Forensic Readiness: Guía de buenas prácticas

Mónica D. Tugnarelli [(1)], Francisco Javier Díaz [(2)]
[(1)] Facultad de Ciencias de la Administración –
Universidad Nacional de Entre Ríos
[(2)] Facultad de Informática – Universidad Nacional de La Plata
e-mail: montug@fcad.uner.edu.ar, jdiaz@unlp.edu.ar

Abstract. En este artículo se presenta una guía de buenas prácticas para la implementación del enfoque preventivo denominado Forensic Readiness, el cual propone aplicar tratamiento de evidencia digital a los datos que se recolecten antes de la ocurrencia de un incidente de seguridad. La guía está dividida en cinco etapas con actividades y resultados para cada una de ellas y puede considerarse una base de partida para la adopción de Forensic Readiness en cualquier tipo de organización que quiere proteger su información y pretende iniciarse en este proceso. Esta guía está estrechamente relacionada e integrada a las políticas de seguridad y a las de continuidad del negocio, requiriendo del compromiso de todos los niveles organizaciones para su correcto cumplimiento.

Keywords: Forensic Readiness, buenas prácticas, continuidad digital, seguridad

1 Introducción

Forensic Readiness o Preparación Forense es un enfoque preventivo que plantea que la evidencia digital se recolecte y asegure de manera anticipada, es decir antes de la ocurrencia de un incidente de seguridad. Este término fue enunciado por John Tan [1] quien lo describió principalmente a través de dos objetivos: maximizar la capacidad del entorno para reunir evidencia digital confiable y minimizar el costo forense durante la respuesta a un incidente.

En trabajos anteriores se ha realizado un análisis comparativo de las prestaciones de este enfoque preventivo contrastándolo con un enfoque reactivo, donde los datos se recolectan a posteriori de un incidente, es decir, sobre un evento consumado, arribando a la conclusión de que Forensic Readiness proporciona un mejor mecanismo activo de anticipación y de respuesta a los incidentes, a la protección de activos y al resguardo de evidencia digital. [2] [3].

Establecer el momento de la recolección de datos es donde radica la principal diferencia con la informática forense, que actúa luego de cometido el delito o incidente, cuando se ha incautado el dispositivo sospechoso y se han establecido puntos de pericia. En este último escenario se tiende a ignorar qué ha sucedido con el objeto de la investigación antes del incidente de seguridad y antes de la decisión de realizar una investigación.

En coincidencia, ambos enfoques consideran a la evidencia como el insumo primario para cualquier investigación forense y que por su carácter preponderadamente volátil debe contemplar aspectos básicos en cuanto a su recolección, integridad, relevancia, almacenamiento, trazabilidad y mantenimiento de la cadena de custodia. Para ello toman lo especificado por normativas tales como la RFC 3227 *"Directrices para la recopilación de evidencias y su almacenamiento"* [4] y la ISO/IEC 27037 "*Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence"* [5], entre otras.

La Preparación Forense, trata a los datos seleccionados como evidencia forense desde el momento de la recolección y, para seleccionar esos datos que serán resguardados como evidencia, es necesario identificar los activos primarios, determinar métodos de recolección, asegurar la cadena de custodia y mantener a toda la organización trabajando en conjunto para asegurar que cada prueba recolectada pueda ser utilizada tanto en el proceso de investigación forense como ante un proceso judicial en caso de ser requerido.

La continuidad digital, entendida como la capacidad de usar la información de la organización de la manera en que se necesite y durante el tiempo que se requiera [6], tiene una relación intrínseca con Forensic Readiness, planteada como tal desde el inicio de la planificación de la continuidad o desde el diseño de la política de seguridad, convirtiéndose esta preparación en uno de los requisitos del negocio y una actividad clave en la identificación de activos de información de la organización.

No existe una normativa estandarizada para implementar la preparación forense, pero en lo que sí coinciden los autores que han avanzado en modelos conceptuales de Forensic Readiness, tales como Pooe y Labuschagne [7] y Jan Collie [8], es que la protección de la información es un punto crítico al que cualquier organización debería prestar atención y en ese sentido preocuparse por adoptar mecanismos para asegurar tanto el resguardo de información como su propia continuidad como negocio.

