POLÍTICA DE USO DE INFORMAÇÕES E RECURSOS

SUMÁRIO

1. OBJETIVO....3
2. ABRANGÊNCIA....3
3. TERMOS E DEFINIÇÕES....3
4. CLASSIFICAÇÃO E TRATAMENTO DA INFORMAÇÃO....4
5. USO ACEITÁVEL DOS ATIVOS....5
5.1 DIRETRIZES GERAIS....5
5.2 NÃO É PERMITIDO....5
5.3 USO DA INTERNET....6
5.4 ARMAZENAMENTO DE ARQUIVOS....6
5.5 USO DO CORREIO ELETRÔNICO....7
6. MESA LIMPA E TELA LIMPA....7
7. ACESSO FÍSICO....8
8. ACESSO LÓGICO....8
8.1 DIRETRIZES GERAIS....8
8.2 LOGIN E SENHA....9
8.3 CONTROLE DE ACESSO....9
8.4 ACESSO REMOTO....9
9. SEGURANÇA EM RECURSOS HUMANOS....9
10. POLÍTICA DE USO DE DISPOSITIVOS MÓVEIS....10
10.1 DIRETRIZES GERAIS....10
10.2 GERENCIAMENTO DE MÍDIAS REMOVÍVEIS....10
11. USO DE EQUIPAMENTO, SOFTWARES E TRANSFERÊNCIA DE MÍDIAS....10
11.1 DIRETRIZES GERAIS....10
11.2 USO EXTERNO DE EQUIPAMENTOS E ENVIO PARA MANUTENÇÃO....11
11.3 ENVIO, DEVOLUÇÕES, PERDAS, FURTOS, ROUBOS E DANOS AOS EQUIPAMENTOS....11
12. PROTEÇÃO CONTRA MALWARE....12
13. PAPÉIS E RESPONSABILIDADES....13
13.1 DIRETORIA....13
13.2 COMITÊ DE SEGURANÇA DA INFORMAÇÃO (CSI)....13
13.3 COLABORADORES....13
13.4 ÁREA DE SEGURANÇA DA INFORMAÇÃO....13
ANEXO I - FR-INF-007 - Registro de entrada e saída de equipamentos....15

1. OBJETIVO

1.1 Estabelecer as regras para o uso aceitável das informações, dos ativos e recursos de processamento associados às informações geradas e/ou custodiadas pela Lojacorr.

2. ABRANGÊNCIA

2.1 Esta política se aplica a todos os colaboradores que utilizam as informações, recursos e/ou demais ativos tangíveis ou intangíveis da Lojacorr.

3. TERMOS E DEFINIÇÕES

Acesso remoto - conexão à distância entre um dispositivo isolado (terminal ou micro) e uma rede.

AWS - *Amazon Web Services*

Cloud - nuvem

Colaboradores – funcionários, prestadores de serviços, estagiários e menor aprendiz.

Confidencialidade - propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados. [ISO/IEC 27000:2014]

Disponibilidade - propriedade de estar disponível e utilizável quando necessário e autorizado. [ISO/IEC 27000:2014]

Estação de trabalho - todos os microcomputadores e notebooks da empresa interligados ou não à rede corporativa da Lojacorr.

Hardware - toda a parte física de um equipamento. Exemplo: computadores, impressoras, unidades de CD, Pendrive, etc.

Incidente de segurança da informação - é indicado por um simples evento ou por uma série de eventos de segurança da informação, indesejados ou inesperados, que possam comprometer ou prejudicar as operações do negócio ou impactar negativamente os ativos da empresa. Ou qualquer ato contrário ao determinado nesse documento.

Integridade - características das informações que somente são alteradas por pessoas e da forma permitida.

Login - nome que o usuário utiliza para acessar o servidor da rede. Para entrar na rede, você precisa digitar sua identificação (login), seguido de uma senha (password).

Malwares - software Malicioso

MFA - Multi Fator de Autenticação

Mídia - meio físico utilizado para armazenar dados, tais como fitas, discos, CDs, pen drive, entre outros.

Rede corporativa - é a rede interna da Lojacorr, o notebook se conecta a ela quando ele estiver fisicamente na sede, conectado na rede ou em qualquer local externo utilizando a VPN.

Segurança da Informação - preservação da confidencialidade, da integridade e da disponibilidade das informações. (ISO/IEC 27000, 2014)

Senha - conjunto de caracteres, de conhecimento único do usuário, utilizados no processo de verificação de sua identidade na rede, assegurando que ele é realmente quem diz ser.

