Decálogo Forense Digital

2022

Decálogo Forense Digital

Ciudad de México a 24 de mayo de 2022

CONSIDERANDO:

Que en el marco del Foro sobre Ciberseguridad, celebrado en octubre de 2017, se firmó el documento "Principios para el fortalecimiento de la ciberseguridad para la estabilidad del Sistema Financiero Mexicano". Entre los cinco principios de este documento destaca el que busca establecer mecanismos seguros para el intercambio de información entre integrantes del Sistema Financiero Mexicano y las Autoridades Financieras, sobre ataques ocurridos en tiempo real y su modo de operación, estrategias de respuesta, nuevas amenazas, así como del resultado de investigaciones y estudios, que permitan a las entidades financieras anticipar acciones para mitigar los riesgos de ciberataques; lo anterior, protegiendo la confidencialidad de la información.

Que el día 24 de mayo de 2018 se firmaron las Bases de Coordinación en Materia de Seguridad de la Información por parte de las personas representantes de las seis Autoridades Financieras del Sistema Financiero Mexicano, la entonces Procuraduría General de la República, (actualmente Fiscalía General de la República), y diversas asociaciones gremiales del Sistema Financiero Mexicano, las cuales tienen por objeto establecer las directrices para la colaboración que las instancias públicas se brindarán entre ellas, en coordinación con las Asociaciones Gremiales y las entidades financieras, en materia de seguridad de la información.

Que a fin de implementar lo dispuesto en las citadas Bases, en particular, en las disposiciones Tercera, Quinta y Séptima de las mismas, y atendiendo al ciclo de gestión de incidentes tradicional, previsto en la disposición Octava del Protocolo de coordinación y colaboración del Grupo de Respuesta a Incidentes Sensibles de Seguridad de la Información, se emite el presente:

Decálogo Forense Digital

PRIMERA. OBJETIVO

El presente documento contiene guías que podrían adoptar las entidades financieras que operan en México para que realicen la identificación, recolección, preservación, análisis y entrega de evidencia forense digital ante la ocurrencia de un incidente que afecte la seguridad de la información. Este documento fue elaborado con base en estándares y buenas prácticas internacionales sobre la materia[1], buscando homologar los procedimientos que sigan las entidades financieras, y cuidando

[1] Por ejemplo: NIST SP 800-86 Guide to Integrating Forensic Techniques into Incident Response y NIST SP 800-61 Computer Security Incident Handling Guide.

que haya un balance en las actividades que las lleven de regreso a la operación y la adecuada recopilación de evidencia forense digital**.**

El objetivo de este documento es difundir entre las entidades financieras, con un enfoque estructurado y planificado, los pasos básicos previo, durante y posterior a que ocurra un incidente de ciberseguridad que podrían seguir para identificar, recolectar y preservar información válida en un proceso legal y cuyo análisis podría determinar el origen del incidente, responder de forma efectiva y realizar acciones para reducir y/o mitigar la probabilidad de que un incidente similar se pueda materializar.

En este sentido, el análisis de la evidencia forense digital recolectada durante un incidente también puede apoyar a las entidades financieras a detectar las vulnerabilidades en un sistema, y a analizar las causas del ataque informático que ha sufrido, con el objetivo principal de extraer datos contenidos en pruebas electrónicas, transformarlos en información de utilidad operativa y presentar las conclusiones.

Las actividades expuestas en el Decálogo Forense Digital son parte de un procedimiento fundamental dentro del proceso de Gestión de Incidentes, ya que no todos los incidentes se pueden resolver con un triage convencional. Por lo que para llegar al objetivo de las mismas se requiere de una valoración de costo-beneficio y de un estudio de factibilidad donde cada entidad financiera identificará los recursos con los que cuenta y las necesarias; esto con el fin de cumplir con las 10 actividades expuestas en el presente documento.

Las etapas de identificación, recolección, preservación, análisis y entrega de evidencia forense digital ante la ocurrencia de un incidente se relacionan con las directrices descritas en estándares internacionales los cuales cuentan con procesos diseñados para respetar la integridad de la evidencia, y con una metodología aceptable para asegurar su admisibilidad en procesos legales.

