PORTARIA

Assunto: Aprova a Norma de Procedimentos: Resposta a Incidentes de Segurança da Informação (TI.03.001.2022)	**Nº** 09	**Ano**: 2022

O **PRESIDENTE DA FUNDAÇÃO GETULIO VARGAS**, no uso de suas atribuições estatutárias e considerando a necessidade de atualização das normas da FGV:

RESOLVE

Aprovar a *Norma de Procedimentos: Resposta a Incidentes de Segurança da Informação*, que estabelece as novas diretrizes a serem observadas para prevenir, classificar e tratar eventos suspeitos e confirmados de incidentes de segurança da informação, atendendo à Política de Segurança da Informação (TI.01.001.2019), em seu mecanismo de proteção de nº 12.

A presente Portaria e a Norma TI.03.001.2022 entram em vigor nessa data.

Rio de Janeiro, 17 de fevereiro de 2022.

Carlos Ivan Simonsen Leal
Presidente

D4Sign 2ef00ec5-c226-4810-aea9-da58e5b03f14 - Para confirmar as assinaturas acesse https://secure.d4sign.com.br/verificar
Documento assinado eletronicamente, conforme MP 2.200-2/01, Art. 10º, §2.

NORMA DE PROCEDIMENTOS:

RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

TI 03.001.2022

FEVEREIRO, 2022

D4Sign 2ef00ec5-c226-4810-aea9-da58e5b03f14 - Para confirmar as assinaturas acesse https://secure.d4sign.com.br/verificar
Documento assinado eletronicamente, conforme MP 2.200-2/01, Art. 10º, §2.

ÍNDICE

1. ABRANGÊNCIA 3
2. DOCUMENTOS DE REFERÊNCIA 3
3. OBJETIVOS 3
4. DEFINIÇÕES 3
4.1 Glossário 3
4.2 Princípios Interpretativos 5
5. PAPÉIS E RESPONSABILIDADES 6
5.1 Liderança da Unidade FGV 6
5.2 Interlocutores para Tratamento de Incidentes 6
5.3 Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (ETRISI) 7
5.4 Comitê de Segurança da Informação 7
6. DISPOSIÇÕES GERAIS 8
6.1. Quanto à Descoberta de Eventos Suspeitos ou de Incidentes 8
6.1.1. Detecção interna ou externa do incidente 8
6.1.2. Convocação da ETRISI 10
6.1.3. Apuração Preliminar 10
6.2. Quanto ao Tratamento e Resposta Inicial de Incidentes 11
6.2.1. Correções Preliminares 11
6.2.2. Notificações Preliminares 12
6.3. Quanto à Resposta Complementar e Documentação para Fechamento de Incidentes 13
6.3.1. Correções Complementares 13
6.3.2. Notificações Complementares 13
6.3.3. Documentação e fechamento do evento 14
7. DISTRIBUIÇÃO 14

D4Sign 2ef00ec5-c226-4810-aea9-da58e5b03f14 - Para confirmar as assinaturas acesse https://secure.d4sign.com.br/verificar
Documento assinado eletronicamente, conforme MP 2.200-2/01, Art. 10º, §2.

1. ABRANGÊNCIA

A presente *Norma de Procedimentos* define diretrizes para receber, classificar e responder a incidentes de segurança da informação, estejam eles associados a informações em qualquer tipo de formato, mídia ou suporte, eletrônico ou não.

São abrangidas em seu âmbito diretrizes sobre descoberta e classificação de eventos suspeitos e, se necessário, procedimentos para seu tratamento preliminar e complementar.

2. DOCUMENTOS DE REFERÊNCIA

i. Portaria FGV nº 65 de 08/10/2019 – Aprova a Política de Segurança da Informação da FGV;
ii. Portaria FGV nº 51 de 14/08/2020 – Aprova a Política de Privacidade e Proteção de Dados Pessoais da FGV;
iii. Portaria FGV nº 07 de 01/02/2021 – Cria o Comitê de Segurança da Informação no contexto da Política de Segurança da Informação da FGV;
iv. Portaria FGV nº 50 de 20/07/2021 – Cria a Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação da FGV (ETRISI);
v. Portaria FGV nº 54 de 29/07/2021 – Aprova a Norma de Procedimentos: Controle de Acessos a Sistemas Informáticos;
vi. Portaria FGV nº 82 de 26/10/2021 – Aprova a Norma de Procedimentos: Aquisição, Desenvolvimento e Manutenção de Sistemas Informáticos;
vii. Portaria FGV nº 83 de 26/10/2021 – Aprova a Norma de Procedimentos: Conformidade de Terceiros à Segurança da Informação e Proteção de Dados Pessoais.