El enfoque preventivo puede ser muy efectivo, lo que ante un incidente de seguridad redundará en un ahorro de tiempo y dinero. Sin embargo, la complejidad del entorno objeto del análisis exige que la definición de los detalles del procedimiento sean precisados desde el inicio con el fin de identificar los activos de la organización, seleccionar los datos a preservar y determinar aspectos de trazabilidad de los datos, entre otros, motivos por los cuales en este trabajo se propone una guía de buenas prácticas, que se presenta en el punto siguiente, y que puede ser de utilidad para la implementación de Forensic Readiness en una organización.

2 Guía de Buenas Prácticas para la implementación de Forensic Readiness

La Guía de Buenas Prácticas que se propone puede considerarse como una base de partida para la implementación de Forensic Readiness y está organizada en cinco etapas. Esta estructura en etapas permite minimizar la complejidad del proceso, así la organización puede avanzar en la medida de su capacidad pero de manera constante, sabiendo que a mayor nivel de madurez alcanzará procesos y procedimientos más detallados y de mejor calidad.
En la Figura 1 se representa gráficamente las etapas propuestas, las actividades mínimas que comprenden y lo que se debería lograr como producto de cada etapa:

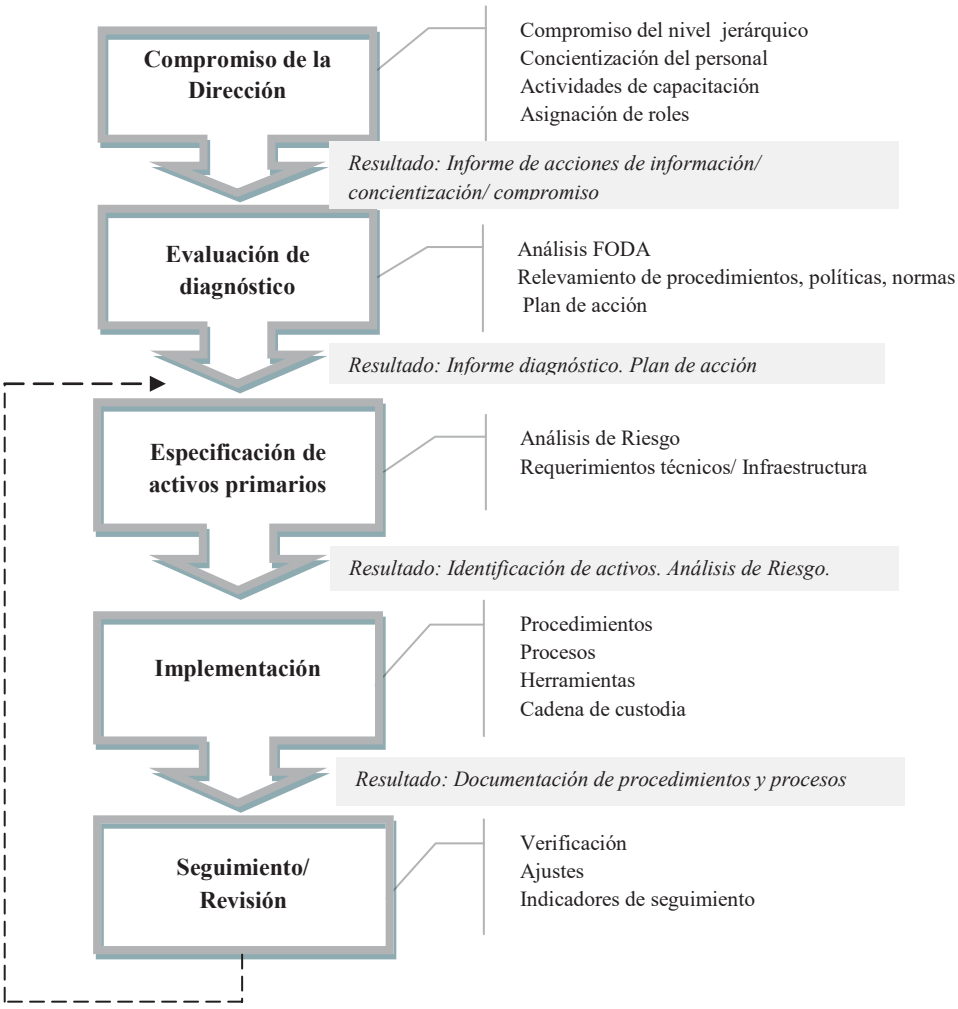

Figura 1. Etapas para la implementación de Buenas Prácticas en Forensic Readiness

A continuación se describen brevemente cada una de las etapas.

2.1 Compromiso de la Dirección

Cuando se decide implementar un enfoque Forensic Readiness, donde los controles sobre la información son muy estrictos, la dirección de la organización tiene una tarea esencial: comprometerse y tratar de lograr el compromiso de todos los niveles. Es fundamental que los niveles jerárquicos asuman la responsabilidad porque son los que tienen una visión estratégica y entienden claramente los objetivos de negocio.

Se deben realizar reuniones informativas, capacitaciones en seguridad informática y acciones de concientización para que cada persona esté al tanto de los procedimientos adoptados, que pueda participar en las diferentes fases de la implementación y así de esta manera, avanzar hacia la meta de que toda la organización trabaje en pos de la seguridad de los datos.

