PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Este **Plano de Resposta a Incidentes** de Segurança da Informação ("PRI") estabelece o procedimento para a gestão de situações após a identificação da ocorrência, ou mera suspeita, de um incidente de segurança da informação na ESSENTIA ENERGIA, incluindo todas as suas controladas e coligadas, marcas e divisões "ESSENTIA"), visando ao combate dos riscos e a minimização de eventuais efeitos relacionados a incidentes desta natureza.

O presente PRI foi elaborado de acordo com a Lei nº 13.709/18 (Lei Geral de Proteção de Dados Pessoais - LGPD) e deve ser lido em conjunto com a Política de Segurança da Informação da ESSENTIA.

ÍNDICE

1. OBJETIVOS

Este PRI estabelece as funções e responsabilidades das equipes para a gestão de situações após a identificação da ocorrência, ou mera suspeita, de um incidente de segurança da informação, inclusive aqueles envolvendo dados de pessoas naturais identificadas ou identificáveis, visando ao combate dos riscos e à minimização de eventuais efeitos relacionados a incidentes desta natureza.

2. DEFINIÇÕES

Para os efeitos deste PRI, as seguintes definições, quando escritas com a primeira letra maiúscula, terão os significados assinalados abaixo:

a) **"Colaborador":** sócios, diretores, administradores, empregados, prestadores de serviços, representantes comerciais, parceiros e/ou quaisquer outros similares que tiverem acesso às dependências e informações da ESSENTIA;

b) **"Dado Pessoal":** informação relacionada a uma pessoa natural identificada ou identificável (p. ex.: nome, CPF, endereço, telefone celular e e-mail), incluindo eventuais dados sensíveis;

c) **"Dado Sensível":** Dado Pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico;

d) **"Incidente":** qualquer ocorrência que comprometa a confidencialidade, disponibilidade, integridade, autenticidade ou auditabilidade dos ativos da ESSENTIA, inclusive Informações Protegidas ou Dados Pessoais tratados pela ESSENTIA; e

e) **"Informações Protegidas":** todo e qualquer dado ou informação que o Colaborador desenvolva ou venha a ter acesso em virtude do seu vínculo com a ESSENTIA ou do desempenho de suas atividades contratadas pela ESSENTIA, desdobrando-se em informações públicas, internas, confidenciais ou secretas, conforme a Política de Segurança da Informação da ESSENTIA.

3. ESCOPO

Este PRI destina-se a todas as áreas e Colaboradores da ESSENTIA, que, no âmbito das suas relações com o grupo, possam vir a ter acesso às áreas, equipamentos, informações, redes e aos arquivos e dados de tratados pela ESSENTIA. Este plano não abrange incidentes não relacionados à segurança cibernética, tais como desastres naturais (por exemplo, enchentes e incêndios) ou falhas físicas de equipamentos

4. O QUE É UM INCIDENTE DE SEGURANÇA DA INFORMAÇÃO?

Considera-se incidente de segurança da informação quaisquer ocorrências que comprometam a confidencialidade, disponibilidade, integridade, autenticidade ou auditabilidade dos ativos da ESSENTIA, inclusive Informações Protegidas ou Dados Pessoais tratados pela ESSENTIA.

Um Incidente pode ocorrer de forma maliciosa ou ser resultado de um erro humano ou, até mesmo, de falha nos sistemas ou ativos que tratam Informações Protegidas ou Dados Pessoais ou nos seus mecanismos de segurança. Isso pode incluir, por exemplo, o furto de um documento, o envio de um e-mail contendo Dados Pessoais para destinatários indesejados, tentativas de invasão a sistemas da ESSENTIA ou outras ações, culposas ou dolosas.

