POLÍTICA DE

SEGURANÇA DA INFORMAÇÃO

JUNHO DE 2023

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

ÍNDICE

1.CONTEXTUALIZAÇÃO

A Reinaldo Teles - Hair Tools possui o compromisso de resguardar e proteger os dados sejam eles pessoais ou não, que estão sob sua guarda.

Nesse sentido, a presente Política de Segurança da Informação RT, apresenta diretrizes gerais de conduta, bem como obrigações a serem seguidas na RT (PSI RT) a fim de mitigar eventuais riscos e danos relacionados a ameaças externas ou internas, deliberadas ou acidentais, que possam impactar na confidencialidade, integridade e disponibilidade das informações de qualquer natureza, objetivando garantir sua preservação.

Amparada nos preceitos da Norma ISO 27001, padrão internacional para processos de gestão da segurança da informação, a PSI RT define também papéis e responsabilidades para a implantação dos seguintes controles de segurança da informação:

1. Conformidade;
2. Políticas de S.I;
3. Segurança de Recursos Humanos;
4. Gestão de Ativos;
5. Controle de Acessos;
6. Criptograficas;
7. Segurança de Operações;
8. Segurança Física e Ambiental;
9. Segurança de Comunicações;
10. Aquisição, Desenvolvimento e Manutenção de Sistemas;
11. Relações com Fornecedores;
12. Gestão de Incidentes de S.I;
13. Aspetos de S.I na Continuidade do Negócio.

2.DEFINIÇÕES

AMEAÇA: evento que tem potencial em si próprio para comprometer os objetivos da fundação, seja trazendo danos diretos aos ativos ou prejuízos indiretos decorrentes de situações inesperadas.

ATIVOS DE INFORMAÇÃO: são os meios de produção, armazenamento, transmissão e processamento de informações, os sistemas de informação, os locais onde se encontram esses meios, as pessoas que têm acesso a informações, assim como as próprias informações coletadas, produzidas, processadas, armazenadas, custodiadas, descartadas e transmitidas pela RT.

AUTENTICIDADE: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.

CLASSIFICAÇÃO DA INFORMAÇÃO: identificação de quais são os níveis de proteção que as informações demandam e estabelecimento de classes e formas de identificá-las, além de determinar os controles de proteção necessários a cada uma delas.

CONFIDENCIALIDADE: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizados e credenciados.

CONFORMIDADE: processo que visa verificar o cumprimento das normas estabelecidas.

CONTROLE DE ACESSO: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso.

CRIPTOGRAFIA: método de codificação da informação que visa evitar que ela seja compreendida ou alterada por pessoas não autorizadas.

CUSTODIANTE DO ATIVO DE INFORMAÇÃO: é aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia.

DADOS PESSOAIS: todo e qualquer dado relacionado a pessoa natural identificada ou identificável (conforme definição trazida no art. 5o, I, da Lei no 13.709/2018 - Lei Geral de Proteção de Dados Pessoais), inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa. Também são considerados dados pessoais para os fins da lei aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada (art. 12, §2o, LGPD).

DISPONIBILIDADE: propriedade de que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade no momento requerido.

EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES EM SEGURANÇA DA INFORMAÇÃO: grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações relacionadas a incidentes com ativos de informação da RT.

FORNECEDORES: no contexto da RT são considerados fornecedores os outros terceiros contratados e subcontratados, pessoa física ou jurídica, não enquadrados como parceiros comerciais.

GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação.

GESTOR DOS ATIVOS DE INFORMAÇÃO: unidade administrativa responsável por gerenciar determinado segmento de informação e todos os ativos relacionados.

GESTOR DE SEGURANÇA DA INFORMAÇÃO: funcionário responsável pela operação do ESI.

GDPR: *General Data Protection Regulation*: conjunto de regras sobre tratamento de dados aprovado em 2016 válido para a União Europeia (EU). Regulamenta também a exportação de dados pessoais para fora da UE.

INFORMAÇÃO: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado.

INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO: instalações prediais (energia, água, climatização, acesso físico), computadores e equipamentos, software, redes e telecomunicações, sistemas de armazenamento e recuperação de dados (arquivos e armazenamento), aplicações computacionais, cabeamento e rede telefônica.

INTEGRIDADE: propriedade de que a informação não foi modificada, suprimida ou destruída de maneira não autorizada ou acidental.