Cabe mencionar que **la presente guía no constituye una regulación**, sino un complemento a la misma. En este sentido, la observancia de esta guía no exime a las entidades financieras del cumplimiento de otras disposiciones que les resulten aplicables.

SEGUNDA. DEFINICIONES

Para efecto del presente documento, adicionalmente a las definiciones contenidas en la disposición ***Segunda de las Bases de Coordinación en Materia de Seguridad de la Información***[2], ya sea que las expresiones se utilicen en singular o plural, se entenderá por:

I. **"Autoridades Financieras":** SHCP, CNBV, BANXICO, CONDUSEF, CONSAR y CNSF.

II. **"Cadena de Custodia":** Principio jurídico relativo a la validez e integridad de las pruebas. Conjunto de actos y medidas que tienen como objeto la recolección, el traslado y la

[2] https://www.banxico.org.mx/sistema-financiero/d/%7BD0502AA8-7721-5C2C-5C8F-05858CBB4AE7%7D.pdf

conservación de los indicios o vestigios obtenidos en el curso de una investigación con el fin de asegurar la autenticidad e integridad de las fuentes de prueba.

III. **"CISO":** Por sus siglas en inglés Chief Information Security Officer, persona que funge como Oficial en Jefe de Seguridad de la Información de una **"Entidad"**. Para el presente documento, la persona que funja como **"CISO"** tiene el rol de coordinar a las áreas de seguridad de la información, a las áreas de tecnología y a las áreas operativas de la **"Entidad"**; a fin de implementar las presentes guías.

IV. **"Componente de infraestructura de TI":** Servidores (p. e. Windows, Linux y/o UNIX); servidores de bases de datos, servidores de aplicaciones, estaciones de trabajo, equipos de cómputo portátil, elementos de telecomunicaciones (switches y/o ruteadores, puntos de acceso, enlaces, etc.), controles de seguridad informática (antivirus, firewall, filtrado de contenido web, firewalls de aplicaciones web, detectores de intrusos, etc.), aplicativos o sistemas críticos satélites, entre otros.

V. **"Consultora especializada":** Empresa que presta servicios especializados y que cuenta con conocimientos, experiencia y certificaciones en Análisis Forense Digital.

VI. **"Entidades":** Las controladoras y subcontroladoras de grupos financieros, instituciones de crédito, casas de bolsa, bolsas de valores, fondos de inversión, sociedades operadoras de fondos de inversión, instituciones de seguros, instituciones de fianzas, administradoras de fondos para el retiro, empresas operadoras de la base de datos nacional SAR, almacenes generales de depósito, uniones de crédito, casas de cambio, sociedades financieras de objeto múltiple reguladas, sociedades financieras populares, instituciones para el depósito de valores, contrapartes centrales, instituciones certificadoras de valores, cámaras de compensación, instituciones de tecnología financiera, sociedades de la información crediticia, sociedades financieras comunitarias sujeta a la supervisión de la CNBV, organismos de integración financiera rural, otras sociedades, instituciones y fideicomisos públicos que realicen actividades financieras y respecto de los cuales la CNBV, la CONSAR o la CNSF ejerzan facultades de supervisión, así como las sociedades cooperativas de ahorro y préstamo sujetas a la supervisión de la CNBV, todas ellas constituidas conforme a las leyes mercantiles y financieras.

Quedarán comprendidas dentro de la presente definición las demás personas físicas y morales, cuando realicen actividades previstas en las leyes relativas al Sistema Financiero Mexicano sujetas a la supervisión y regulación de la CNBV, la CONSAR o la CNSF, así como las sociedades autorizadas para operar con Modelos Novedosos, en términos de la Ley para Regular las Instituciones de Tecnología Financiera.

VII. **"Evidencia Forense Digital Volátil":** Datos que pudieran establecer o refutar hechos, que se pierden si los **"Componentes de infraestructura de TI"** en donde estos residen son

apagados. Ejemplos de **"Evidencia Forense Digital Volátil"** son: procesos en ejecución, actividad de la red y conexiones, y datos en la memoria RAM.

VIII. **"FGR":** Fiscalía General de la República.

IX. **"Imagen Forense Digital":** Es una copia "bit a bit" de los medios de almacenamiento internos de los **"Componentes de infraestructura de TI"**. Las **"Imágenes Forenses Digitales"** se pueden generar cuando los **"Componentes de infraestructura de TI"** estén encendidos o apagados.