3. OBJETIVOS

No conjunto de normas e controles previstos na Política de Segurança da Informação da FGV (TI.01.001.2019), consta como mecanismo de conformidade no processo de gestão da segurança da informação o item "12 – Gestão de Incidentes de Segurança da Informação".

Dessa maneira, a presente *Norma de Procedimentos* foi criada para atender ao item supracitado, criando um plano para resposta a incidentes de segurança da informação.

4. DEFINIÇÕES

4.1 Glossário

São definições sobre conceitos apresentados ao longo deste documento:

ANPD: Autoridade Nacional de Proteção de Dados Pessoais, entidade vinculada à Administração Pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional.

Cliente: pessoa física ou jurídica - que também pode ser um patrocinador, doador, financiador ou parceiro externo - para a qual a FGV desenvolve uma das atividades previstas no Artigo 2º do Título I do seu Estatuto.

D4Sign 2ef00ec5-c226-4810-aea9-da58e5b03f14 - Para confirmar as assinaturas acesse https://secure.d4sign.com.br/verificar
Documento assinado eletronicamente, conforme MP 2.200-2/01, Art. 10º, §2.

Comitê de Segurança Da Informação: comitê nomeado nos termos designados pela Portaria n.º 07 de 1 de fevereiro de 2021 e/ou outra norma competente que lhe venha a substituir ou alterar o teor.

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 a verificar a implementação e o cumprimento das normas públicas ou privadas concernentes às atividades da FGV.

Controladora: em operações de tratamento de dados pessoais, pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento, podendo ou não agir em concreto mediante auxílio de uma ou mais Operadoras.

Credencial: conjunto de informações e dados pessoais que permitem a uma pessoa ser identificada por um sistema e acessá-lo.

Dados Pessoais: todo e qualquer dado relacionado a pessoa natural identificada ou identificável (inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa).

Dados Pessoais Sensíveis: qualquer 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, quando vinculado a uma pessoa natural.

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.

Encarregado de Proteção de Dados Pessoais: na FGV, pessoa vinculada à Diretoria de Controles Internos (DCI) e indicada pela Presidência para manter e monitorar o programa de conformidade da FGV à Lei 13.709/2018 e às legislações correlatas.

ESI: Escritório de Segurança da Informação, Equipe vinculada à Diretoria de Operações e liderada pelo Chefe de Segurança da Informação (*Chief Information Security Officer*, no acrônimo em inglês), responsável pelo planejamento, execução e monitoramento das ações de segurança da informação no âmbito da FGV.

ETRISI: Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação, designada na forma da Portaria 50 de 20/07/2021 e que é responsável por apurar e indicar procedimentos preliminares para contenção de situações de crise em segurança da informação.

Fornecedores: no contexto da FGV são considerados fornecedores os terceiros contratados e subcontratados, modalidade pessoa física ou jurídica, desde que não qualificados como parceiros comerciais.

Incidente de Segurança da Informação: definido no item 6 desta *Norma de Procedimentos*.

Informações: qualquer dado, seja pessoal ou não pessoal, 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.

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

D4Sign 2ef00ec5-c226-4810-aea9-da58e5b03f14 - Para confirmar as assinaturas acesse https://secure.d4sign.com.br/verificar
Documento assinado eletronicamente, conforme MP 2.200-2/01, Art. 10º, §2.

LGPD: Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais, dispõe sobre o tratamento de dados pessoais, em meios físicos ou digitais, por pessoa natural ou por pessoa jurídica de direito público, ou privado.

Operadora: em operações de tratamento de dados pessoais, é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento em nome do Controlador.

Parceiros Comerciais: no contexto da FGV são considerados parceiros comerciais os terceiros contratados, modalidade pessoa física ou jurídica, que atuam em seu nome, como: Consultores, Conveniados e Agentes Comerciais.

Política de Segurança da Informação: política que estabelece as diretrizes gerais de proteção da informação na FGV. É válida e aplicável, no âmbito da FGV, a Política aprovada na forma da Portaria nº 65 de 2019 (TI.01.001.2019) e/ou outra versão posterior que lhe venha a substituir ou alterar o teor.

Terceiros: são os parceiros comerciais e os fornecedores da FGV.

Titular de Dados Pessoais: pessoa natural à qual um dado pessoal, identificado ou identificável, se refere. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais (art. 17, LGPD).

Tratamento: quaisquer ações referentes, de forma geral e não exaustiva, ao acesso, à recepção, produção, reprodução, utilização, transporte, transmissão, distribuição, armazenamento, eliminação e controle de informações e/ou dados pessoais.

Unidade FGV**:** são as áreas da Instituição que compõem a Administração Superior, a Administração Geral, Serviços, Índices e Publicações, Ensino e Programas Especiais.

