos de segurança e riscos.
- Devem ser estabelecidos limites lógicos (por exemplo, firewalls) para segregar domínios de rede.
- A classificação de risco e as necessidades de negócios dos domínios devem reger o nível de proteção requerida.
- Os controles de roteamento devem ser implementados para garantir que conexões e fluxos de informações não violem os requisitos de controle de acesso estabelecidos nesta política.
- Sempre que possível, os controles de roteamento devem validar endereços de origem e de destino contra restrições de segurança.

<b>Elaborador:</b> Fabiano Alves	<b>Classificação:</b> Uso Interno	<b>Aprovador:</b> José Furtado
-------------------------------------	--------------------------------------	-----------------------------------

	<b>NEXA</b>  <b>Padrão Gerencial</b>	<b>Código</b>	PG-CTI-GTI-001-PT
		<b>Revisão</b>	1.0
	<b>Título:</b>  Controle de Acesso Lógico	<b>Área</b>	TI
		<b>Páginas</b>	6 / 13

- Somente os usuários autorizados podem acessar as pastas de rede mediante aprovação do responsável (owner) de cada pasta e na sua ausência o Gerente Geral da Área.

### 6.3 Banco de Dados

Os sistemas de banco de dados devem limitar o acesso aos recursos de informações da empresa somente a usuários autorizados, de acordo com os requisitos do negócio. O acesso deve ser limitado e quando possível, por funções específicas (por exemplo, leitura, modificação, exclusão).


O acesso aos recursos de banco de dados deve ser controlado pela autenticação do usuário para validar a sua identidade. Através do processo de autorização, o usuário validado deve ter acesso ao recurso protegido e as ações permitidas (leitura, gravação/adição, gravação/atualização ou exclusão) são verificadas.

## 7. GESTÃO DE SENHAS

O nível de segurança fornecido por uma senha como um método de autenticação depende da sua complexidade e do manuseio correto. Esta seção procura evitar o comprometimento de senhas e o risco resultante de divulgação de informações da firma através da introdução de controles para garantir que as senhas sejam suficientemente seguras.

- Deve haver um processo formal para a alocação e uso de senhas que deve incluir os seguintes requisitos mínimos:
- As senhas devem ser inicialmente definidas pela área de Tecnologia da Informação e alteradas na primeira utilização;
- As senhas não devem ser anotadas;
- As senhas devem ser transmitidas e armazenadas de maneira segura;
- As senhas padrão não devem ser utilizadas.
- Deve ser exigido por padrão a utilização de senhas fortes e garantir que as mesmas sejam utilizadas com segurança.
- Os seguintes requisitos devem ser impostos:

<b>Elaborador:</b> Fabiano Alves	<b>Classificação:</b> Uso Interno	<b>Aprovador:</b> José Furtado
-------------------------------------	--------------------------------------	-----------------------------------

	<b>NEXA</b>  <b>Padrão Gerencial</b>	<b>Código</b>	PG-CTI-GTI-001-PT
		<b>Revisão</b>	1.0
	<b>Título:</b>  Controle de Acesso Lógico	<b>Área</b>	TI
		<b>Páginas</b>	7 / 13

- Alteração das senhas a cada 60 dias;
- Não reutilizar as últimas 10 senhas anteriormente configuradas.
- As senhas devem ser alteradas imediatamente, se os usuários suspeitarem que foram comprometidas e conhecidas por outras partes.
- O fingerprint poderá ser utilizado.

### 7.1 Alteração de Senhas

A área de Tecnologia da Informação deve implementar um processo para alterar senhas de usuários quando necessário. Este processo deve assegurar que:

- A equipe tenha autorização apropriada antes da redefinição da senha;
- Novas senhas sejam transmitidas de maneira segura ao usuário.
- O Usuário deve alterar a senha no primeiro Login

## 8. PROCESSO DE CONCESSÃO DE ACESSOS


As definições desta seção estabelecem os controles existentes para manutenção da política de concessão e exclusão de acessos no processo de admissão, a fim de garantir o alinhamento com os requisitos de negócios da companhia.