Un rol destacado tendrán los puestos de administrador del sistema de información, el administrador de redes de datos y el administrador de la seguridad. Sobre ellos recae la responsabilidad técnica de aplicar los procedimientos específicos sobre los datos a recolectar. Deben estar capacitados profesionalmente en seguridad informática, en ciberseguridad, en herramientas de Ethical Hacking, entre otros, para contar con las competencias y habilidades adecuadas para este proceso de preparación forense. Serán los primeros que deberán detectar las fallas de seguridad y reaccionar en consecuencia, tratando de mantener operativa la infraestructura de la organización, aplicar las herramientas de forensia, asegurar la evidencia y dar rápida respuesta para mantener la continuidad digital.

Como resultado de esta etapa se debe producir un documento que detalle las acciones de capacitación y concientización llevadas a cabo, indicando el grado de cumplimiento y la cantidad de personal que ha participado en las diversas instancias.

2.2 Evaluación de diagnóstico

De acuerdo a las acciones realizadas en la Etapa 1, el personal de la organización estará en condiciones de participar de este diagnostico aportando desde las características propias de sus puestos de trabajo en relación a cuestiones de seguridad y actividades relacionadas con el tratamiento de los datos. Como herramientas participativas de diagnóstico pueden emplearse entrevistas, reuniones por sector y ampliadas, encuestas, cheklists y demás instrumentos que ayuden a lograr una evaluación integral de la organización y su contexto.

Por otra parte, se deben analizar los procedimientos y políticas existentes con respecto a la seguridad informática, como así también las normas y leyes vigentes que correspondan aplicar.

Si es necesario puede completarse el diagnostico con un análisis FODA para conocer las amenazas, debilidades, oportunidades y fortalezas de la organización, sobre todo en lo relativo a la seguridad interna y externa.
Como producto de esta etapa se debe lograr un diagnostico completo y un plan de acción que identifique los objetivos y el alcance que guiaran la implementación de la Preparación Forense. Este plan de acción debe detallar además, como mínimo, acciones prioritarias, asignación, responsables y tiempo previsto para cada tarea, recursos asignados, etc. Dependiendo del tamaño de la organización este plan de acción puede ser para un sector de la misma o para su totalidad