4.2 Princípios Interpretativos

São princípios que auxiliam a interpretação das obrigações dispostas no item de obrigações gerais deste documento:

Menor privilégio: dispõe que somente deve ser concedido o menor acesso (mínimo necessário) para que uma pessoa possa exercer suas funções. Sua aplicação baseia-se no fato de que, no caso de comprometimento de uma credencial, qualquer acesso extra resultará em dano adicional não desejado.

Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de informações e/ou dados pessoais.

Rastreabilidade: dispõe que toda operação considerada importante, o que inclui aquela realizada com informações sensíveis, deve ser rastreável, sendo assim possível identificar o que, quem, quando e onde a informação foi tratada. Sua aplicação se baseia na necessidade de identificar possíveis problemas de segurança e suas origens, quando ocorrerem.

Responsabilização e prestação de contas: demonstração da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de segurança da informação e proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

D4Sign 2ef00ec5-c226-4810-aea9-da58e5b03f14 - Para confirmar as assinaturas acesse https://secure.d4sign.com.br/verificar
Documento assinado eletronicamente, conforme MP 2.200-2/01, Art. 10º, §2.

Segurança: utilização de medidas técnicas e administrativas aptas a proteger as informações e os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Transparência: garantia de demonstração, em patamar razoável, das medidas de zelo e cuidado para processar informações ou tratar dados pessoais, respeitados os segredos industrial e comercial.

5. PAPÉIS E RESPONSABILIDADES

5.1 Liderança da Unidade FGV

À Liderança da Unidade FGV compete:

- A leitura desta *Norma de Procedimentos*, para compreender possíveis implicações para a FGV de incidentes de segurança da informação;
- Apontar e informar à ETRISI o nome de um (ou mais) ponto(s) focal(is) com conhecimentos dos processos e rotinas da Unidade – especialmente os que digam respeito a sistemas e tecnologia da informação – para atuar(em) no papel de **Interlocutor(es) para Tratamento de Incidentes**, caso ocorra um incidente no âmbito de sua Unidade.

5.2 Interlocutores para Tratamento de Incidentes

São atribuições do Interlocutor(a) para Tratamento de Incidentes:

- A leitura desta *Norma de Procedimentos*, para compreender possíveis implicações para a FGV de incidentes de segurança da informação, especialmente os procedimentos listados ao seu item 6, funcionando como intermediários junto aos membros da ETRISI em caso de suspeita ou confirmação de incidentes de segurança da informação.

Entre as atividades listadas no item 6, de responsabilidade dos Interlocutores para Tratamento de Incidentes, destacam-se especialmente:

- Notificar/informar à ETRISI por e-mail caso suspeite da ocorrência de um incidente de segurança da informação.
- Auxiliar a ETRISI para a tomada de ações preliminares emergenciais que se façam necessárias para cessar ou mitigar o incidente de segurança da informação;
- Levantar listas de Titulares de Dados Pessoais ou outras informações sobre as circunstâncias do incidente;
- Colaborar no que for preciso para notificações preliminares ou complementares;

D4Sign 2ef00ec5-c226-4810-aea9-da58e5b03f14 - Para confirmar as assinaturas acesse https://secure.d4sign.com.br/verificar
Documento assinado eletronicamente, conforme MP 2.200-2/01, Art. 10º, §2.

- Intermediar comunicações que eventualmente sejam obrigatórias a Entidades externas (a exemplo, mas não limitado, a Clientes ou Terceiros) afetadas por um incidente de segurança da informação;

5.3 Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (ETRISI)

São atribuições da ETRISI:

- À ETRISI caberá receber e apurar as suspeitas ou ocorrências de incidentes de segurança da informação para fazer cumprir esta *Norma de Procedimentos*.

Entre as atividades listadas no item 6 de responsabilidade da ETRISI, destacam-se especialmente:

- O recebimento e processamento de denúncias ou comunicações de ameaças de incidentes de segurança da informação ou de incidentes confirmados;

- A realização de reuniões emergenciais ou complementares para avaliar a criticidade de incidentes e a requisição de recomendações ou esclarecimentos;

- A avaliação de ações técnicas preliminares e/ou complementares necessárias, ouvido o ESI, para fazer cessar o incidente ou mitigar seus riscos ou danos, inclusive com comunicação e apoio dos Interlocutores para Tratamento de Incidentes;

- O encaminhamento de notificações preliminares e/ou complementares, ouvido o Encarregado de Proteção de Dados Pessoais quando o incidente envolver dados pessoais, com o apoio da Diretoria de Comunicação e Marketing e/ou dos Interlocutores para Tratamento de Incidentes;

- A documentação e fechamento do incidente, subsidiando o aprendizado e a prevenção de eventos similares no futuro;

- A comunicação ou submissão de consultas ou situações críticas ao Comitê de Segurança da Informação.