X. **"Incidente de Seguridad de la Información" o "ISI" o "Incidente":** Evento que efectiva o potencialmente pone en peligro la confidencialidad, integridad o disponibilidad de un componente o la totalidad de la infraestructura tecnológica o de la información que se procesa, almacena o transmite; que puede representar una pérdida, alteración o extravío de información; o bien que constituye una violación o una amenaza inminente de violación de las políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable; que puede derivar en interrupción o daño o pérdida del servicio o bien, en daño o pérdida para clientes de la **"Entidad"** afectada, para el público en general, para sus contrapartes o para la **"Entidad"** misma, que afecte la entrega de los servicios o exponga información crítica de la persona que sea cliente o de la **"Entidad"**. Entre ellos se encuentran:

a) El acceso no autorizado a los datos, especialmente datos confidenciales.

b) Equipos infectados con programas maliciosos, tales como gusanos, virus, troyanos o botnets.

c) Actividades de reconocimiento, como escaneos de red en busca de vulnerabilidades informáticas conocidas o "de día cero".

d) Ataques de Denegación de Servicio (DoS).

e) Defacement de sitios web.

f) Violación a las políticas de seguridad.

XI. **"Incidente Sensible de Seguridad de la Información" o "ISSI":** Evento evaluado que efectiva o potencialmente pone en peligro la confidencialidad, integridad o disponibilidad de un componente o la totalidad de la infraestructura tecnológica o de la información que se procesa, almacena o transmite; que puede representar una pérdida, alteración o extravío de información; o bien, que constituye una violación o una amenaza inminente de violación de las políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable; que puede derivar en interrupción del servicio; o bien, en daño o pérdida para las personas que

sean clientes de la **"Entidad"** afectada, para el público en general, para sus contrapartes o para la **"Entidad"** misma, siempre y cuando dicho evento:

a) Pudiera representar una afectación a:

- Más de una **"Entidad"**;
- Un número significativo de personas que sean clientes de las **"Entidades"**;
- La estabilidad del sistema financiero mexicano o de pagos, o bien;
- A los sistemas centrales de pagos, cámaras de compensación o a las personas que funjan como depositarias centrales de valores, u;

b) Observe las siguientes características:

- Genere pérdida económica, de información o interrupción de los servicios de la **"Entidad"** de que se trate;
- Su modo de operación se pueda replicar a otras **"Entidades"**;
- Pueda representar un alto riesgo a la reputación de las **"Entidades"** u otras personas participantes del sistema financiero, o bien;
- Pueda generar desconfianza del público.

XII. **"Indicador de Compromiso" o "IOC":** Un indicador de compromiso (Indicator of compromise, por sus siglas en inglés) es artefacto técnico u observable (un evento en una red o sistema) asociado a un ataque, y que sugiere si dicho ataque es inminente, está ocurriendo o que ya ocurrió. Este observable podría ser una dirección IP, un nombre de dominio, una URL que refiere contenido malicioso, el "hash" o "huella digital" de un archivo malicioso (p.e. un script, malware, exploit, etc.), el texto de un asunto de un mensaje de correo electrónico, entre otros.

XIII. **"Protocolo para compartir información de inteligencia de amenazas e incidentes":** Documento que establece los pasos que la **"Entidad"** deberá seguir para distribuir inteligencia de ciberamenazas con las **"Autoridades Financieras"**, **"FGR"** y otras **"Entidades"** (p. e. **"Indicadores de Compromiso"** generados durante un incidente de ciberseguridad).

XIV. **"SIEM":** Security Information and Event Management o sistema correlacionador de eventos.

TERCERA. ACTIVIDADES A EJECUTAR PREVIO A UN "INCIDENTE"

Fase del proceso de respuesta a incidentes al que corresponde: Preparación.

Las actividades de la presente sección podrán aplicarse por la **"Entidad"** bajo la coordinación de la persona que funja como **"CISO"** para estar preparadas ante la eventual materialización de un **"Incidente"**:

1. **Identificar** los elementos **("Componentes de infraestructura de TI"** y aplicativos) y definir las infraestructuras críticas que soportan los procesos de la **"Entidad"**, así como aquellos que proveen servicios de acceso remoto, firewalls perimetrales de Internet y, en su caso, de Directorio Activo.