Os Incidentes podem ser de vários tipos, como por exemplo:

(i) **Vazamento.** É o Incidente no qual Informações Protegidas e/ou Dados Pessoais são indevidamente expostos e disponibilizados, por meios físicos ou digitais, para pessoas não autorizadas;

(ii) **Negação de Serviço.** É o Incidente no qual o acesso (lógico ou físico) a um sistema que armazene Informações Protegidas e/ou Dados Pessoais é prejudicado ou impossibilitado, de forma que a integridade das Informações Protegidas ou dos

Dados Pessoais (existência e/ou veracidade) pode ser comprometida permanentemente, dada a indisponibilidade do acesso;

(iii) **Acesso Não Autorizado.** É o Incidente no qual o acesso (lógico ou físico) a um sistema que tenha Informações Protegidas ou Dados Pessoais é tentado ou obtido, sem que se tenha a devida autorização para tal acesso. Considera-se acesso não autorizado qualquer acesso cuja permissão para conexão, leitura, gravação, autenticação, modificação, eliminação ou criação não foi concedida; e

(iv) **Uso Inapropriado.** É o Incidente no qual há a violação das leis ou políticas de uso de dados, informações e sistemas da ESSENTIA, incluindo a Política de Segurança da Informação, Política de Privacidade e demais políticas aplicáveis.

5. RESPONSABILIDADES

Cada área, sejam as áreas diretamente envolvidas na governança da ESSENTIA ou não, tem responsabilidades quando da ocorrência ou mera suspeita de um Incidente, conforme segue:

5.1. OBRIGAÇÕES DE TODAS AS ÁREAS

(i) comunicar imediatamente a Equipe de Resposta (conforme descrito abaixo), sobre a ocorrência ou a mera suspeita de um Incidente;
(ii) cumprir rigorosamente a Política de Segurança da Informação, contribuindo para a mitigação de riscos; e
(iii) participar de treinamentos e programas de conscientização para mitigação de Incidentes.

5.2. OBRIGAÇÕES DA EQUIPE DE RESPOSTA

A Equipe de Resposta é a equipe que realiza o gerenciamento de Incidentes da ESSENTIA, encarregada da coordenação, comunicação, acionamento de gestores ou demais departamentos e da tomada de decisões diante de suspeitas ou da efetiva ocorrência de Incidentes. Os membros da Equipe de Resposta podem ser consultados no ANEXO 1 deste PRI. Suas principais funções e responsabilidades são:

(i) Agir como primeiro ponto de contato para os usuários relatarem qualquer suspeita de Incidentes;
(ii) Registrar os Incidentes relatados com a gravidade identificada na análise inicial;
(iii) Acompanhar o andamento dos Incidentes;
(iv) Prover escalonamento e tratamento para os Incidentes;
(v) Após a resolução, solucionar os Incidentes; e
(vi) Coordenar o processo de resposta a Incidentes entre a ESSENTIA e parceiros.

5.3. OBRIGAÇÕES DA EQUIPE EXPANDIDA DE RESPOSTA

A Equipe Expandida de Resposta a Incidentes é um time multidisciplinar, formada pela Equipe de Resposta a Incidentes e por gestores de diversos departamentos, responsáveis por tomar decisões em casos de suspeita ou confirmação de Incidentes, além de coordenar os esforços e as comunicações internas e externas. Os membros podem ser consultados no ANEXO 2 – Membros da Equipe Expandida de Resposta. Suas principais funções e responsabilidades são:

(i) Informar as autoridades reguladoras conforme necessário;
(ii) Fornecer aconselhamento jurídico para quaisquer problemas, conforme necessário;
(iii) Instruir qualquer investigação externa de terceiros;
(iv) Aconselhar a ESSENTIA em questões relacionadas à força de trabalho;
(v) Ter ciência dos casos de eventos provocados por ações de colaboradores internos ou terceiros;
(vi) Elaborar e enviar comunicados internos e para acionistas ou outros interessados; e
(vii) Educar e conscientizar os Colaboradores sobre a detecção e resposta aos Incidentes.

5.3.1. ACIONAMENTO DA EQUIPE EXPANDIDA DE RESPOSTA

Sempre que um Incidente for identificado e classificado como de severidade média, alta ou crítica, a Equipe de Resposta deve acionar a Equipe Expandida de Resposta. A origem, o destino, o horário e os métodos de comunicação serão definidos conforme a criticidade dos Incidentes. Caso o método previsto esteja indisponível ou comprometido, poderão ser adotados meios alternativos. A ordem de acionamentos pode ser consultada no ANEXO 3 – Fluxo de comunicação para Incidentes.