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD): Lei no 13.709/2018, que dispõe sobre o tratamento de **dados pessoais**, em meios físicos ou digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado. Toda pessoa natural tem assegurada a titularidade de seus **dados pessoais** e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos da Lei (arts. 1° e 17, LGPD).

PARCEIROS COMERCIAIS: no contexto da RT são considerados parceiros comerciais os **terceiros** contratados, pessoa física ou jurídica, que atuam em seu nome: Consultores, Conveniados e Agentes Comerciais (aqueles que indicam atividades onde a RT pode atuar como contratada).

QUEBRA DE SEGURANÇA: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações.

SEGURANÇA DE COMUNICAÇÕES: processo de proteção de dados digitais em trânsito.

SISTEMA ESTRUTURANTE: conjunto de sistemas de informática fundamentais e imprescindíveis para a consecução das atividades administrativas, de forma eficaz e eficiente.

TERCEIROS: São os parceiros comerciais e os fornecedores da RT.

TRATAMENTO DA INFORMAÇÃO: conjunto de ações referentes à recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação.

VULNERABILIDADE: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

3.POLÍTICA DE SEGURANÇA DA INFORMAÇÃO RT

Estabelece o compromisso da Reinaldo Teles - Hair Tools em resguardar e proteger as informações - sejam elas pessoais ou não - que estão sob sua guarda além de definir a governança de segurança da informação na RT.

Esta Política de Segurança da Informação exige o cumprimento do Código de Conduta RT e de todas as leis e regulamentações aplicáveis e em vigor relacionadas a proteção de dados incluindo, sem limitação, a Lei Geral de Proteção de Dados Pessoais (LGPD) e a General Data Protection Regulation (GDPR).

Esta Política se insere no Sistema de Controles Internos e de Conformidade RT como sendo o documento que estabelece as diretrizes do Programa de Conformidade para com a Lei Geral de Proteção de Dados Pessoais.

4.DESTINATÁRIOS

A presente Política se aplica a todos os membros do Conselho Diretor, Conselho Curador, Presidente, Vice-Presidentes, empregados, estagiários, parceiros comerciais (consultores, agentes comerciais e conveniados) que atuam em nome da RT e fornecedores (outros contratados e subcontratados pela RT) e que, no âmbito dessa relação, possam acessar as áreas, equipamentos, informações, arquivos, redes e dados de titularidade ou propriedade da RT. Desta forma:

Todos os destinatários deverão observar as presentes regras e recomendações em quaisquer operações que possam impactar na segurança das informações na RT. O não cumprimento das disposições ora previstas sujeitará o infrator às sanções previstas fixadas pelo Comitê de Segurança de Informação (CSI) previsto nesta Política, sem prejuízo das medidas previstas em lei, caso se aplique.

5.APLICABILIDADE

Esta Política estabelece as diretrizes para garantir que seus destinatários entendam e cumpram as leis de proteção de dados pessoais, bem como os padrões e medidas técnicas visando a segurança da informação na RT.

6.OBJETIVOS

Esta Política de Segurança da Informação (PSI RT) tem como objetivos:

- Estabelecer as diretrizes que assegurem e reforcem o compromisso da Instituição com as práticas e medidas preventivas garantidoras de segurança da informação;
- Definir o referencial para a normatização das questões de segurança da informação na RT;
- Criar condições para que a RT eleva continuamente a sua maturidade em segurança da informação por meio da adoção de diretrizes, normas e procedimentos destinados a proteger os ativos de informação da RT visando a promoção da Integridade, Confidencialidade, Autenticidade e Disponibilidade dos ativos de informação da RT;
- Prover a RT de mecanismos de atendimento e conformidade às leis de segurança da informação, nacionais e internacionais;
- Descrever as regras comportamentais e diretrizes a serem seguidas na condução das atividades desenvolvidas pela RT que garantam a prevenção de incidentes de segurança da informação e a proteção de dados pessoais.

Os demais documentos da RT que se relacionam com esta Política são:

- Código de Ética e Conduta;
- Política de Controles Internos e de Conformidade;
- Política geral de uso de dispositivos móveis;
- Política geral de uso e responsabilidade da "Cloud Acadêmica";
- Modelo de Segurança para ambientes computacionais na RT;
- Normas para uso da rede RT, da Internet e do Correio Eletrônico da RT.