2.3 Especificación de activos primarios

Los datos, la información, los procesos, los sistemas y servicios son activos fundamentales para una organización. Tienen requisitos de seguridad tales como confidencialidad, integridad y disponibilidad indispensables para mantener la continuidad del negocio, la rentabilidad, la competitividad y la reputación ante los usuarios/clientes, aspectos que son requeridos en el logro de los objetivos propios de la organización.
Hay varias metodologías que sirven de base para el análisis de riesgo y la identificación de activos, especialmente de los activos primarios que marcaran los requisitos de seguridad para los demás componentes del sistema.
Este análisis se inicia con un inventario de activos, información que puede tomarse de la etapa anterior de diagnóstico, lo cual servirá para diferenciar entre activos estratégicos, tácticos y operacionales. Los activos estratégicos son los servicios o productos que sustentan la capacidad competitiva de la organización, los activos tácticos los procesos involucrados para la correcta entrega de esos servicios o productos, y los activos operacionales aquellas actividades que se determinan como críticas en cada proceso.
El inventario también puede emplearse para conocer el estado de situación de infraestructura y las posibles adecuaciones necesarias con vista a la implementación de la Preparación Forense, sobre todo la infraestructura de almacenamiento requerida para dar soporte a la metodología preventiva.
De ser necesario se puede ajustar el plan de acción luego de seleccionados los activos primarios, con indicación de prioridades, datos a recolectar, tiempo de recolección y responsable asignado.
Es imprescindible comprender la operatoria, protocolos asociados, la estructura y demás características del activo seleccionado, porque ese conocimiento ayudará a detectar rápidamente un comportamiento sospechoso o anómalo.
Como resultado de esta etapa se contará con un conocimiento detallado de los activos y de los riesgos asociados a los mismos, la probabilidad de ocurrencia, el impacto y los controles que se deberán efectuar para su mitigación. Cada uno de los

riesgos identificados deberá estar relacionado con una o más de las dimensiones de seguridad informática establecidas como requisitos del sistema, lo cual permitirá establecer el nivel de riesgo y los controles específicos que correspondan.

2.4 Implementación

Definidos los activos primarios y efectuado el análisis de riesgo correspondiente, se puede iniciar con la etapa de implementación de Forensic Readiness.
Esta es una instancia más bien técnica donde, sobre los activos identificados, se iniciará la recolección de datos y el tratamiento de los mismos como evidencia digital.
Los procedimientos que se apliquen sobre los datos recolectados deben orientarse a resguardar la integridad de la evidencia y a asegurar la confiabilidad y la disponibilidad como requisitos a cumplir por parte del sistema de seguridad que comienza a funcionar.
Se reitera la importancia de mantener la cadena de custodia desde el inicio, para asegurar la plena admisibilidad como prueba legal de la evidencia. Esta cadena de custodia implica el registro detallado de cada paso dado con respecto a los datos, es decir, asegurar la trazabilidad de la información y mantener la integridad de los archivos con algoritmos de hash que producirán una huella digital unívoca para el conjunto de datos.
Por idénticos motivos deben documentarse las herramientas tecnológicas utilizadas tanto para recolectar como las aplicadas en el análisis de datos, las responsabilidades asignadas y las prioridades consideradas con respecto al resguardo de datos.
El valor temporal que la organización le otorgue a sus datos determinará las necesidades de infraestructura de almacenamiento para el registro centralizado de los datos considerados evidencia. Este repositorio debe recibir tratamiento con el rango de activo primario.
La aplicación de herramientas de forensia informática se realiza en esta etapa tanto para la vigilancia de incidentes como para el análisis de datos. Existen numerosas soluciones comerciales y open source que deberán ser cuidadosamente seleccionadas dependiendo de sus prestaciones, utilizando también una combinación de varias herramientas diferentes para lograr una mayor potencia y perfomance.
Las vulnerabilidades descubiertas deben ser reportadas al responsable designado de manera inmediata para su tratamiento, como así también deberá hacerlo cualquier persona de la organización que crea estar frente a un fallo de seguridad.
Como resultado de esta etapa se obtendrán procedimientos detallados de la implementación de Forensic Readiness, incluyendo descripción de herramientas empleadas, formularios que registren cada instancia de la cadena de custodia y instrumentos de reporte de incidentes.