5.4. NÍVEIS DE ESCALONAMENTO

Cada Incidentes deve ter um proprietário, responsável pelo seu gerenciamento e conclusão. O encaminhamento deve ocorrer se o proprietário atual não for capaz de fornecer recursos suficientes para garantir a resolução do Incidente. Cada nível tem autonomia para solucionar chamados de uma determinada severidade, ou incrementar a severidade e o nível para os próximos patamares:

- Nível 1: Formado pela Equipe de Resposta e possui autonomia para solucionar Incidentes de severidade baixa.
- Nível 2: Formado pela Gerência de Operações e possui autonomia para solucionar Incidentes de severidade média.
- Nível 3: Formado pela Diretoria de Operações e possui autonomia para solucionar Incidentes de severidade alta.
- Nível 4: Formado pela Presidência e possui autonomia para solucionar Incidentes de severidade crítica.

A tabela a seguir resume o caminho de escalonamento padrão para o proprietário dos Incidentes:

Nível	Proprietário	Severidade do Incidente	Autonomia
1	Equipe de Resposta	Baixa	Solucionar o Incidente ou escalar para nível 2
2	Gerencia de Operações	Média	Solucionar o Incidentes ou escalar para nível 3
3	Diretoria de Operações	Alta	Solucionar o Incidentes ou escalar para nível 4
4	Presidência	Crítica	Solucionar o Incidente

6. PROCEDIMENTO DE RESPOSTA

6.1. DETECÇÃO DO INCIDENTE

Detectar um Incidente de forma rápida e eficiente é essencial para uma resolução bem-sucedida. São várias as formas de detecção, de modo que é difícil desenvolver uma metodologia que contemple cada uma. Desta forma, **todos os Colaboradores** devem atentar-se aos sinais mais comuns que podem desencadear um Incidente, como invasões de rede, perda ou furto de documentos, arquivos ou dispositivos, *phishing*, *malware*, instabilidades sistêmicas etc.

Uma vez detectada a mera suspeita de um Incidente, o Colaborador deverá comunicar imediatamente a Equipe de Resposta a Incidentes, conforme canais de contato listados no ANEXO 1 deste PRI, mantendo o seu líder imediato sempre em cópia.

Na medida do possível, essa comunicação deverá conter (i) a hora e a data em que a suspeita do Incidente foi descoberta; (ii) o tipo de informações envolvidas; (iii) a causa e a extensão do Incidente; (iv) o contexto do ocorrido; bem como (v) qualquer informação adicional que sirva para facilitar o entendimento do evento, suas causas e consequências.

A COMUNICAÇÃO SOBRE A SUSPEITA DE UM INCIDENTE É VITAL PARA A ESSENTIA. ASSIM, CASO O COLABORADOR SUSPEITE DE UM INCIDENTE E NÃO O COMUNIQUE, SANÇÕES DISCIPLINARES PODERÃO SER APLICADAS, A DEPENDER DA GRAVIDADE DO INCIDENTE E DA COMPROVAÇÃO DE EVENTUAL NEGLIGÊNCIA DO COLABORADOR.

6.2. ANÁLISE E CLASSIFICAÇÃO DO INCIDENTE

Uma vez que o Incidente seja identificado, a Equipe de Resposta deverá priorizá-lo conforme o nível de risco oferecido à ESSENTIA e a gravidade da ocorrência para a definição de procedimentos de resposta.

Os Incidentes serão classificados pela Equipe de Resposta conforme abaixo, adotando-se ordem crescente de priorização:

Severidade	Critério
Crítica	• Impactos financeiros significativos e confirmados à ESSENTIA; • Necessidade de comunicação externa aos órgãos reguladores; • A ESSENTIA é incapaz de fornecer seus serviços; • O tempo de recuperação não é previsível ou a recuperação não é possível, sendo necessária a provisão de recursos com alto custo; • Além dos critérios acima, a classe de Informação Protegida afetada é secreta.
Alta	• Prejuízo parcial à disponibilidade e integridade dos recursos tecnológicos, à imagem da Empresa, porém, as operações externas com órgãos reguladores continuem operacionais e não tenham sido afetadas; • Possibilidade de impactos financeiros significativos à Essentia; • A ESSENTIA é incapaz de fornecer seus serviços para um grupo específico de usuários ou clientes; • O tempo de recuperação não é previsível e será necessária a provisão de alguns recursos; • Além dos critérios acima, a classe de Informação Protegida afetada é confidencial ou secreta.
Média	• A operação não tenha sido afetada, mas que necessite de atuação imediata para que o incidente não se agrave ou se propague; • Não existe impacto financeiro evidente ou significativo; • O incidente está controlado, mas deve ser monitorado; • A ESSENTIA ainda é capaz de fornecer seus serviços, porém a eficiência foi minimamente comprometida; • O tempo de recuperação é previsível, porém, será necessária a provisão de alguns recursos; • Além dos critérios acima, a classe de Informação Protegida afetada é de interna ou confidencial.
Baixa	• Baixo impacto coletivo ou departamental, considerado caso isolado; • Baixo risco funcional e financeiro. • Não afeta a capacidade da ESSENTIA de fornecer os seus serviços; • O tempo de recuperação é previsível e será atendido com os recursos existentes; • Além dos critérios acima, a classe de Informação Protegida afetada é pública ou interna.

Caso o Incidente envolva Dados Pessoais, a Equipe de Resposta deverá acionar o Encarregado, para que seja possível avaliar a necessidade de comunicação do Incidente às autoridades competentes e aos titulares de Dados Pessoais, conforme item 7 abaixo.

6.3. CONTENÇÃO, ERRADICAÇÃO E RECUPERAÇÃO

6.3.1. CONTENÇÃO

Na etapa de contenção, deverão ser tomadas as medidas adequadas para minimizar os danos causados pelo Incidente, enquanto é elaborada uma resposta apropriada para erradicá-lo. São processos de contenção:

- desconexão de uma sub rede suspeita;
- elaboração de relatórios de risco;
- execução de backup completo do(s) sistema(s);
- alteração de senha nos sistemas comprometidos;
- notificação ao *helpdesk*;
- análise de vulnerabilidade dos sistemas para identificar a origem do problema; ou
- qualquer outra ação necessária para mitigar os efeitos do Incidente.

As estratégias de contenção variam conforme a classificação do Incidente.

6.3.2. ERRADICAÇÃO

Esta fase inclui todas as ações associadas à identificação da causa raiz do Incidente, remoção de conteúdo malicioso e expulsão dos atacantes.

A erradicação é um processo necessário para eliminar os resquícios do Incidente e consiste na supressão de *malwares*, desabilitação de contas de usuário invadidas, identificação e mitigação das vulnerabilidades exploradas etc. Neste processo, é importante identificar todos os sistemas, as contas e as redes afetadas para que possa ser efetuado o reparo. Em alguns Incidentes, a erradicação pode não ser necessária ou, ainda, ser realizada durante a recuperação.

A fase de erradicação pode envolver os seguintes processos:

- executar os processos de escalonamento e notificações do Incidente de acordo com sua criticidade;
- verificação de sistemas;
- remoção de vírus e códigos maliciosos;
- avaliação de impacto em sistemas operacionais;
- restrição de permissões de acesso;
- mudanças em configurações de *softwares* e *hardwares*;
- outras ações para a erradicação de tipos específicos de Incidentes.

6.3.3. RECUPERAÇÃO

O objetivo desta etapa é normalizar os sistemas afetados, garantindo que não ocorra outro Incidente. Na recuperação, há a restauração dos sistemas afetados, confirmação de que todos os sistemas estão operando normalmente e, se necessário, a correção das falhas que desencadearam o Incidente. A recuperação pode ocorrer simultaneamente à etapa de erradicação e envolver os seguintes processos:

- reconstrução de sistemas;
- reposição de arquivos comprometidos;
- instalação de patches;
- fortificação de sistemas operacionais;
- reinicialização de sistemas (para negações de serviço);
- restauração de backups;
- reinstalação; e
- outras ações para a erradicação de tipos específicos de Incidentes.

6.4. ATIVIDADES PÓS INCIDENTE

Após o incidente deve ser realizado o levantamento de evidências que subsidiem a documentação do Incidente, bem como reportes externos, caso seja necessário. A documentação do Incidente deve ser atualizada e incrementada, contendo, além das informações iniciais:

- A indicação do responsável pela gestão do Incidente;
- As lições aprendidas a partir do Incidente; e
- A descrição das iniciativas que foram tomadas para ajudar a mitigar e eliminar futuros Incidentes.