Cada um desses documentos tem objetivos específicos, mas em todos está reforçado o compromisso da RT com a segurança da informação.

7.PRINCÍPIOS

O compromisso da RT com o tratamento adequado das informações se baseia nos seguintes princípios:

- **Autenticidade** - todos os esforços serão feitos para que as informações sejam confiáveis, e corretas, ou seja, as informações não serão alteradas de forma não autorizada ou indevida;
- **Confidencialidade** - o acesso à informação é permitido somente para pessoas autorizadas e quando ele for de fato necessário;
- **Disponibilidade** - somente as pessoas autorizadas têm acesso à informação sempre que necessário;
- **Integridade** - todos os esforços serão feitos para que as informações sejam exatas e completas bem como seu processamento.

8.DIRETRIZES

8.1. DIRETRIZES GERAIS

- A gestão da segurança da informação na RT é de responsabilidade do Comitê de Segurança da Informação (CSI) cujos membros são indicados pelo Presidente da RT;
- O cumprimento desta Política e de suas normas de procedimentos complementares deve ser avaliado periodicamente por meio de verificações de conformidade, realizadas por um grupo de trabalho designado pelo Comitê de Segurança da Informação (CSI).
- A RT, além das diretrizes estabelecidas nesta PSI, deve também se orientar pelas melhores práticas e procedimentos de segurança da informação

recomendados por órgãos e entidades públicas e privadas responsáveis pelo estabelecimento de padrões relacionados à segurança da informação.

8.2. DIRETRIZES E NORMAS COMPLEMENTARES ESPECÍFICAS

Para cada um dos controles complementares propostos pela ISO 27001 o Comitê de Segurança da Informação deve elaborar estratégias, diretrizes e normas de procedimentos complementares (Políticas de SI - controle ISO 27001 #2), assim como manuais, procedimentos de conduta e avaliações periódicas de conformidade.

A PSI RT preconiza a implantação priorizada das seguintes normas de procedimentos com as seguintes diretrizes:

8.2.1 GESTÃO DE ATIVOS DE INFORMAÇÃO (CONTROLE ISO 27001 #4):

Os ativos de informação devem:

A. Ser inventariados e protegidos;
B. Ter identificados os seus proprietários e custodiantes;
C. Ter mapeadas as suas ameaças, vulnerabilidades e interdependências;
D. Ter a sua a entrada e saída nas dependências da RT autorizadas e registradas por autoridade competente;
E. Ser passíveis de monitoramento e ter seu uso investigado quando houver indícios de quebra de segurança, por meio de mecanismos que permitam a rastreabilidade do uso desses ativos;
F. Ser regulamentados por norma de procedimentos específica quanto a sua utilização; g) Ser utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins.

E, além disso:

I. A RT deve criar, gerir e avaliar critérios de tratamento e classificação da informação de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor.

II. Os recursos tecnológicos e as instalações de infraestrutura devem ser protegidos contra indisponibilidade, acessos indevidos, falhas, bem como perdas, danos, furtos, roubos e interrupções não programadas.
III. Os sistemas de informação e as aplicações da RT devem ser protegidos contra indisponibilidade, alterações ou acessos indevidos, falhas e interrupções não programadas.
IV. O acesso dos usuários aos ativos de informação e sua utilização, quando autorizados, deve ser condicionado ao aceite do termo de sigilo e responsabilidade.
V. Os ativos de informação devem possuir mecanismos que permitam a auditoria dos eventos de acesso e alteração dos registros. Esta auditoria deve estar sempre ativa (salvo quando explicitamente dispensado este requisito) e os registros devem ser armazenados pelo período mínimo de um ano.

8.2.2 GESTÃO DE RISCOS E INCIDENTES (CONTROLE ISO 27001 #12):

I. O gestor dos ativos de informação deve estabelecer processos de Gestão de Riscos de Segurança da Informação - GRSI que possibilitem identificar ameaças e reduzir vulnerabilidades dos ativos de informação, assim como reduzir os impactos de eventuais incidentes com os mesmos.
II. A GRSI é um processo contínuo e deve ser aplicado na implementação e operação da Gestão de Segurança da Informação, levando em consideração o planejamento, execução, análise crítica e melhoria da SI na RT.