   Es importante dar la máxima prioridad en la identificación señalada en este punto para los sistemas que soportan los procesos críticos y gestionan los recursos económicos que son más susceptibles a amenazas cibernéticas tales como el robo o secuestro de información sensible (p. e. *ransomware*) y la instrumentación de operaciones financieras no reconocidas principalmente para la transferencia de recursos económicos de la **"Entidad"** y/o de las personas que sean clientes de la misma, es decir, los servicios ofertados por las Entidades (p. e. sistemas o procesadores de pagos, sistemas de corresponsalía, sistemas de cajeros automáticos, servicio de transferencias a través de sucursales, transferencias de fondos para retiro de efectivo, banca móvil, banca en internet, entre otros).

2. **Realizar**, al menos cada semana, respaldos de información completos de servidores identificados en el numeral 1, así como **validar** que dichos respaldos están siendo resguardados en un sistema especializado para tal propósito.

3. **Confirmar** o, en su caso, **realizar** los ajustes necesarios para que las bitácoras generadas por los elementos identificados en el numeral 1, contengan, al menos, lo estipulado en el Anexo A del presente documento.

   Resguardar, al menos diariamente, una copia de las bitácoras generadas por los elementos identificados en el numeral 1, y de los controles de seguridad informática en un sistema especializado para tal propósito (p. e. un **"SIEM"**), considerando una retención de estas conforme a lo establecido en la regulación aplicable.

4. **Contar** con un **"Protocolo para compartir información de inteligencia de amenazas e incidentes"**, mantener actualizado el directorio de contactos y previstos los mecanismos para reportar un **"Incidente"** a las **"Autoridades Financieras"** correspondientes y a la **"FGR"**, principalmente para presentar la denuncia y evidencia recolectada en un eventual **"Incidente".**

CUARTA. ACTIVIDADES A EJECUTAR DURANTE UN "INCIDENTE"

Fase del proceso de respuesta a incidentes al que corresponde: Detección, Análisis y Contención.

Las actividades de la presente sección podrán aplicarse por la **"Entidad"** bajo la coordinación de la persona que funja como **"CISO"**, a partir de que éste último ha confirmado la materialización de un **"Incidente"**:

5. **Desconectar o aislar** de la red institucional los elementos identificados en el numeral 1 relacionados con el **"Incidente"**. Es recomendable mantener el estado del dispositivo (si está apagado, no encenderlo y viceversa). Estos elementos no podrán ser utilizados para restaurar la operación hasta que la persona que funja como **"CISO"** confirme la conclusión del proceso de recolección forense digital, por lo que la **"Entidad"** deberá poner en marcha los mecanismos de operación alterna que tenga implementados.

6. Tan pronto como sea posible y una vez que se haya realizado la contención del **"Incidente"**, **reportar** el mismo a las **"Autoridades Financieras"** correspondientes. Para solicitar apoyo técnico y legal durante la investigación del **"Incidente"**, contacte a la **"FGR".**

7. **Realizar al menos** las actividades siguientes para que la recolección de evidencia permita generar un análisis forense:

    - **Obtener "Evidencia Forense Digital Volátil"** y bitácoras de servidores, estaciones de cómputo y equipos de cómputo portátil identificados en el numeral 1 relacionados con el **"Incidente"**.

    - **Obtener "Imágenes Forenses Digitales"** de los medios de almacenamiento internos de los servidores, estaciones de cómputo y equipos de cómputo portátil identificados en el numeral 1 relacionados con el **"Incidente"**.

    - **Recolectar** bitácoras de los elementos de telecomunicaciones, de los controles de seguridad informática con los que cuente y de aquellos que proveen servicios de acceso remoto, firewalls perimetrales de Internet y Directorio Activo, que fueron identificados en el numeral 1 y que estén relacionados con el **"Incidente"**, así como de las bitácoras almacenadas en el **"SIEM"** indicados en el numeral 3.

    - **Generar**, al menos, tres copias de la información recolectada y **resguardarlas** en medios de almacenamiento externo previamente formateados a bajo nivel. Una copia será considerada como la "copia original", y las otras dos copias se propone se destinen para los análisis correspondientes por parte de la **"Entidad"** y, en su caso, por parte de la **"FGR"**.