### 8.1 Princípios do Controle de Acesso

Os procedimentos de controle de acesso devem incluir e respeitar as seguintes orientações:

- O acesso é concedido com base no princípio do menor privilégio;
- O acesso é concedido com base em regras de negócios;
- Os papéis de gerenciamento de acesso são segregados;
- Os acessos são registrados e o acesso à informação são armazenados para referência futura.

<b>Elaborador:</b> Fabiano Alves	<b>Classificação:</b> Uso Interno	<b>Aprovador:</b> José Furtado
-------------------------------------	--------------------------------------	-----------------------------------

	<b>NEXA</b>  <b>Padrão Gerencial</b>	<b>Código</b>	PG-CTI-GTI-001-PT
		<b>Revisão</b>	1.0
	<b>Título:</b>  Controle de Acesso Lógico	<b>Área</b>	TI
		<b>Páginas</b>	8 / 13

## 8.2 “Menor privilégio” e “Necessário Saber”

Privilégios de acesso são atribuídos de acordo com os princípios "privilégio mínimo" e "necessário saber". O princípio do menor privilegio deve ser aplicado a empregados e terceiros, e prevê que cada usuário só possui os privilégios necessários para realizar uma tarefa específica.

## 8.3 Segregação de Função

O princípio da segregação de funções deve ser aplicado aos empregados e sócios. As seguintes funções devem ser minimamente divididas entre si:

- A pessoa que fez o pedido de acesso;
- Quem aprova o pedido;
- Quem executa o pedido.

## 8.4 Contratação de Novos Empregados (Admissão)

Ao admitir um novo empregado, a área do DHO deverá seguir as recomendações existentes na política de segurança da informação. Quando a área do DHO recebe os documentos do novo profissional deve-se realizar o cadastro do mesmo no sistema SAP RH.

Uma vez que o usuário esteja disponível na base do SAP a área de DHO recebe um e-mail automático, confirmando que o usuário foi disponibilizado na base do sistema. Após concluir essa etapa é enviado ao Gestor imediato do empregado o checklist para criação dos acessos básicos de rede que é solicitado via chamado. Os acessos específicos são requisitados posteriormente e necessitam de aprovação do gerente responsável.


## 8.5 Contratação de Terceiros

A área de T.I. deve seguir e ter conhecimento da Política de Segurança de Informação relativo aos terceiros antes de efetuar qualquer ação neste sentido.

O processo de requisição deve ter aprovação do gerente da área responsável e também do gerente de Tecnologia da Informação. Dado o cenário

<b>Elaborador:</b> Fabiano Alves	<b>Classificação:</b> Uso Interno	<b>Aprovador:</b> José Furtado
-------------------------------------	--------------------------------------	-----------------------------------



	<b>NEXA</b>  <b>Padrão Gerencial</b>	<b>Código</b>	PG-CTI-GTI-001-PT
		<b>Revisão</b>	1.0
	<b>Título:</b>  Controle de Acesso Lógico	<b>Área</b>	TI
		<b>Páginas</b>	9 / 13

mencionado somente deve iniciar a atividade de criação da conta após as devidas aprovações.

A conta do terceiro não deve ser inserida em nenhuma lista de distribuição da companhia.


Por questões de segurança a conta deve ser colocada para expirar a cada 60 dias e ser mantida em uma OU (Organization Unit) separada. Adicionalmente é extremamente recomendado que o responsável informe a data correta de expiração (tempo de uso), etc.

### 8.6 Acesso Remoto para Terceiros

- Sistemas e aplicações devem ser configurados para permitir o acesso remoto somente se houver necessidades de negócios.
- Apenas empregados e os terceiros devidamente aprovados podem ter permissão para se conectar remotamente à rede.
- O acesso remoto aos recursos de rede, contendo informações confidenciais de clientes, deve empregar métodos seguros de autenticação.
- Os dispositivos móveis devem funcionar em conformidade com a política da rede para estabelecer uma conexão de acesso remoto a sistemas de informação que são desenvolvidos, operados e utilizados na rede.
- O acesso remoto a sistemas de informação de rede deve ser aprovado, concedido e revisado de acordo com os requisitos descritos nesta política.
- O acesso de terceiros a sistemas e aplicações deve ser feito de forma aberta e monitorado, seguindo autorização e reconhecimento.
- Acessos diretos são estritamente proibidos para sistemas de terceiros, para aplicações locais e remotamente.
- No caso de acesso remoto, todos os acessos deverão ser registrados.
- Quando for necessário, para usuários com acesso de super-usuário ou direitos administrativos, deve haver um sistema de gerenciamento de privilégios de acesso, não permitindo o uso direto de senhas administrativas.