5.4 Comitê de Segurança da Informação

São atribuições do Comitê de Segurança da Informação:

- Avaliar casos especiais que digam respeito à aplicação desta *Norma de Procedimentos*;

- Supervisionar a ETRISI no que for necessário em relação a apurações e contenções de incidentes de segurança da informação.

D4Sign 2ef00ec5-c226-4810-aea9-da58e5b03f14 - Para confirmar as assinaturas acesse https://secure.d4sign.com.br/verificar
Documento assinado eletronicamente, conforme MP 2.200-2/01, Art. 10º, §2.

6. DISPOSIÇÕES GERAIS

É considerado um incidente de segurança da informação a violação de confidencialidade, integridade e/ou disponibilidade da informação. Esta violação deverá ser devidamente descoberta, apurada e classificada, a fim de receber tratamento preliminar e complementar com vistas a eliminar ou mitigar seu dano ou risco de dano. Um incidente poderá se relacionar tanto a informações contidas em sistemas eletrônicos de tecnologia da informação quanto àquelas contidas em suporte ou mídia física e/ou impressa.

Podem ser exemplos de incidentes os acessos não autorizados, as situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou outra forma de tratamento inadequado ou ilícito de informações. O incidente poderá ainda, envolver dados pessoais, caso em que será necessário avaliar se ele implica em dano ou risco relevante aos Titulares de Dados Pessoais e avaliar comunicações que se façam necessárias segundo a LGPD e a ANPD.

As diretrizes de segurança da informação e proteção de dados pessoais relativas a esta *Norma de Procedimentos* são concentradas na ETRISI, observadas as etapas abaixo dispostas para o recebimento e o tratamento preliminar e complementar de incidentes de segurança da informação.

6.1. Quanto à Descoberta de Eventos Suspeitos ou de Incidentes

Todo evento que implique em suspeita razoável de incidente de segurança da informação ou em incidente confirmado deverá receber tratamento por parte da ETRISI, observada nesta etapa de descoberta os seguintes passos:

6.1.1. Detecção interna ou externa do incidente

- Canais de internos de notificação/denúncia de incidentes e conteúdo da notificação:

- Quando necessário, qualquer pessoa, interna ou externa à FGV, poderá notificar/denunciar suspeitas de incidentes de segurança da informação ou incidentes confirmados à ETRISI, **utilizando-se do seguinte canal de e-mail:**

➡ **comitedeseguranca@fgv.br**

Caso o notificante/denunciante seja interno à FGV, é possível ainda usar, de forma subsidiária e caso ocorra qualquer problema de envio com o e-mail acima, um entre os seguintes canais:

(i) Uso de canal próprio intranet presente no Portal de Serviços da FGV, por meio do caminho "Portal de Serviços da FGV" > "Tecnologia da Informação" > "Portal Serviços TIC" > "Escritório de Segurança da Informação" > "Incidente de Segurança da

D4Sign 2ef00ec5-c226-4810-aea9-da58e5b03f14 - Para confirmar as assinaturas acesse https://secure.d4sign.com.br/verificar
Documento assinado eletronicamente, conforme MP 2.200-2/01, Art. 10º, §2.

Informação" ou de outro caminho ou solução que vier a substituir a acima apresentada;

(ii) Uso de canal próprio (a ser desenvolvido) no Sistema de Conformidade da FGV.

- Sempre que possível, a notificação/denúncia deverá conter o máximo de informações disponíveis entre as abaixo listadas, permitindo a identificação e compreensão do evento suspeito, a exemplo de:

(i) Data e hora da detecção do evento;

(ii) Data e hora do incidente e sua duração;

(iii) Circunstância em que ocorreu a suspeita de incidente de segurança da informação ou o incidente confirmado (exemplo: se uma perda, furto, roubo, cópia não autorizada, vazamento ou outro evento indesejado);

(iv) Descrição das informações e/ou dados pessoais envolvidos, sua natureza e conteúdo, indicando-se quantitativos de informações, organizações ou pessoas naturais afetadas;

(v) Resumo do evento com indicação da localização física e do meio de armazenamento das informações e/ou dados pessoais envolvidos;

(vi) Possíveis consequências e efeitos negativos para as organizações ou pessoas naturais afetadas;

(vii) Medidas de segurança, de ordem técnica e administrativa, que eram usadas preventivamente para proteger as informações e/ou dados pessoais;

(viii) Resumo de ações emergenciais que eventualmente já tenham sido tomadas antes do conhecimento da ETRISI sobre o evento e de medidas implementadas para controlar possíveis danos;

(ix) Indicação de eventuais implicações transnacionais do evento (se o evento envolver organizações ou pessoas vinculadas a outras jurisdições);

(x) Outras informações que possam ser úteis às pessoas naturais ou organizações afetadas para prevenir ou mitigar danos causados pelo evento.