7. NOTIFICAÇÃO DO INCIDENTE ÀS AUTORIDADES

7.1. NOTIFICAÇÃO DE INCIDENTES À AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

Em cumprimento à legislação brasileira, Incidentes que possam acarretar risco ou dano relevante aos titulares devem ser comunicados à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares. A avaliação sobre quais Incidentes são materialmente relevantes cabe à Equipe de Resposta a Incidentes junto ao Encarregado.

Para realizar a avaliação de risco do Incidente, conforme as orientações estabelecidas na Resolução CD/ANPD nº 15/2024, é necessário considerar a existência de, pelo menos, uma das condições descritas no Primeiro Critério e, cumulativamente, uma das condições descritas no Segundo Critério, elencados abaixo:

- **Primeiro Critério.** Quando o Incidente puder afetar significativamente os interesses e direitos fundamentais dos titulares. Por exemplo, quando o Incidente puder:

    - Impedir o exercício de direitos ou a utilização de um serviço; ou
    - Ocasionar danos materiais ou morais aos titulares, tais como atividades que envolvam (i) discriminação; (ii) violação à integridade física; (iii) violação ao direito de imagem e à reputação; (iv) fraude financeira; e (v) roubo de identidade.

- **Segundo Critério.** quando o Incidente envolver:

    - Dados Sensíveis;
    - dados de crianças, de adolescentes e idosos;
    - dados financeiros, assim considerados os Dados Pessoais relacionados às transações financeiras do titular, inclusive para contratação de serviços e aquisição de produtos;
    - dados de autenticação em sistemas, assim considerados qualquer Dado Pessoal utilizado como credencial para determinar o acesso a um sistema ou para confirmar a identificação de um usuário, como contas de login, tokens e senhas;
    - dado pessoal protegido por sigilo legal, judicial ou profissional; e
    - dados em larga escala, ou seja, abrange um número significativo de titulares, levando em consideração o volume de dados envolvidos e a extensão geográfica de localização dos titulares afetados.

Caso haja necessidade de notificação, o Encarregado providenciará, juntamente com o Departamento Jurídico, a comunicação do Incidente à ANPD e/ou aos titulares no prazo de 3 (três) dias úteis, contados do conhecimento de que o Incidente afetou Dados Pessoais.

A comunicação do Incidente deverá ser feita por peticionamento eletrônico no site da ANPD, através do preenchimento de formulário eletrônico disponível no site da autoridade. As informações poderão ser complementadas, de maneira fundamentada, no prazo de 20 (vinte) dias úteis, a contar da data da comunicação.

7.2. NOTIFICAÇÃO DE INCIDENTES À AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA

Em conformidade com a Resolução Normativa ANEEL nº 964/2021, a ESSENTIA deverá proceder à notificação imediata da equipe de coordenação setorial designada pela ANEEL sempre que ocorrer incidente cibernético de maior impacto, entendidos como aqueles que afetem de maneira substancial a segurança das instalações, a operação ou os serviços aos usuários ou de dados da ESSENTIA. Para fins deste PRI consideram-se incidentes de maior impacto aqueles classificados como de severidade Crítica ou Alta, conforme critérios estabelecidos no item 6.2 deste PRI.

A comunicação deve ocorrer assim que a ESSENTIA tiver ciência do incidente e de sua dimensão, e deve incluir, no mínimo:

- a análise da causa do Incidente;
- a avaliação do impacto (operacional, de dados, na continuidade do serviço etc.); e
- as ações de mitigação adotadas.

Essa notificação à ANEEL é complementar e não substitui outras obrigações de comunicação estabelecidas por outras legislações ou normativos, como aquelas previstas na LGPD ou pela Autoridade Nacional de Proteção de Dados (ANPD) e titulares afetados.

8. ATUALIZAÇÃO DESTE PLANO

Esse PRI poderá ser revisto, atualizado e alterado a qualquer tempo, a exclusivo critério da ESSENTIA, sempre que algum fato relevante ou evento motive sua revisão antecipada. Em caso de dúvidas, comentários ou sugestões relacionadas a este PRI, favor entrar em contato com a Equipe de Resposta a Incidentes.