### 8.7 Determinar e Alterar um Endereço Eletrônico

<b>Elaborador:</b> Fabiano Alves	<b>Classificação:</b> Uso Interno	<b>Aprovador:</b> José Furtado
-------------------------------------	--------------------------------------	-----------------------------------

	<b>NEXA</b>	<b>Código</b>	PG-CTI-GTI-001-PT
		<b>Revisão</b>	1.0
	<b>Padrão Gerencial</b>	<b>Área</b>	TI
		<b>Páginas</b>	10 / 13
	<b>Título:</b>		
	Controle de Acesso Lógico		

Uma vez que a área do DHO inseriu as informações do novo empregado no sistema SAP, o fluxo segue conforme mencionado no item acima 8.4. O endereço eletrônico é determinado pelo sistema FIM (Forefront Identity Manager) , que fará a melhor escolha do alias disponível, seguindo os padrões.

O usuário não deve estipular qual endereço eletrônico ele deve usar, uma vez que este processo é automático com exceção de casos comuns como casamento e separação. As regras de política do AD (Active Directory) devem ser mantidas e respeitadas.

### 8.8 Contas de Serviço

O processo de criação de uma conta de serviço não envolve a área do DHO, a área de Tecnologia da Informação deverá solicitar via chamado que irá usar o sistema FIM e entrar com os dados diretamente no sistema, onde o mesmo ficará disponível na base do AD (Active Directory).


O processo de requisição deve ter a aprovação do gerente da área responsável, e também pela área de Segurança da Informação . Dado o cenário mencionado somente deve iniciar a atividade de criação da conta após as devidas aprovações.

A conta de serviço não deve ser inserida em nenhuma listagem de distribuição da companhia.

Por questões de segurança, a conta deve ser colocada para expirar a cada 90 dias na base do AD (Active Directory). Adicionalmente é extremamente recomendado, que o responsável informe a data correta de expiração (tempo de uso), etc.

Também é recomendado que uma conta de serviço seja convertida de tipo "regular" para "shared".

<b>Elaborador:</b> Fabiano Alves	<b>Classificação:</b> Uso Interno	<b>Aprovador:</b> José Furtado
-------------------------------------	--------------------------------------	-----------------------------------

	<b>NEXA</b>  <b>Padrão Gerencial</b>	<b>Código</b>	PG-CTI-GTI-001-PT
		<b>Revisão</b>	1.0
	<b>Título:</b>  Controle de Acesso Lógico	<b>Área</b>	TI
		<b>Páginas</b>	11 / 13

### **8.9 Tempo de Replicação do Cadastro e Remoção do Cadastro**

Uma vez que os dados foram inseridos no SAP, as informações são automaticamente replicadas para os sistemas: FIM.

Uma vez que a conta do usuário esteja disponível no AD (Active Directory), é necessário aguardar de 2 horas até no máximo 24 horas para que a conta esteja disponível no address book do Outlook.

### **8.10 Primeiro Acesso e Disponibilização das Credenciais**

Seguindo a Política da Segurança de Informação disponível na Intranet/GQI-Nexa, todas as contas de usuário devem possuir uma senha forte e secreta, conhecida apenas pelo proprietário da conta, adicionalmente os usuários devem manter seguras suas senhas e não compartilha-las ou divulga-las. O procedimento mencionado logo abaixo deve ser adotado:

- No momento da entrega do computador ao usuário, e quando é disponibilizado as credenciais da rede ao mesmo, a conta deve ser colocada para expirar para que o usuário realize a troca de senha, ou seja, o usuário não deve permanecer com a senha temporária;
- O formato da criação de senha, deve observar e seguir as diretrizes que constam na política de segurança da informação.


### **8.11 Revisão dos Direitos de Acesso**

Os Administradores dos Sistemas Legados, devem analisar os direitos de acesso e privilégios concedidos aos usuários dos sistemas, no mínimo anualmente, e validar se todos os direitos de acesso ainda são necessários e estão de acordo com as necessidades da função.