- **Etiquetar, embalar, y almacenar** los medios de almacenamiento externo, en presencia de alguna persona que funja como representante legal o tercera persona contratada para este propósito; y de un auditor interno o externo.

- **Documentar** el procedimiento realizado como parte de lo señalado en el presente numeral 7 y la o las cadenas de custodia respectivas[3].

QUINTA. ACTIVIDADES A EJECUTAR POSTERIOR A UN "INCIDENTE"

Fase del proceso de respuesta a incidentes: Erradicación y Recuperación.

8. **Realizar** el análisis forense digital conforme se vayan generando las copias de la información recolectada en el numeral 7 y si se requiere, apoyarse de una empresa **"Consultora especializada"** que cuente con las certificaciones técnicas requeridas para este fin. Una vez que se recolectó la evidencia de todos los sistemas involucrados en el **"Incidente",** iniciar el proceso de erradicación y recuperación de un **"Incidente"**, el cual abarca la restauración de los **"Componentes de infraestructura de TI"**, aplicativos afectados y el regreso a las operaciones habituales de la **"Entidad".**

   Analizar la evidencia forense digital recolectada en el siguiente orden:
   - **"Evidencia Forense Digital Volátil"** y bitácoras de: servidores, estaciones de cómputo y equipos de cómputo portátil.
   - Bitácoras de los elementos de telecomunicaciones, controles de seguridad informática y aquellos que proveen servicios de acceso remoto, firewalls perimetrales de Internet y Directorio Activo; así como de bitácoras almacenadas en el **"SIEM".**
   - **"Imágenes Forenses Digitales".**

9. **Identificar** nuevos elementos asociados con el **"Incidente"** y **efectuar** nuevamente las actividades previstas en los numerales 7, 8 y 9. Conforme se vaya obteniendo información adicional del análisis forense e **"Indicadores de Compromiso"**, compartirla con las **"Autoridades Financieras"** y la **"FGR"**.

10. **Entregar** una copia de la información recolectada en el numeral 7 a la **"FGR"**, con el fin de obtener apoyo en su análisis, **documentar** la cadena de custodia e informar a la **"Autoridad Financiera"** competente. Explicar a la **"FGR"** los hechos que conozca sobre el **"Incidente"**,

[3] Se sugieren revisar las siguientes referencias para documentar la cadena de custodia: 1) DOF: 12/02/2015 ACUERDO A/009/15 por el que se establecen las directrices que deberán observar los servidores públicos que intervengan en materia de cadena de custodia. Anexo 3 "Registro de Cadena de Custodia" 2)ISO/IEC 27037:2012, 3)ISO/IEC 27041:2015, 4)ISO/IEC 27042:2015, 5)ISO/IEC 27043:2015 y 6) NIST SP 800-86.

considerando la descripción del **"Incidente"**, el impacto a la **"Entidad"**, los elementos involucrados hasta el momento, entre otros.

La seguridad de la información es una responsabilidad de todos.

Banco de México
Dirección General de Contraloría y Administración de Riesgos
Dirección de Ciberseguridad
Gerencia del Centro de Inteligencia y Respuesta

"ANEXO A"

Registro de eventos en las bitácoras de "Componentes de infraestructura de TI" y aplicativos

El registro de eventos en una bitácora estará formado por campos, en los cuales se podrá incorporar información cuyo análisis coadyuvará a dar una respuesta objetiva a lo sucedido en un determinado momento dentro de un **"Componente de infraestructura de TI"** o un aplicativo.

Dentro de los campos a incorporar en los eventos se encuentran al menos los siguientes campos:

1. Fecha y hora de la generación del evento considerando preferentemente la zona horaria de la Ciudad de México. Se recomienda sincronizar el reloj interno del **"Componente de infraestructura de TI"** o aplicativo con un servidor NTP (*Network Time Protocol*).
2. Tipo de evento, por ejemplo: acceso denegado a un usuario no autorizado.
3. Nombre, dirección IP y si es el caso el puerto TCP/UDP utilizados por el **"Componente de infraestructura de TI"** o aplicativo que realizó la actividad o aplicativo que genera el evento (origen).
4. Nombre, dirección IP y si es el caso el puerto TCP/UDP utilizado por el **"Componente de infraestructura de TI"** o aplicativo en donde se presentó el evento (destino).
5. Nombres, claves o cualquier otro identificador de las personas usuarias involucradas.
6. Nivel de severidad o criticidad del evento.