Caso as informações acima não possam ser fornecidas de forma completa, qualquer dos itens supramencionados poderá ser informado para dar sequência à apuração pela ETRISI, acompanhado sempre que possível de prints ou registros dos eventos suspeitos.

- À ETRISI, mediante o suporte do ESI, caberá levantar as informações restantes, especialmente e se for o caso, requisitando ou recuperando *logs* ou registros de sistemas.

- Meios adicionais de detecção de incidentes:

D4Sign 2ef00ec5-c226-4810-aea9-da58e5b03f14 - Para confirmar as assinaturas acesse https://secure.d4sign.com.br/verificar
Documento assinado eletronicamente, conforme MP 2.200-2/01, Art. 10º, §2.

Sem prejuízo dos canais de notificação/denúncia acima, as suspeitas ou ocorrências confirmadas de incidente de segurança da informação poderão ser descobertas a partir de fontes internas ou externas à FGV (ou, concomitantemente, de mais de uma delas).

- No âmbito de fontes internas adicionais para detecção de incidentes, cita-se os seguintes exemplos de situações pelas quais ETRISI poderá tomar ciência de um evento, sem prejuízo de outras situações não aqui listadas: denúncias/notificações encaminhadas por empregados, terceiros, alunos, pesquisadores, bolsistas ou quaisquer outras pessoas com vínculo com a FGV, bem como outros tipos de situações ou consultas que cheguem à ciência do ESI, do Encarregado de Proteção de Dados Pessoais ou do Diretor de Comunicação e Marketing da FGV e que possam implicar em um incidente de segurança da informação.

- No âmbito de fontes externas para detecção de incidentes, cita-se igualmente como exemplos de situações em que a ETRISI poderá tomar ciência de um evento, sem prejuízo de outras situações não aqui listadas: denúncias/notificações encaminhadas por terceiros (especialmente Instituições de Ensino Conveniadas ao Instituto de Desenvolvimento Educacional - IDE), por Clientes, por veículos de mídia/blogs/jornais ou por quaisquer outras pessoas naturais ou instituições externas à FGV.

6.1.2. Convocação da ETRISI

- Reunião emergencial

Uma vez detectada uma denúncia/notificação de suspeita ou ocorrência confirmada de incidente de segurança da informação, o membro da ETRISI que primeiro tiver ciência do evento suspeito deverá convocar os demais para uma reunião emergencial de apuração e levantamento preliminar de ações necessárias, conforme o item 6.1.3 abaixo.

Se, por qualquer motivo, algum membro da ETRISI não puder estar presente nas reuniões emergenciais de apuração e este não houver indicado um substituto, ou este não puder ser encontrado, caberá aos demais membros seguir com as apurações necessárias sobre o evento.

6.1.3. Apuração Preliminar

- Identificação da tipologia do evento

Convocada a reunião emergencial da ETRISI, caberá aos seus membros uma avaliação preliminar sobre o evento notificado, a partir dos indicadores e informes disponíveis. Nesta etapa, caberá com especial atenção aos pareceres do ESI e do Encarregado de Proteção de Dados Pessoais, definir a tipologia do evento, indicando a melhor opção de resposta concomitante para cada um dos pontos (i), (ii) e (iii) a seguir:

> (i) Se o evento decorre de ação oriunda de uma ou mais das seguintes opções: (a) acidental, (b) maliciosa, (c) exploração de vulnerabilidade em boa-fé ("*ethical hacking*" *ou "white hat hacking*"), ou, (d) ainda não classificada;

D4Sign 2ef00ec5-c226-4810-aea9-da58e5b03f14 - Para confirmar as assinaturas acesse https://secure.d4sign.com.br/verificar
Documento assinado eletronicamente, conforme MP 2.200-2/01, Art. 10º, §2.

(ii) Se a violação ou suspeita de violação afeta uma ou mais das seguintes propriedades: (a) confidencialidade, (b) integridade e/ou a (c) disponibilidade das informações ou dados pessoais, bem como o grau de certeza dos informes recebidos;

(iii) Se a violação ou suspeita de violação envolve ou poderá envolver uma ou ambas as seguintes circunstâncias: (a) dados pessoais segundo a LGPD e, ainda, se implica ou pode implicar em (b) dano ou risco relevante aos respectivos Titulares de Dados Pessoais, especialmente se envolver dados pessoais sensíveis, ou titulares em situação de vulnerabilidade ou outra situação que possa agravar o risco em concreto.

- Avaliação de verossimilhança e classificação do evento para prosseguimento

Uma vez avaliadas as informações acima, a ETRISI ponderará se existem elementos razoáveis para seguir com o prosseguimento da apuração do evento, classificando-o como *uma* das opções abaixo:

(i) Evento descartado, registrados os fundamentos para tanto;

(ii) Evento de suspeita fundamentada de incidente de segurança da informação;

(iii) Evento confirmado de incidente de segurança da informação.