Servidor - computador em uma rede, responsável pelo compartilhamento de recursos com os demais computadores a ele conectados.

SGSI - Sistema de Gestão de Segurança da Informação

Software - programa de computador.

Spam - lixo eletrônico, mensagem eletrônica recebida sem a solicitação do usuário do e-mail. Geralmente enviada a um grande número de pessoas através de "correntes".

Vírus - programa desenvolvido com intenção nociva que, quando inserido em um computador, pode causar queda de desempenho, destruição de arquivos e disco rígido, ocupar espaço livre de memória, entre outros.

VPN - *Virtual Privace Network*

4. CLASSIFICAÇÃO E TRATAMENTO DA INFORMAÇÃO

4.1. A informação é um recurso que move o mundo, é um ativo crítico para a realização do negócio e a execução da missão da empresa. É um bem que tem valor para a empresa e precisa ser gerenciado e protegido. A informação é intangível, então é importante perceber que quando você se comunica, seja em uma conversa, em um e-mail, em aplicativos de mensagens ou redes sociais, você transmite informação. Essa informação pode ter valor para a empresa e deve ser considerada restrita.

4.2. A Lojacorr realiza a classificação da informação. Ou seja, aplica um rótulo à informação que circula na empresa.

4.3. Toda informação gerada ou custodiada pela Lojacorr deve ser classificada de acordo com o nível de sensibilidade que representa para o negócio.

4.4. A classificação deve considerar o valor da informação, os requisitos legais, a sensibilidade, a criticidade, a vida útil da informação, a necessidade de compartilhamento e restrição, a análise de riscos e os impactos para o negócio.

4.4.1 A classificação da informação deve ser realizada no momento em que a informação é gerada ou inserida nos processos da Lojacorr ou no momento em que é identificada que

ainda não foi classificada.

4.4.2 Os seguintes níveis devem ser considerados na classificação da informação na Lojacorr:

a) **Confidencial:** É toda informação cujo acesso não-autorizado ou uso indevido possa comprometer a operação do negócio, causar danos financeiros ou danificar a imagem da empresa. É o nível máximo de classificação da informação na organização.
b) **Secreta:** É toda informação restrita a uma área, grupo de trabalho.
c) **Restrita:** São informações restritas a todos os colaboradores da Lojacorr.
d) **Particular:** É uma informação de caráter pessoal que diz respeito a uma pessoa física ou jurídica.
e) **Pública:** É toda informação que pode ser amplamente divulgada, não apresentando potencial de risco à empresa. Não há qualquer tipo de restrição sobre essa informação.

5. USO ACEITÁVEL DOS ATIVOS

5.1 DIRETRIZES GERAIS

5.5.1 A POL-TI-002 Política Segurança da Informação contém as diretrizes gerais para o uso aceitável dos ativos.

5.2 NÃO É PERMITIDO

5.2.1 Utilizar a marca da Lojacorr sem autorização;

5.2.2 Copiar ou emprestar softwares desenvolvidos ou adquiridos pela Lojacorr sem a autorização formal da diretoria executiva;

5.2.3 Conversar sobre assuntos confidenciais, secretos ou restritos relacionados à Lojacorr em locais públicos;

5.2.4 Deixar recados com assuntos confidenciais em secretárias eletrônicas, mensagens de áudio de WhatsApp ou correio de voz;

5.2.5 Consumir comidas e bebidas próximo às estações de trabalho, evitando danos ao equipamento fornecido para trabalho diário. A Lojacorr oferece acesso à internet na sede em São José dos Pinhais - Paraná e São Paulo - SP, correio eletrônico (e-mail) e espaço para armazenamento de informações no Google Workspace a seus colaboradores, para que todos possam exercer suas atividades com eficiência. Para garantir a utilização aceitável destes recursos, a empresa se reserva o direito de utilizar ferramentas para verificar o conteúdo de mensagens eletrônicas, arquivos armazenados

nos servidores e para monitorar o uso da internet.