2.5 Seguimiento/Revisión

Se requiere un seguimiento activo de todo el proceso de la Preparación Forense para verificar su correcto funcionamiento y para detectar a tiempo errores o falencias que puedan ocurrir.
Es importante evaluar si las actividades desarrolladas se realizan conforme a lo previsto y la confidencialidad, integridad y disponibilidad de los datos se encuentra garantizada. Para esta evaluación se pueden construir indicadores de seguimiento que reflejen los resultados de eficiencia y efectividad de lo implementado y que ayuden a tomar decisiones al respecto, tales como: resultados de auditorías; resultados de análisis de intrusión; observaciones recibidas; informaciones de avance sobre acciones preventivas y correctivas; mediciones y actualización de vulnerabilidades entre otros.
Los cambios en la organización, en la tecnología y en las leyes aplicables pueden producir cambios en los objetivos de negocio, en las amenazas detectadas, en las oportunidades del entorno y en la efectividad de los controles implementados por lo que es conveniente la revisión periódica de los activos primarios y los riesgos que los afectan. Lo importante es que desde la Dirección se mantenga una actitud proactiva de vigilancia sobre el desarrollo de todas las actividades relacionadas, para asegurar los recursos requeridos y como mejora continua del proceso de Preparación Forense.

3 Conclusiones y trabajos futuros

En este artículo se ha presentado una propuesta de Guía de Buenas Prácticas para la implementación de Forensic Readiness en cualquier tipo de organización que quiera adoptar este enfoque para la protección de sus datos y como método de anticipación de incidentes de seguridad.
La característica de considerar a los datos como evidencia digital desde el momento de la recolección trae aparejados cambios operativos en el modo de trabajo y una variación en la forma de utilizar la información, por eso es adecuado contar con una guía básica para organizar la implementación.
Es un factor clave el compromiso de todas las personas de la organización, tanto para el cumplimiento de los estrictos requisitos que se proponen sobre los datos considerados evidencia como así también para la aplicación de las políticas de seguridad y el esquema de continuidad digital, cuestiones que están intrínsecamente ligadas a Forensic Readiness.
A futuro se podría avanzar con el análisis del grado de madurez necesario en una organización para adoptar este modelo de trabajo, como así también en el diseño de un framework que permita implementar Forensic Readiness en cualquier tipo de organización lo cual, además, puede ser una estrategia para incentivar la cultura de

la protección de datos y seguridad de la información tan demanda frente a la tendencia de crecimiento sostenido de los delitos informáticos.

Referencias

[1] TAN, John. (2001). Forensic Readiness. http://isis.poly.edu/kulesh/forensics/forensic_readiness.pdf

[2] Tugnarelli, M.; Fornaroli, M.; Santana, S.; Jacobo, E.; Díaz, F.J. Análisis de metodologías de recolección de datos digitales. Workshop de Investigadores en Ciencias de la Computación (WICC 2017). ISBN: 978-987-42-5143-5. http://sedici.unlp.edu.ar/handle/10915/61343

[3] Tugnarelli, M., Fornaroli,M. Santana,S. Jacobo, E. Díaz, J. Analysis of Methodologies of Digital Data Collection in Web Serves. Communications in Computer and Information Science (Springer), Vol. 790, Pag.265. (2018) https://link.springer.com/content/pdf/bfm%3A978-3-319-75214-3%2F1.pdf

[4] RFC 3227 Guidelines for Evidence Collection and Archiving. https://www.ietf.org/rfc/rfc3227.txt

[5] Guidelines for identification, collection, acquisition and preservation of digital evidence" ISO/IEC 27037:2012

[6] The National Archives. Managing digital continuity. http://www.nationalarchives.gov.uk/information-management/manage-information/policy-process/digital-continuity

[7] Pooe, A & Labuschagne, Les. A conceptual model for digital forensic readiness. (2012) Information Security for South Africa - Proceedings of the ISSA 2012 Conference. 1-8. 10.1109/ISSA.2012.6320452.

[8] Collie, Jan. A Strategic Model for Forensic Readiness. (2018). Athens Journal of Sciences. https://www.athensjournals.gr/sciences/2018-1-X-Y-Collie.pdf