Nos casos **(ii) e (iii)** acima – evento suspeito ou confirmado –, a ETRISI deverá seguir para a etapa de tratamento e resposta inicial de incidentes conforme o item 6.2 abaixo, sem prejuízo de reavaliação da classificação adotada acima caso surjam novos elementos.

6.2. Quanto ao Tratamento e Resposta Inicial de Incidentes

De forma concomitante, as seguintes ações abaixo deverão ser avaliadas para a resposta inicial ao incidente de segurança da informação.

6.2.1. Correções Preliminares

- Ações emergenciais aplicáveis:

Uma vez identificada a procedência da suspeita fundamentada ou do evento confirmado de incidente de segurança da informação e a sua classificação, a ETRISI deliberará se existe alguma correção preliminar em regime de urgência a ser tomada, a exemplo, mas não limitado, a: desligamento/retirada do ar parcial ou integral de um sistema ou aplicação; comunicação à Autoridade Policial, caso seja detectado que o evento decorre de ação maliciosa; ou a contratação de consultoria externa especializada em cibersegurança para conter ou fazer cessar a ameaça.

Caberá aos Interlocutores para Tratamento de Incidentes auxiliar a ETRISI nesse processo e seguir as orientações dela recebidas, especialmente as recomendações técnicas emanadas pelo ESI, solicitando o auxílio de quem se fizer necessário na FGV para mitigar o dano ou risco apurado.

D4Sign 2ef00ec5-c226-4810-aea9-da58e5b03f14 - Para confirmar as assinaturas acesse https://secure.d4sign.com.br/verificar
Documento assinado eletronicamente, conforme MP 2.200-2/01, Art. 10º, §2.

Caso detecte que as ações emergenciais a serem tomadas exijam a contratação de consultoria externa especializada em cibersegurança, a ETRISI poderá solicitar ou indicar a solicitação de investimentos em caráter de urgência às instâncias competentes da FGV.

6.2.2. Notificações Preliminares

- Apuração de existência do dever de notificar, especialmente, mas não limitado, à ANPD:

Serão ainda avaliados eventuais compromissos decorrentes de normas de ordem pública, não adstritos à LGPD, para a notificação a eventuais interessados, observadas as seguintes nuances abaixo.

6.2.2.1. Caso o incidente de segurança da informação envolva dados pessoais e, se a FGV figurar em concreto como a Controladora de dados pessoais, tais compromissos poderão, após avaliação técnica/jurídica, incluir a notificação à ANPD e aos Titulares de dados pessoais, nos prazos e na forma designados pela própria ANPD e/ou pela LGPD.

Tais avaliações serão de competência primária da Equipe do Encarregado de Proteção de Dados Pessoais, a qual registrará, no documento interno "*Avaliação do Dever de Notificação de Incidentes com Dados Pessoais Conforme a LGPD*" (ou outro que o substitua) e, se for necessário, em parecer, as razões e observações peculiares sobre o caso e os motivos determinantes para a recomendação de abstenção ou sequência com a notificação.

Neste último caso, o Comitê de Segurança da Informação da FGV será, antes da emissão das notificações, ouvido em caráter emergencial. Após seu parecer, a Equipe do Encarregado de Dados Pessoais poderá seguir com as notificações obrigatórias à ANPD nos termos da LGPD.

Quando o dever de notificação aos Titulares de dados pessoais for detectado, a ETRISI deverá se preocupar em notificar ações para conter ou fazer cessar os riscos a estes Titulares. São exemplos destas notificações: instruções para evitar fraudes, troca de senhas, bem como mecanismos para monitoramento de documentos pessoais e prevenção a golpes de engenharia social, entre outros. Ainda, caberá à Diretoria de Comunicação e Marketing (DICOM) auxiliar, caso necessário, com o disparo das mensagens. Os Interlocutores para Tratamento de Incidentes auxiliarão, ainda, no que eventualmente se fizer necessário para levantar o contato dos Titulares afetados.

6.2.2.2. Se o incidente de segurança da informação envolver dados pessoais para os quais a FGV figurar como a Operadora, caberá à ETRISI, ouvido o Comitê de Segurança da Informação, a avaliação e recomendação de notificação do evento à Instituição Externa que figurar como Controladora (seja um Cliente ou Terceiro). O envio da notificação, contudo, será de competência

D4Sign 2ef00ec5-c226-4810-aea9-da58e5b03f14 - Para confirmar as assinaturas acesse https://secure.d4sign.com.br/verificar
Documento assinado eletronicamente, conforme MP 2.200-2/01, Art. 10º, §2.

dos Interlocutores para Tratamento de Incidentes e/ou quem por eles for indicado.