5.3 USO DA INTERNET

5.3.1 Visando garantir a segurança das informações geradas e/ou custodiadas pela Lojacorr, não é permitido acessar sites que comprometam a integridade da rede e ou equipamentos, abrir ou armazenar arquivos, enviar ou responder mensagens eletrônicas de conteúdo desconhecido que infrinjam direitos autorais ou proibidos por lei, tais como:

a) Racista ou discriminatório de qualquer natureza;
b) Pedófilo, pornográficos ou que possam caracterizar assédio sexual;
c) Ameaçadores, ofensivos, agressivos ou que induzam à criminalidade.
d) Filmes, músicas, livros e outras obras de direitos autorais reservados.
e) Acessar seu e-mail particular (Gmail, Hotmail, Yahoo) através da rede corporativa da empresa.
f) Participar de qualquer discussão pública sobre os negócios da Lojacorr por meio de salas de chat, grupos de discussão, redes sociais ou qualquer outro tipo de fórum público sem autorização prévia;
g) Utilizar redes sociais, ferramentas e/ou serviços de troca de mensagens instantâneas, tais como: Skype, Facebook, Instagram, WhatsApp, Telegram através da rede corporativa da empresa.
h) Utilizar serviços de armazenamento na nuvem diferentes dos fornecidos pela Lojacorr, tais como: OneDrive, Dropbox, Mega e etc.

5.3.2 Caso ocorra alguma necessidade de liberação dos acessos aos e-mails, redes sociais, fóruns e serviços de armazenamento em nuvem deve ser aberto um chamado para área de infraestrutura ou solicitado pelo Gestor direto para documentação via central de chamados.

5.4 ARMAZENAMENTO DE ARQUIVOS

5.4.1 O espaço para armazenamento e compartilhamento de informações fornecido pela organização são destinados exclusivamente às atividades profissionais relacionados a Lojacorr, por isso não é permitido armazenar arquivos pessoais, tais como: fotos, vídeos, músicas e etc.

5.5 USO DO CORREIO ELETRÔNICO

5.5.1 O correio eletrônico (e-mail corporativo) fornecido pela empresa deve ser utilizado somente para troca de informações relacionadas às atividades profissionais relacionados a Lojacorr e não deve ser utilizado para recebimento de mensagens particulares.

5.5.2 Não é permitido enviar ou receber informações relacionadas ao negócio da Lojacorr por meio de correio particular.

5.5.3 O uso do correio corporativo é pessoal e o colaborador é o responsável por toda mensagem enviada pelo seu endereço.

5.5.4 O colaborador deve:

a) Conferir os destinatários antes de enviar uma mensagem, pois nos contatos pode haver homônimos.
b) Utilizar a assinatura de e-mail padrão da Lojacorr ao enviar ou responder mensagens.
c) Armazenar mensagens eletrônicas somente nos equipamentos disponibilizados pela empresa.

5.5.5 O colaborador não deve abrir mensagens de origem desconhecida, com nome de remetentes ou títulos estranhos ou clicar em links, executar ou abrir arquivos não solicitados ou que não sejam esperados, mesmo que de origem conhecida ou aparentemente inofensiva.

6. MESA LIMPA E TELA LIMPA

6.1 Todo colaborador não deve deixar documentos em papel ou mídia (HDs, pendrives, CDs, etc.) expostos.

6.2 Documentos impressos com informações confidenciais ou secretas devem ser guardados em armários ou gavetas com chaves.

6.3 Após as reuniões, nenhum tipo de informação deve ser deixada no ambiente utilizado.

6.4 Os documentos da empresa em meio digital devem ser armazenados nos servidores corporativos e nas áreas com acesso restrito aos colaboradores autorizados.

6.5 Ao imprimir documentos contendo informações confidenciais ou secretos o colaborador deve permanecer próximo à impressora.

6.6 Documentos impressos e mídias não utilizadas devem ser descartados de forma adequada. Não é permitida a reutilização como lembretes ou rascunhos de documentos impressos classificados como confidenciais, secretos ou restritos.

6.7 Todo colaborador deve bloquear sua estação de trabalho sempre que se ausentar do seu local de trabalho.

6.8 Todas as estações de trabalho e servidores sem monitoramento devem ativar o bloqueio da tela.

7. ACESSO FÍSICO

7.1 Todos os colaboradores que necessitem acessar as dependências da Lojacorr, devem solicitar o cadastro da biometria via central de chamados para liberação das dependências da empresa via autorização do gestor direto.

7.2 Todos os visitantes devem ser devidamente registrados, identificados e acompanhados durante a permanência nas dependências da empresa.

7.3 PERÍMETRO DE SEGURANÇA FÍSICA: Os locais de processamento e armazenamento de informações sensíveis são de acesso restrito; o acesso é permitido apenas aos colaboradores autorizados e com biometria cadastrada.