### **8.12 Gestão de Contas Privilegiadas**

- Todas as contas criadas no AD (Active Directory), exceto para terceiros, são usuários do domínio.
- As contas privilegiadas só devem ser concedidas aos usuários que necessitam desse acesso para desempenhar sua função de trabalho, com prévia autorização do Gerente Geral e Área de Segurança de TI.

<b>Elaborador:</b> Fabiano Alves	<b>Classificação:</b> Uso Interno	<b>Aprovador:</b> José Furtado
-------------------------------------	--------------------------------------	-----------------------------------

	<b>NEXA</b>  <b>Padrão Gerencial</b>	<b>Código</b>	PG-CTI-GTI-001-PT
		<b>Revisão</b>	1.0
	<b>Título:</b>  Controle de Acesso Lógico	<b>Área</b>	TI
		<b>Páginas</b>	12 / 13

- Os usuários com conta privilegiada também devem ter uma conta não privilegiada, que deve ser usada para todos os fins que não exijam acesso privilegiado.

### 8.13 Controle de Acesso ao Código-Fonte de Programas

O acesso ao código-fonte de programas deve ser controlado para prevenir a introdução de funcionalidades não autorizadas e para evitar mudanças intencionais e não intencionais. As atualizações de código-fonte devem ser registradas e efetuadas após autorização pertinente.

## 9. PROCESSO DE REVOGAÇÃO DE ACESSOS

As definições desta seção, estabelecem os controles existentes para manutenção da política de concessão e exclusão de acessos no processo de saída do empregado, a fim de garantir o alinhamento com os requisitos de negócios da companhia.

### 9.1 Desligamento (Revogação dos acessos)


O processo de desligamento de um empregado é realizado pela área do DHO, onde os mesmos são contatados pelas áreas internas da companhia. Uma vez que a ação de desligamento é formalizada, a área do DHO deve mudar o status daquele empregado no sistema SAP HR e notificar o CSC.

Uma vez efetuado esta baixa pelo CSC, o status de desligado da conta é replicado em todos os sistemas e o bloqueio será realizado automaticamente na base do AD (Active Directory) e do SAP, e também para as outras aplicações integradas com o AD.

Caso exista a necessidade de um bloqueio imediato (exceções), a área de Operação de TI (OGS) e GRC, devem ser comunicadas diretamente, então esta ação pode ser realizada diretamente no AD e no SAP.

Mensalmente é feito uma checagem (revisão) diretamente no banco do cadastro geral no SAP, cruzando assim os dados dos desligados, caso exista qualquer diferença a exclusão é realizada.

<b>Elaborador:</b> Fabiano Alves	<b>Classificação:</b> Uso Interno	<b>Aprovador:</b> José Furtado
-------------------------------------	--------------------------------------	-----------------------------------

	<b>NEXA</b>  <b>Padrão Gerencial</b>	<b>Código</b>	PG-CTI-GTI-001-PT
		<b>Revisão</b>	1.0
	<b>Título:</b>  Controle de Acesso Lógico	<b>Área</b>	TI
		<b>Páginas</b>	13 / 13

### 9.2 Exclusão Definitiva de uma Conta de Rede

Conforme rotina interna, o processo de exclusão definitiva de uma conta de rede, ocorre automaticamente após 30 dias de inatividade (Status de bloqueada) na base do AD.

### 9.3 Tempo de Retenção da Conta do Usuário após Exclusão

De acordo com a rotina existente, as contas são excluídas das bases do AD (Active Directory) após 30 dias tendo o status de bloqueada. Em caso de um novo cadastro, não será possível utilizar aquele mesmo usuário (alias) através do processo de criação automático, uma vez que aquele endereço eletrônico fica retido por 360 dias.

## 10. INFORMAÇÕES COMPLEMENTARES

Não aplicável.

## 11. ANEXOS

Não aplicável.

<b>Elaborador:</b> Fabiano Alves	<b>Classificação:</b> Uso Interno	<b>Aprovador:</b> José Furtado
-------------------------------------	--------------------------------------	-----------------------------------