8.2.3 SEGURANÇA EM RECURSOS HUMANOS (CONTROLE ISO 27001 #3):

I. Os destinatários devem ter ciência:
    A. Das ameaças e preocupações relativas à segurança da informação e;
    B. De suas responsabilidades e obrigações no âmbito desta PSI.
II. Todos os destinatários devem difundir e exigir o cumprimento da PSI, das normas de segurança e da legislação vigente acerca do tema;
III. Devem ser estabelecidos processos permanentes de conscientização, capacitação e sensibilização em segurança da informação, que alcancem todos os destinatários, de acordo com seu relacionamento e atribuições na RT.

8.2.4 OS USUÁRIOS DEVEM SER SENSIBILIZADOS E CONSCIENTIZADOS:

I. O controle de usuários de sistemas:

a) É de responsabilidade do titular da unidade da RT juntamente com o DRH; e
b) Deve ser implementado controles de perfis, permissões e procedimentos necessários para a salvaguarda dos ativos de informação da RT.

8.2.5 SEGURANÇA DAS OPERAÇÕES DE TI DA RT (CONTROLE ISO 27001 #7):

O Comitê de Segurança da Informação deve estabelecer normas de procedimentos específicos contendo diretrizes de segurança da informação para a disponibilização e execução dos serviços, sistemas e infraestruturas de TIC da RT.

8.2.6 SEGURANÇA DAS COMUNICAÇÕES DA RT (CONTROLE ISO 27001 #9):

O Comitê de Segurança da Informação deve estabelecer normas de procedimentos específicos contendo diretrizes de segurança da informação para a disponibilização e utilização de serviços de comunicação relacionados aos ativos de informação da RT.

8.2.7 ASSINATURA DIGITAL E CRIPTOGRAFIA (CONTROLE ISO 27001 #6):

O Comitê de Segurança da Informação deve estabelecer norma de procedimentos específica contendo parâmetros para o uso de assinaturas digitais que reflitam as necessidades específicas de garantia de autenticidade dos dados RT.

Também deve ser estabelecida norma específica ditando quando e onde recursos criptográficos devem ser utilizados dentro da RT para proteger suas informações, além de estabelecer quais padrões de criptografia são aceitáveis.

8.2.8 CONTROLES DE ACESSOS (CONTROLE ISO 27001 #5):

O Comitê de Segurança da Informação deve estabelecer norma de procedimentos específica contendo parâmetros para a gestão de acesso aos dados RT, atendendo os requisitos abaixo:

1. Devem ser registrados eventos relevantes, previamente definidos, para a segurança e o rastreamento de acesso às informações.
2. Devem ser criados mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação.
3. Os usuários da RT são responsáveis por todos os atos praticados com suas identificações, tais como: nome de usuário/senha, crachá, carimbo, correio eletrônico e certificado digital.
4. A identificação do usuário, qualquer que seja o meio e a forma, deve ser pessoal e intransferível, permitindo de maneira clara e inequívoca o seu reconhecimento.
5. A autorização, o acesso e o uso das informações e dos recursos computacionais devem ser controlados e limitados ao necessário, considerando as atribuições de cada usuário, e qualquer outra forma de uso ou acesso além do necessário depende de prévia autorização do gestor da área responsável pela informação.
6. Todos os sistemas de informação da RT, automatizados ou não, devem ter um gestor, formalmente designado pela autoridade competente, que deve definir os privilégios de acesso às informações.
7. Sempre que houver mudança nas atribuições de determinado usuário, os seus privilégios de acesso às informações e aos recursos computacionais devem ser adequados imediatamente, devendo ser cancelados em caso de desligamento da RT ou bloqueados em caso de afastamento.
8. Os sistemas estruturantes devem possuir normas específicas, no âmbito de sua atuação, que regrem o controle de acesso quanto:
    a. Ao acesso às suas bases de dados;
    b. À extração, carga e transformação de dados e;
    c. Aos serviços acessíveis via linguagem de programação.
9. Os sistemas estruturantes devem possuir mecanismos automáticos para:
    a) Revogar as concessões e desativar as contas de acesso do servidor nos casos de exoneração, demissão, aposentadoria e falecimento do servidor;

b) Bloquear as contas de acesso do servidor nos casos de licença, afastamento, cessão e disponibilidade do servidor e;
c) Tratar os casos de remoção e redistribuição do servidor, segundo as definições constantes na norma de controle de acesso ao sistema.