7.4 DESCARTE E REUTILIZAÇÃO DE MÍDIAS E DOCUMENTOS FÍSICOS: Mídias, equipamentos e papéis com informações sensíveis devem ser descartadas ou reutilizadas de acordo com o procedimento de classificação e tratamento da informação.

8. ACESSO LÓGICO

8.1 DIRETRIZES GERAIS

8.1.2 Os colaboradores devem ter acesso somente às informações que sejam necessárias ao desenvolvimento de suas atividades profissionais.

8.1.3 O acesso à rede, sistemas e serviços disponibilizados pela Lojacorr, deve ser realizado apenas por meio de login e senha.

8.1.4 Acesso às plataformas em *Cloud*, deve obrigatoriamente ser realizadas através de VPN, com MFA para autenticação e acesso.

8.1.5 É proibido a utilização dos equipamentos da Lojacorr para fins particulares durante o horário de expediente.

8.1.6 É proibido o envio de dados do ambiente corporativo para ambiente particular sem uma justificativa e aprovação da gestão imediata.

8.2 LOGIN E SENHA

8.2.1 Não é permitido compartilhar senhas pessoais.

8.2.2 Criar senhas complexas, com o mínimo de 8 caracteres, contendo letras, números e caracteres especiais.

8.2.3 Todo colaborador deve alterar senha temporária no primeiro acesso.

8.2.4 Não anotar senhas em qualquer meio que coloque em risco a sua descoberta.

8.2.5 Será solicitado a cada 2 (dois) meses a alteração da senha para garantir a segurança no processo de autenticação em todos os sistemas e ferramentas fornecidos pela Lojacorr.

8.3 CONTROLE DE ACESSO

8.3.1 A liberação do acesso a solicitação, aprovação e liberação do acesso lógico à rede e aos sistemas deve ser registrada na ferramenta de chamados à área de infraestrutura.

8.3.2 Bloqueio e cancelamento do acesso e autorizações.

8.3.3 O acesso será cancelado ou bloqueado nas seguintes situações:

a) Quando ocorre o desligamento do usuário.
b) Quando houver indício de uso inadequado dos sistemas e serviços.
c) Quando solicitado pelo gestor.
d) Quando o mesmo estiver de férias ou afastado por motivo de saúde ou de âmbito particular (Falecimentos etc.)

8.4 ACESSO REMOTO

8.4.1 O acesso remoto à rede corporativa da Lojacorr é restrito aos colaboradores autorizados formalmente pelo diretor ou gestor.

8.4.2 As ferramentas utilizadas para acesso remoto são aprovadas pela infraestrutura, e é extremamente proibido a utilização de ferramentas sem a homologação do setor.

8.4.3 As solicitações de acessos, fora do território nacional, devem ser previamente acertadas com o setor de G & G e o gestor direto.

9. SEGURANÇA EM RECURSOS HUMANOS

9.1 Todos os colaboradores e prestadores de serviço devem assinar um Termo de Sigilo e Confidencialidade no momento da contratação.

9.2 O Termo de Sigilo e Confidencialidade deve conter cláusulas sobre não utilização/divulgação das informações da empresa, continuando válido mesmo após a extinção do contrato de prestação de serviços.

9.3 O formulário de contratação e desligamento de pessoal deve ser preenchido e encaminhado para as áreas providenciar a liberação dos acessos e disponibilização dos recursos necessários às atividades do colaborador/prestador de serviços no momento da contratação.

9.4 Todo colaborador deverá receber um treinamento inicial de apresentação da política de segurança da informação, na data em que iniciar suas atividades na empresa.

10. POLÍTICA DE USO DE DISPOSITIVOS MÓVEIS

10.1 DIRETRIZES GERAIS

10.1.1 Todo dispositivo móvel de propriedade da Lojacorr fornecido aos colaboradores deve ser registrado e controlado pela área de infraestrutura.

10.1.2 Os colaboradores que receberam o dispositivo devem assinar um termo de responsabilidade se comprometendo a zelar pelo dispositivo tendo o devido cuidado principalmente estando fora das dependências da empresa.

10.1.3 Ao utilizar o dispositivo fora das dependências da empresa, não conecte em redes *wifi* públicas, em locais como aeroportos, hotéis, cafés, lanchonete, utilize apenas o serviço de dados.