El campo 2, "tipo de evento", describe un suceso específico ocurrido en un **"Componente de infraestructura de TI"** o aplicativo que posiblemente esté relacionado con una anomalía o con su seguridad informática. Los eventos que son de interés para la seguridad informática son aquellos que proveen información clave para la búsqueda proactiva de anomalías y amenazas, para la detección temprana de **"ISI" e "ISSI",** y para el cómputo forense incluyendo al menos los siguientes eventos:

- Accesos exitosos a los **"Componentes de infraestructura de TI"** o aplicativos.
- Intentos de acceso fallidos a los **"Componentes de infraestructura de TI"** o aplicativos.
- Accesos exitosos y fallidos a información sensible contenida en los **"Componentes de infraestructura de TI"** o aplicativos, incluyendo al menos:
    - Carpetas compartidas.
    - Bases de datos.
    - Configuración para la administración de los **"Componentes de infraestructura de TI"** o aplicativos.
    - Entre otros.
- Creación, accesos, modificación y/o borrado de información restringida contenida en los **"Componentes de infraestructura de TI"** o aplicativos.
- Modificaciones en la administración de personas usuarias, incluyendo:
    - Creación y/o eliminación de personas usuarias o grupos.

  - Cambios en los niveles de privilegios de las personas usuarias.
  - Modificación de las contraseñas de personas usuarias.
  - Cambios en la forma en la que se conectan las personas usuarias (por ejemplo: local y remoto).
- Cambios en las configuraciones para la administración de los **"Componentes de infraestructura de TI"** o aplicativos.
- Conexiones de red establecidas con otros **"Componentes de infraestructura de TI"** o aplicativos.
- Inicio, finalización y/o reinicio de procesos y/o servicios de los **"Componentes de infraestructura de TI"** o aplicativos.
- Activación, desactivación y/o falla de controles de seguridad informática implementados en los **"Componentes de infraestructura de TI"** o aplicativos, por ejemplo: el antivirus.
- Fallas en la validación de entrada y salida de datos en las interfaces con las cuales interactúan los **"Componentes de infraestructura de TI"** o aplicativos con las personas usuarias, por ejemplo: una aplicación web.
- Fallas y/o comportamiento anormal de los recursos de **"Componentes de infraestructura de TI**" o aplicativos, por ejemplo: debido al agotamiento anormal de los recursos como son CPU, memoria, conexiones de red, ancho de banda de red, espacio en disco duro, entre otros.
- En caso de tratarse de un control de seguridad informática (p. e. el servidor antivirus), las actividades relacionadas con la detección y bloqueo de actividad sospechosa o maliciosa de **"Componentes de infraestructura de TI"** que este protegiendo.

El campo 6, "nivel de severidad o criticidad del evento", permite identificar de forma expedita su importancia, el análisis de la información contenida en los restantes campos del evento, las acciones a ejecutar y la urgencia con que se ejecutarán, si es el caso.

Cada **"Componente de infraestructura de TI"** o aplicativo podría registrar los eventos clasificándolos en, al menos, los siguientes niveles de severidad o criticidad:

- Informativo: informar sobre la ocurrencia de acciones anormales en el funcionamiento de los **"Componentes de infraestructura de TI"** o aplicativos.
- Advertencia: anunciar situaciones de falla o indisponibilidad de algún **"Componente de infraestructura de TI"** o aplicativo, que no afectan necesariamente su funcionamiento general.
- Error: notificar fallas en el **"Componente de infraestructura de TI"** o aplicativo que pueden conllevar a comportamientos inestables y/o resultados inexactos o erróneos.
- Alerta: indicar sucesos relevantes que representan afectaciones significativas en el funcionamiento del **"Componente de infraestructura de TI"** o aplicativo.
- Alarma: indicar vulneraciones de seguridad del **"Componente de infraestructura de TI"** o aplicativo.

BANCO DE MÉXICO®

www.banxico.org.mx