8.2.9 AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS (CONTROLE ISO 27001 #10):

O Comitê de Segurança da Informação deve editar norma de procedimentos específica estabelecendo critérios e metodologia de segurança para desenvolvimento de sistemas de informação, de forma a abranger todas as fases do ciclo de desenvolvimento e sustentação de sistemas.

8.2.10 RELAÇÃO COM FORNECEDORES (CONTROLE ISO 27001 #11):

O Comitê de Segurança da Informação deve estabelecer norma de procedimentos específica que vise o atendimento de demandas em segurança da informação para contratos, convênios, acordos e afins, conforme os requisitos abaixo:

1. Os acordos com terceiros que possuam algum relacionamento com ativos de informação da RT devem observar as disposições e normas da PSI RT.
2. Os contratos, convênios, acordos e instrumentos congêneres devem conter cláusulas que estabeleçam a obrigatoriedade de observância desta PSI e de suas normas complementares.
3. O contrato, convênio, acordo ou instrumento congênere devem prever a obrigação da outra parte de divulgar esta PSI e suas normas complementares aos seus empregados e prepostos envolvidos em atividades na RT.
4. Um plano de contingência deve ser elaborado no caso de uma das partes desejar encerrar a relação antes do final do acordo.

8.2.11 GESTÃO DE INCIDENTES (CONTROLE ISO 27001 #12):

O Comitê de Segurança da Informação deve instituir uma Equipe de Tratamento e Resposta a Incidentes de Segurança.

8.2.12 ASPECTOS DE SEGURANÇA DA INFORMAÇÃO EM CONTINUIDADE DAS ATIVIDADES (CONTROLE ISO 27001 #13):

O Comitê de Segurança da Informação deve instituir metodologias e normas de procedimentos que endurecem as tratativas de segurança da informação relacionadas à disponibilidade dos ativos de informação da RT.

8.2.13 GESTÃO DE CONFORMIDADE (CONTROLE ISO 27001 #1):

I. Deve ser realizada, com periodicidade mínima anual, verificação de conformidade das práticas de segurança da informação da RT e de suas unidades administrativas com esta PSI e suas normas de procedimentos complementares, bem como com a legislação específica de segurança da informação.
II. A verificação de conformidade deve também ser realizada nos contratos, convênios, acordos de cooperação e outros instrumentos do mesmo gênero celebrados com a RT.
III. O calendário de ações de verificação de conformidade é elaborado com base na priorização dos riscos identificados ou percebidos.
IV. Nenhuma unidade da RT pode permanecer sem verificação de conformidade de suas práticas de segurança da informação por período superior a 2 (dois) anos.
V. É vedado a prestadores de serviços executar a verificação da conformidade de segurança da informação dos próprios serviços prestados.
VI. A verificação de conformidade pode combinar ampla variedade de técnicas, tais como análise de documentos, análise de registros (logs), análise de código-fonte, entrevistas e testes de invasão.
VII. Os resultados de cada ação de verificação de conformidade são documentados em relatório de avaliação de conformidade, o qual será encaminhado pelo Gestor de segurança da informação ao Gestor da unidade verificada, para ciência e tomada das ações cabíveis.
VIII. Para que seja possível efetuar as verificações de conformidade, a equipe delegada pelo CSI deve possuir acesso aos ambientes computacionais da RT.

8.2.14 PLANO DE INVESTIMENTOS EM SEGURANÇA DA INFORMAÇÃO DA RT:

I. Os investimentos em segurança da informação serão realizados de forma planejada e consolidados em um plano de investimentos plurianual.
II. O plano de investimentos será elaborado com base na priorização dos riscos a serem tratados e será obtido a partir da aplicação de método que considere, no mínimo, o produtor entre a probabilidade de ocorrência e o impacto do risco no negócio ou na imagem da RT.
III. Os planos de investimento e seus orçamentos são produzidos, apresentados e geridos pelo Comitê de Segurança da Informação.