6.2.2.3. Por fim, caso o incidente de segurança da informação não envolva dados pessoais, mas a ETRISI verifique em concreto que existe dever de notificação decorrente de norma pública, ela indicará, após ouvido o Comitê de Segurança da Informação, o seu parecer aos Interlocutores para Tratamento de Incidentes para que procedam com as comunicações necessárias junto a Clientes ou Terceiros que eventualmente se façam pertinentes. Se não houver dever decorrente de norma pública para notificação, a ETRISI encaminhará igualmente o seu parecer, cabendo, contudo, aos Interlocutores para Tratamento de Incidentes acionar o respectivo Departamento Jurídico competente da FGV para avaliar se existem obrigações decorrentes de contrato para notificação.

6.3. Quanto à Resposta Complementar e Documentação para Fechamento de Incidentes

6.3.1. Correções Complementares

- Ações complementares aplicáveis:

Após tomadas as ações preliminares/emergenciais de correção do incidente de segurança da informação, a ETRISI acompanhará a eventual necessidade de ações complementares de correção de erros ou vulnerabilidades detectadas e poderá cobrar a apresentação, por parte dos Interlocutores para Tratamento de Incidentes – ou de outras pessoas por eles indicadas – de plano de medidas corretivas contendo cronograma de ações.

Igualmente, se for necessária a contratação de serviços externos para execução de ações complementares de correção do incidente de segurança da informação, a ETRISI poderá solicitar ou indicar a solicitação de investimentos às instâncias competentes da FGV.

6.3.2. Notificações Complementares

- Apuração de existência do dever de complementar notificação, especialmente, mas não limitado, à ANPD:

Após efetuadas notificações preliminares e no mesmo sentido do item 6.2.2, a ETRISI avaliará a necessidade de proceder com eventuais notificações complementares, cumprindo especialmente os prazos e expedientes determinados pela ANPD caso o incidente de segurança da informação envolva dados pessoais.

Na eventualidade da ANPD determinar a instauração de qualquer procedimento ou expediente administrativo para apurar o incidente de segurança da informação, também caberá à ETRISI, especialmente a partir da Equipe do Encarregado de Proteção de Dados Pessoais e do ESI, acompanhar e auxiliar na resposta a questionamentos, diligências ou requisições que forem dirigidas à FGV.

D4Sign 2ef00ec5-c226-4810-aea9-da58e5b03f14 - Para confirmar as assinaturas acesse https://secure.d4sign.com.br/verificar
Documento assinado eletronicamente, conforme MP 2.200-2/01, Art. 10º, §2.

6.3.3. Documentação e fechamento do evento

- Fechamento do evento e arquivamento criptografado no Núcleo de Documentação

Uma vez efetuadas as correções e as notificações complementares que se façam necessárias e, eventualmente se determinada a baixa/conclusão da ocorrência junto às Autoridades e órgãos oficiais, a ETRISI procederá ao arquivamento da ocorrência, especialmente dos documentos e registros concernentes ao caso. Em até 6 (seis) meses do término do evento, será solicitado ao Núcleo de Documentação da FGV (NDOC) o arquivamento dos registros internos.

Para o arquivamento do processo no NDOC, haja vista o sigilo das ocorrências, será feito o envio de um arquivo criptografado com parâmetros seguros de senha, a qual por sua vez será mantida no Cofre de Senhas da FGV.

- Lições aprendidas

Por fim, caso já não o tenha feito ao decorrer das demais etapas anteriores, a ETRISI avaliará o evento traçando recomendações para evitar/prevenir que ele se repita na FGV, a partir das lições e experiências do caso enfrentado.

Será, ainda, construído um banco de dados contendo classificação dos incidentes ocorridos e as formas de tratamento para cada um.

7. DISTRIBUIÇÃO

Esta *Norma de Procedimentos* se destina ao Presidente, Vice-Presidentes, empregados, estagiários, alunos, parceiros comerciais (consultores, agentes comerciais e conveniados) que lidem ou possam lidar com informações ou dados pessoais presentes nos sistemas e/ou registros da FGV, estejam eles associados a qualquer tipo de formato, mídia ou suporte, eletrônico ou não.

D4Sign 2ef00ec5-c226-4810-aea9-da58e5b03f14 - Para confirmar as assinaturas acesse https://secure.d4sign.com.br/verificar
Documento assinado eletronicamente, conforme MP 2.200-2/01, Art. 10º, §2.