Responsáveis:

Nome	Cargo	Função

Histórico:

Versão	Data	Descrição da Alteração	Revisado por	Aprovado por

9. ELABORAÇÃO DESTE PLANO

Responsáveis:

Nome	Cargo	Função	Assinaturas
Patricia de Araujo Levy	Gerente Executiva Jurídica e Diretora	Elaboração, Revisão e Aprovação	DocuSigned by: Patrícia de Araujo Levy 1695328762FE469...
Adrisson Floriano	Gerente de Tecnologia IT & OT	Elaboração e Revisão	Signed by: Adrisson Floriano C1E67E962241431...
Gilberto Luis Peixoto dos Santos Filho	COO	Revisão e Aprovação	Assinado por: C08C4748C6CC42A...

ANEXO 1 - MEMBROS DA EQUIPE DE RESPOSTA A INCIDENTES

Função	Nome	E-mail	Telefone
Analista OT	André Felipe	andre.alves@essentiaenergia.com.br	(084) 99211-5422
Analista IT	Gabriel Batista	gabriel.batista@essentiaenergia.com.br	(11) 95154-8309
Gerente de Tecnologia IT & OT	Adrisson Consoni Floriano	adrisson.floriano@essentiaenergia.com.br	(48) 99695-2570

ANEXO 2 – MEMBROS DA EQUIPE EXPANDIDA DE RESPOSTA

Função	Nome	E-mail	Telefone
General Counsel	Patrícia Levy	patricia.levy@essentiaenergia.com.br	+55 11 983816828
Gerente O&M e TI	Hudson Souza	hudson.souza@essentiaenergia.com.br	+55 11 99688-6347
COO	Gilberto Peixoto	gilberto.peixoto@essentiaenergia.com.br	+55 11 993690226
CFO	Gabriel Farias	gabriel.farias@essentiaenergia.com.br	+55 11 99353-1265
CEO	Francisco Moya	francisco.moya@essentiaenergia.com.br	+55 11 97561-8570

ANEXO 3 – FLUXO DE COMUNICAÇÃO PARA INCIDENTES

Este anexo estabelece o fluxo de comunicação a ser seguido em caso de Incidentes, garantindo uma resposta rápida, coordenada e eficaz. O objetivo é assegurar que todos os envolvidos sejam notificados de forma adequada e no tempo correto, de acordo com o nível de criticidade do Incidente.

a) Crítico

Origem	Destino	Horário	Método
Diretoria de Operações	Presidência Equipe Expandida de Resposta	24x7	Ligação telefônica Chat de grupo privado Mensagem por e-mail Microsoft Teams
Gerencia de Operações	Diretoria de Operações	24x7	Ligação telefônica Chat de grupo privado Mensagem por e-mail Microsoft Teams
Equipe de Resposta	Gerencia de Operações Outras equipes técnicas, conforme necessário	24x7	Ligação telefônica Chat de grupo privado Mensagem por e-mail Microsoft Teams
Colaborador	Equipe de Resposta	24x7	Ligação telefônica Chat de grupo privado Mensagem por e-mail Microsoft Teams

b) Alto

Origem	Destino	Horário	Método
Diretoria de Operações	Presidência	24x7	Ligação telefônica Chat de grupo privado Mensagem por e-mail Microsoft Teams
Gerencia de Operações	Diretoria de Operações	24x7	Ligação telefônica Chat de grupo privado Mensagem por e-mail Microsoft Teams
Equipe de Resposta	Gerencia de Operações Outras equipes técnicas, conforme necessário	24x7	Ligação telefônica Chat de grupo privado Mensagem por e-mail Microsoft Teams
Colaborador	Equipe de Resposta	24x7	Ligação telefônica Mensagem por e-mail

c) Médio

Origem	Destino	Horário	Método
Equipe de Resposta	Gerencia de operações	Horário comercial	Ligação telefônica Chat de grupo privado Mensagem por e-mail Microsoft Teams

Gerencia do SOC	Equipe de Resposta	Horário comercial	Mensagem por e-mail

d) **Baixo**

Origem	Destino	Horário	Método
Equipe de Resposta	Gerencia de operações	Horário comercial	Mensagem por e-mail
Colaborador	Equipe de Resposta	Horário comercial	Mensagem por e-mail