9.PAPÉIS E RESPONSABILIDADES REFERENTES A SEGURANÇA DA INFORMAÇÃO

9.1. COMITÊ DE SEGURANÇA DA INFORMAÇÃO

A. Supervisionar a segurança da informação no âmbito da RT;
B. Constituir a Equipe de Tratamento e Resposta a Incidentes em Segurança da Informação (ETRISI);
C. Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;
D. Elaborar normas específicas que complementam esta Política em consonância com a Política da Estrutura Normativa RT;
E. Conduzir apurações quando da suspeita de ocorrências e incidentes em segurança da informação na RT;
F. Avaliar e aprimorar continuamente a PSI RT e suas normas de procedimentos complementares, visando a sua aderência aos objetivos institucionais da RT e às legislações aplicáveis vigentes;
G. Dirimir eventuais dúvidas e deliberar sobre assuntos relativos à PSI RT;
H. Monitorar e avaliar periodicamente o plano estratégico de segurança da informação, assim como determinar os ajustes cabíveis;
I. Apoiar a Alta Administração da RT no planejamento dos investimentos em segurança da informação com base nas exigências estratégicas e legais.

9.2. EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES EM SEGURANÇA DA INFORMAÇÃO (ETRISI)

Cabe à Equipe de Tratamento e Resposta a Incidentes em Segurança da Informação (ETRISI):

A. Coordenar as atividades de tratamento e resposta a incidentes de segurança;
B. Promover a recuperação de sistemas junto a área de TIC responsável;
C. Agir pró-ativamente com o objetivo de evitar que ocorram incidentes de segurança, divulgando práticas e recomendações de segurança da informação e avaliando condições de segurança de redes por meio de verificações de conformidade;
D. Realizar ações reativas que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos buscando causas, danos e responsáveis;
E. Analisar ataques e intrusões na rede da RT;
F. Executar as ações necessárias para tratar quebras de segurança;
G. Obter informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, causas, data de ocorrência, frequência e custos resultantes;
H. Cooperar com outras equipes de Tratamento e Resposta a Incidentes;
I. Apurar ações que violem a PSI RT ou quaisquer de suas diretrizes e normas de procedimento. Aos responsáveis serão aplicadas as sanções penais, administrativas e civis em vigor;
J. Participar em fóruns, redes nacionais e internacionais relativos à segurança da informação.

9.3. GESTOR DO ATIVO DE INFORMAÇÃO

Cabe ao Gestor do Ativo de Informação:

A. Seguir as diretrizes desta Política;
B. Garantir a segurança dos ativos de informação sob sua responsabilidade;
C. Definir e gerir os requisitos de segurança para os ativos de informação sob sua responsabilidade, em conformidade com esta Política;

D. Conceder e revogar acessos aos ativos de informação;
E. Comunicar à ETRISI a ocorrência de incidentes de segurança da informação;
F. Designar custodiante dos ativos de informação, quando aplicável.

9.4. CUSTODIANTE DO ATIVO DE INFORMAÇÃO

O Custodiante do Ativo de Informação:

A. Deve proteger e manter as informações, bem como controlar o acesso, conforme requisitos definidos pelo gestor da informação e em conformidade com esta PSI.
B. Deve ser formalmente designado pelo gestor do ativo de informação. A não designação pressupõe que o gestor é o próprio custodiante.

9.5. TITULAR DA UNIDADE RT

Cabe ao Titular da Unidade RT:

A. Conscientizar os usuários sob sua supervisão em relação às políticas e normas de segurança da informação da RT.
B. Incorporar aos processos de trabalho de sua unidade, ou de sua área, boas práticas em segurança da informação.
C. Tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da segurança da informação por parte dos usuários sob sua supervisão.
D. Garantir a realização do tratamento e a classificação da informação definidos nas Políticas e normas de procedimentos.
E. Autorizar, de acordo com a legislação vigente e as diretrizes do Comitê de Segurança da Informação, a divulgação das informações produzidas na sua unidade administrativa.
F. Comunicar à ETRISI os casos de quebra de segurança.
G. Solicitar suporte à ETRISI quando perceber riscos ou suspeitas de incidentes em segurança da informação;
H. Manter lista atualizada dos ativos de informação sob sua responsabilidade com seus respectivos gestores;

I. Informar a Diretoria de Recursos Humanos sobre a movimentação de pessoal de sua Unidade.

9.6. TERCEIROS E PARCEIROS COMERCIAIS DA RT

Cabe aos Terceiros e Parceiros Comerciais:

A. Tomar conhecimento e seguir as diretrizes estabelecidas pela RT em relação à segurança da informação.
B. Fornecer listas atualizadas da documentação dos ativos, licenças, acordos ou direitos relacionados aos ativos de informação, objetos do contrato.
C. Fornecer toda a documentação dos sistemas, produtos, serviços relacionados às suas atividades