DOCUMENTO	Norma de Procedimentos: Resposta a Incidentes de Segurança da Informação
DIMENSÃO	Estrutura Normativa de Procedimentos
TIPO DE INSTRUMENTO NORMATIVO	Norma de Procedimentos
CATEGORIA DO ASSUNTO	Tecnologia da Informação
ASSUNTO	Segurança da Informação e Conformidade
IDENTIFICAÇÃO	TI. 03.001.2022
VERSÃO ANTERIOR	Não se aplica

ELABORAÇÃO:	**APROVAÇÃO:**
NOME: Jordan Vinícius de Oliveira	NOME: Carlos Ivan Simonsen Leal
POSIÇÃO: Encarregado de Proteção de Dados Pessoais	POSIÇÃO: Presidente
VERSÃO: 1.0/2022	PORTARIA Nº: 09/2022

D4Sign 2ef00ec5-c226-4810-aea9-da58e5b03f14 - Para confirmar as assinaturas acesse https://secure.d4sign.com.br/verificar
Documento assinado eletronicamente, conforme MP 2.200-2/01, Art. 10º, §2.

DICOM

D4Sign 2ef00ec5-c226-4810-aea9-da58e5b03f14 - Para confirmar as assinaturas acesse https://secure.d4sign.com.br/verificar
Documento assinado eletronicamente, conforme MP 2.200-2/01, Art. 10º, §2.

Portaria 09 22 NP Resposta a Incidentes pdf

Código do documento 2ef00ec5-c226-4810-aea9-da58e5b03f14

Anexo: TI.03.001.22 NP Resposta a Incidentes.pdf

Assinaturas

Thiago Antonio França Oliveira
thiago.oliveira@fgv.br
Reconheceu

Thiago Antonio França Oliveira

LEONARDO JOSÉ MELO BRANDÃO
leonardobrandao@deciofreire.com.br
Assinou

LEONARDO JOSÉ MELO BRANDÃO

Carlos Ivan Simonsen Leal
Carlos.Leal.1944@fgv.br
Assinou

Carlos Ivan Simonsen Leal

Eventos do documento

24 Feb 2022, 18:53:51
Documento 2ef00ec5-c226-4810-aea9-da58e5b03f14 **criado** por ROBERTO FLAVIO OTTONI BARBOSA JUNIOR (c65b7783-18d1-4caa-a46d-1ee092e82c11). Email:Roberto.ottoni@fgv.br. - DATE_ATOM: 2022-02-24T18:53:51-03:00

24 Feb 2022, 18:58:18
Assinaturas **iniciadas** por ROBERTO FLAVIO OTTONI BARBOSA JUNIOR (c65b7783-18d1-4caa-a46d-1ee092e82c11). Email: Roberto.ottoni@fgv.br. - DATE_ATOM: 2022-02-24T18:58:18-03:00

25 Feb 2022, 10:46:25
THIAGO ANTONIO FRANÇA OLIVEIRA **Reconheceu** (09334ea1-2566-470a-b44d-8f4879533300) - Email: thiago.oliveira@fgv.br - IP: 201.39.147.100 (201.39.147.100 porta: 31162) - Geolocalização: -22.9407 -43.1863 - Documento de identificação informado: 105.867.597-43 - DATE_ATOM: 2022-02-25T10:46:25-03:00

25 Feb 2022, 17:34:42
LEONARDO JOSÉ MELO BRANDÃO **Assinou** (0419d26c-da12-46e1-a9ea-213fdeb2cf82) - Email: leonardobrandao@deciofreire.com.br - IP: 179.107.103.82 (82-103-107-179.telbrax.net.br porta: 45262) - Geolocalização: -19.9473864 -43.9608197 - Documento de identificação informado: 562.287.596-04 - DATE_ATOM: 2022-02-25T17:34:42-03:00

25 Feb 2022, 17:48:27
CARLOS IVAN SIMONSEN LEAL **Assinou** (2e1bb2c8-afe2-4769-9e94-af8fb312b834) - Email: carlos.leal.1944@fgv.br - IP: 179.132.73.13 (179-132-73-13.user.vivozap.com.br porta: 63856) - Geolocalização: 40.76513165695124

-73.9748491508653 - Documento de identificação informado: 441.982.057-87 - DATE_ATOM: 2022-02-25T17:48:27-03:00

Hash do documento original

(SHA256):32dbbe81b361f9046513e7b23bea6cc07c0fec4754d6d5d2c4b754b4bcfd166b
(SHA512):999f1e3ea95eb3e2266b24fa91ca5cf925a326b7b2f22895fff43db9469552aec551555106a12bcc96017ea1bf47772f94b1aa212b548450c53c94a9cdcb3f62

Hash dos documentos anexos

Nome: TI.03.001.22 NP Resposta a Incidentes.pdf
(SHA256):49276132bfbb34658b9e326c7513b59240bd9318e512d2a7d45b36d72af1183e
(SHA512):16f655d9136e596c9ea9e888fffc0a69c51830a09b17b32509fcc5d7da8f8a7f4c91acce096fa1bbd41cff054a70d6030b93f30286bed0eeb80b886cb1d137e9

Esse log pertence **única** e **exclusivamente** aos documentos de HASH acima

Esse documento está assinado e certificado pela D4Sign