Protocolo de Entrega al Correo Argentino de Artefactos Binarios del Sistema de Captura y Transmisión de Acta

Índice

1 Entrega al Correo Argentino de los Artefactos Binarios del Sistema de Captura y Transmisión de Actas 3
2 Requerimiento 4
3 Objetivos 5
4 Componentes o utilitarios a utilizar: 6
5 Proceso de fijación de la evidencia digital 7
5.1 Proceso de Recolección 7
5.2 Proceso de Cifrado y Firmado 7
5.3 Proceso de Almacenado 8
5.4 Proceso de Fijación de evidencia 8
5.5 Proceso de Aceptación y Resguardo 8
6 Proceso de auditoria posterior 9
6.1 Proceso de Extracción 9
6.2 Proceso de Validación de firmas 9
6.3 Proceso de Descifrado 9
6.4 Proceso de Despliegue y validación 10
6.5 Proceso de Auditoria 10
6.6 Proceso de emisión de informes 10
7 Anexo 11
7.1 Acta de Cadena de Custodia de Evidencia Digital 11

1 Entrega al Correo Argentino de los Artefactos Binarios del Sistema de Captura y Transmisión de Actas

Acto establecido para la entrega de los aplicativos desplegados durante los eventos electorales de Argentina y dar cumplimiento al requerimiento del (i) Pliego de Condiciones Particulares para el Servicio de Recuento Provisional de Resultados de fecha 20 de diciembre de 2018, y (ii) de las Especificaciones Técnicas para la licitación para la Transmisión de Imágenes de Actas de Escrutinio.

La cláusula 7.2.2. Entregables, del Pliego de Condiciones Particulares para el Servicio de Recuento Provisional de Resultados de fecha 20 de diciembre de 2018 prevé: *"(...) de conformidad con la normativa vigente deberá ponerse bajo resguardo de la Justicia Nacional Electoral una copia del software que se utilizará en cada jornada electoral (...)"*.

2 Requerimiento

Entrega por parte del Correo Argentino de los aplicativos desplegados para las Elecciones Primarias, Abiertas, Simultáneas y Obligatorias (en adelante, las "PASO") de la República Argentina. La entrega debe realizarse en el plazo de 96 (noventa y seis) horas previas del inicio del proceso electoral, con los recaudos correspondientes para proteger la propiedad intelectual y la integridad de los mismos, y acompañado del proceso de fijación de la evidencia digital y el proceso de auditoria posterior.

3 Objetivos

Smartmatic deber realizar lo siguiente:

1. Recolectar 96 (noventa y seis) horas antes del proceso, los artefactos binarios de los componentes del Sistema de Captura y Transmisión de Actas.
2. Entregar de manera cifrada los binarios firmados digitalmente junto al digerido criptográfico (HASH) de cada componente desplegado en las elecciones PASO
3. Facilitar auditorias posteriores y proveer todos los recaudos para preservar la propiedad intelectual, la integridad y autenticidad de los artefactos binarios correspondientes a los componentes desplegados del Sistema de Captura y Transmisión de Actas en el proceso electoral de las PASO.
4. Fijar en un acta de cadena de custodia de evidencia digital el digerido criptográfico (HASH) cada artefacto binario en conjunto con la identificación del medio de almacenamiento origen y el medio de almacenamiento destino.

4 Componentes o utilitarios a utilizar:

(i) El algoritmo de sumarización criptografica SHA-256 utilizando el aplicativo SHA256SUM para validar integridad de cada binarios

(ii) El algoritmo de firmas digitales RSA utilizando el aplicativo GPG para validar autenticidad.

(iii) La criptografía simétrica con AES 256 utilizando el aplicativo GPG para preservar la confidencialidad del código fuente y binarios.

(iv) Los comandos propios del Sistema Operativo /usr/bin/lshw para identificar los servidores donde se extraen los binarios del sistema desplegado.

(v) 2 (dos) pendrives como medio de almacenamiento externo y una laptop (laptop_recolección_evidencia) como medio de extracción, ejecución de scripts, almacenamiento intermedio, cálculo de digeridos criptográficos, cifrado y copia de entregables a discos de almacenamiento externo.