10.1.4 Em caso de perda/roubo deve informar imediatamente à empresa para que sejam tomadas as providências cabíveis.

10.1.5 Caso o colaborador seja desligado da empresa deve devolver imediatamente os dispositivos.

10.2 GERENCIAMENTO DE MÍDIAS REMOVÍVEIS

10.2.1 Não é permitido a utilização de mídias removíveis para armazenar informações da Lojacorr, exceto mediante autorização formal do gestor.

10.2.2 As portas USBs e unidades de DVD-ROM das estações de trabalho devem ser bloqueadas, de maneira que não permita a transferência de dados. Exceto quando formalmente autorizado pelo gestor.

11. USO DE EQUIPAMENTO, SOFTWARES E TRANSFERÊNCIA DE MÍDIAS

11.1 DIRETRIZES GERAIS

11.1.1 Apenas os colaboradores da área de infraestrutura podem realizar a instalação de equipamentos e softwares.

11.1.2 Todos os colaboradores NÃO devem:

a) Instalar hardwares ou softwares nas estações de trabalho, que não estejam homologados e autorizados.
b) Utilizar os recursos da rede corporativa para desenvolver negócios pessoais.
c) Utilizar equipamentos não autorizados pela área de infraestrutura na rede corporativa da empresa, especialmente roteadores, hubs, pontos de acesso e extensores de rede ou recursos computacionais.
d) Colocar seu computador em modo Ponto de Acesso.
e) Trocar de lugar ou substituir os equipamentos da sede (equipamentos que possuem placa de patrimônio) sem autorização da área de infraestrutura, como por exemplo, desktops, monitores, notebooks, aparelhos de telefone e etc.
f) Emprestar os equipamentos fornecidos para pessoas não autorizadas a utilizar os equipamentos da Lojacorr.

11.2 USO EXTERNO DE EQUIPAMENTOS E ENVIO PARA MANUTENÇÃO

11.2.1 Todos os equipamentos devem ser registrados no formulário ANEXO I - FR-INF-007 - Registro de entrada e saída de equipamentos. Link:
FR-INF-007 - Registro de entrada e saida de equipamento.docx

11.3 ENVIO, DEVOLUÇÕES, PERDAS, FURTOS, ROUBOS E DANOS AOS EQUIPAMENTOS

11.3.1 Em caso de furto e ou roubo o Colaborador, deverá comunicar imediatamente seu gestor e a área de infraestrutura para bloqueio do usuário do colaborador. Após, deverá fazer o Boletim de Ocorrência e enviá-lo à área de G&G (Gente & Gestão) e (por chamado na Central de Chamados).

11.3.2 O usuário deve manter o equipamento em perfeitas condições de uso e zelar pelo mesmo.

11.3.3 É proibido colar adesivos nos equipamentos fornecidos pela Lojacorr.

11.3.4 A Lojacorr disponibiliza para todo colaborador um equipamento novo, sendo de responsabilidade do colaborador sua utilização dentro dos padrões seguros definidos pela Lojacorr.

11.3.5 É responsabilidade do colaborador residente em municípios localizados a até 30km de São José dos Pinhais, o recebimento do equipamento na Sede, no dia e horário que for previamente agendado com a infraestrutura.

11.3.6 O envio para colaboradores residentes em cidades diversas do item 11.3.5, é realizado através dos Correios ou transportadora, sendo de responsabilidade do colaborador acompanhar a entrega pelo código de rastreamento que lhe será enviado e receber os

equipamentos na ocasião da entrega.

11.3.7 É responsabilidade do colaborador informar à área de infraestrutura, por chamado, qualquer defeito que identificar no equipamento, seja após o recebimento dele, seja durante o período em que o equipamento estiver em sua posse.

11.3.8 A área de infraestrutura irá analisar o defeito apontado, elaborar um laudo técnico descrevendo o que foi constatado e se o dano ao equipamento decorrer de mau uso, fará o conserto. Após, enviará à área de Gente & Gestão o laudo e o valor gasto para o conserto, para que seja descontado da remuneração do colaborador e pessoa jurídica, em folha de pagamento ou em distrato contratual.

11.3.9 Em caso de desligamento é responsabilidade do colaborador a devolução do equipamento no mesmo estado em que o recebeu. Qualquer defeito que a área de Infraestrutura identificar no equipamento, que não tenha sido informado previamente pelo Colaborador (por chamado conforme item 11.3.7), que for decorrente de mau uso, que será descrita no laudo técnico, enviado à área de G&G, juntamente com o orçamento para o conserto para que seja descontado da rescisão ou em folha de pagamento

11.3.10 O colaborador desligado, possui um prazo de dois dias úteis a partir da data do comunicado de rescisão, para o envio dos equipamentos, sob pena de ter o desconto em sua rescisão.

12. PROTEÇÃO CONTRA MALWARE

12.1 DIRETRIZES

12.1.1 Os equipamentos, servidores e os computadores para uso individual ou coletivo, de qualquer porte, serão dotados de mecanismos de proteção contra malwares.

12.2 CUIDADOS COM SPAM

12.2.1 Nunca cadastre o e-mail corporativo em sites ou serviços para recebimento de propagandas, ou qualquer assunto que não esteja relacionado com as atividades profissionais. A maioria destes serviços são propagadores de Spam. O spam pode trazer conteúdo impróprio ou mesmo ilegal, além de ser uma fonte de propagação de vírus e de programas maliciosos e perigosos.

13. PAPÉIS E RESPONSABILIDADES

13.1 DIRETORIA

13.1.1 Direcionar as ações de segurança da informação alinhadas com o negócio;

13.1.2 Aprovar procedimentos operacionais padrão relacionados a governança e segurança da informação;

13.1.3 Viabilizar recursos para implementação dos mecanismos de proteção acordados.

13.2 COMITÊ DE SEGURANÇA DA INFORMAÇÃO (CSI)

13.2.1 Dirigir, monitorar e avaliar a segurança da informação por meio de indicadores;

13.2.2 Recomendar mecanismos de proteção da informação com base nos requisitos de segurança da informação do negócio e riscos identificados;

13.2.3 Zelar que os mecanismos de proteção acordados sejam implementados na organização;

13.2.3 Garantir que seja realizada análise crítica de todos os documentos que compõem a política de segurança da informação no mínimo uma vez ao ano ou sempre que ocorrerem mudanças significativas.

13.3 COLABORADORES

13.3.1 Cada colaborador é corresponsável pela Gestão da Segurança da Informação da Lojacorr. Para isso, é fundamental conhecer, cumprir e disseminar as diretrizes da empresa.

13.3.2 Todo colaborador deve:

a) Conhecer e cumprir as orientações definidas na Política de Segurança da Informação e procedimentos de segurança aplicáveis a suas atividades;

b) Zelar pela segurança das informações que acessam, independente do meio em que estejam armazenados;

c) Utilizar as informações e recursos disponibilizados pela Lojacorr respeitando a legislação vigente, direitos autorais, regras de licenciamento de softwares, direitos de propriedade, privacidade, proteção de propriedade intelectual e procedimentos internos.

13.4 ÁREA DE SEGURANÇA DA INFORMAÇÃO

13.4.1 Gerenciar as atividades de gestão de segurança da informação;

13.4.2 Garantir que a informação documentada do SGI esteja pertinente, atualizada e

divulgada conforme apropriado;

13.4.3 Recomendar ações de segurança da informação e apoiar o comitê gestor de segurança da informação em assuntos relacionados à segurança da informação na organização;

13.4.4 Discutir as boas práticas de segurança e monitorar sua implementação na Lojacorr;

13.4.5 Acionar o plano de resposta a incidentes em caso de identificação.

ANEXO I - FR-INF-007 - Registro de entrada e saída de equipamentos

	REGISTRO DE ENTRADA E SAÍDA DE EQUIPAMENTOS			PAGINA *1/1*
	CÓDIGO: **FR-INF-007**	REVISÃO: 01	Data da versão 20/05/2024	Classificação: RESTRITA
	Elaborado por: Anderson Souza	Aprovado por: Alex Martins		

Data/Hora	Descrição do equipamento (tipo, fabricante, modelo)	Patrimônio/ Série	Objetivo da Saída do Equipamento	Nome do Responsável pela Saída	Visto do Responsável
Saída __/__/____ __:__					
			Situação de Recebido do Equipamento	Nome do Responsável pelo Recebimento	Visto do Responsável
Entrada __/__/____ __:__					
Data/Hora	**Descrição do equipamento (tipo, fabricante, modelo)**	**Patrimônio/ Série**	**Objetivo da Saída do Equipamento**	**Nome do Responsável pela Saída**	**Visto do Responsável**
Saída __/__/____ __:__					
			Situação de Recebido do Equipamento	Nome do Responsável pelo Recebimento	Visto do Responsável
Entrada __/__/____ __:__					

FR-INF-007 - Registro de entrada e saida de equipamento.docx