(vi) El utilitario Docker para extraer de los binarios utilizados en el ambiente de producción

(vii) Un acta de cadena de custodia de evidencia digital con el digerido criptográfico de cada uno de los archivos entregados firmada por la Dirección del Correo Argentino

Para cumplir los objetivos descritos se han creado 2 (dos) procesos.

(i) El primero es el proceso de fijación de la evidencia digital con todos los recaudos para preservar integridad, autenticidad y confidencialidad;

(ii) El segundo es el proceso de auditoría posterior.

Ambos procesos se describen a continuación.

5 Proceso de fijación de la evidencia digital

El proceso de fijación de evidencia digital es un protocolo que prevé la recolección 96 (noventa y seis) horas antes de un proceso los artefactos binarios de los componentes desplegados para la automatización de un proceso.

El protocolo de fijación de la evidencia tiene como objetivo generar toda la evidencia necesaria para facilitar procesos de auditoria posteriores.

Para garantizar la integridad de la evidencia recolectada y la autenticidad, se utilizarán utilitarios que permitirán obtener los digendos criptográficos, cifrar y firmar digitalmente la evidencia recolectada, además de identificar la evidencia, el origen de la misma, para finalmente tener todos los insumos para fijar la evidencia en un acta de cadena de custodia de evidencia digital firmada por los responsables de Smartmatic y el Correo Argentino como ente a cargo de la solución y la firma del ente receptor como ente garante de la custodia de la evidencia digital fijada.

El proceso de fijación de evidencia digital establece y describe los procesos de recolección, cifrado, firma, almacenamiento, fijación de evidencia y resguardo, así como los procedimientos a seguir para la ejecución de cada proceso

5.1 Proceso de Recolección

El proceso de recolección consiste en recolectar todos los artefactos binarios del Sistema de Captura y Transmisión. Para la recolección se debe seguir el siguiente procedimiento:

Procedimiento de Recolección

En el pendrive se deberá cargar los scripts de extracción previamente validados por el Correo Argentino.

1. Conectar el pendrive a la laptop_recolección_evidencia
2. Crear la carpeta en /home/usuario_auditoria/binarios
3. Descargar en /home/usuario_auditoria/binarios los binarios de los componentes desplegados para las elecciones PASO utilizando el script extracción

5.2 Proceso de Cifrado y Firmado

1. Ejecutar los utilitarios para cifrar y luego firmar los entregables

5.3 Proceso de Almacenado

1. Copiar los binarios cifrados en el disco de almacenamiento externo junto a sus firmas digitales y digerido criptográfico

5.4 Proceso de Fijación de evidencia

1. Abrir el archivo Acta de cadena de custodia
2. En la sección de Artefactos recolectados se deberá describir el artefacto recolectado junto a su digerido criptográfico
3. Imprimir acta de cadena de custodia.
4. Firmar con la firma manuscrita de cada responsable de la fijación de la evidencia y los aprobadores del contenido del acta de cadena de custodia de evidencia digital

5.5 Proceso de Aceptación y Resguardo

El proceso de aceptación y resguardo es ejecutado por el ente receptor de la evidencia digital, de manera corroborar que los artefactos recibidos corresponden con los artefactos descritos en el acta de cadena de custodia.

1. Firmar con la firma manuscrita del responsable de la recepción de la evidencia.
2. Almacenar acta de cadena de custodia y medio de almacenamiento con los artefactos en el sobre dispuesto para el resguardo de la evidencia.

6 Proceso de auditoria posterior

La auditoría posterior es el protocolo diseñado para auditar los artefactos binarios de los componentes desplegados para la automatización de un proceso.

El protocolo de auditoria posterior tiene como objetivo validar la integridad y autenticidad de los binarios resguardados generados por el proceso de fijación de evidencia digital y compararlos con los binarios a fin comparar la autenticidad e integridad de ambos artefactos.

Una vez validada la autenticidad e integridad de los artefactos, se ejecutarán las auditorias correspondientes.

El proceso de auditoria posterior establece y describe los procesos de extracción, validación de firmas, descifrado, despliegue, comparación de ambientes, auditoria y emisión de informe.

6.1 Proceso de Extracción

El proceso de extracción consiste en abrir los sobres de resguardo del acta de cadena de custodia de evidencia digital y el disco de almacenamiento externo.

Revisar los datos de identificación del disco de almacenamiento externo.

Conectar el disco de almacenamiento externo en la máquina dispuesta para el proceso de validación de integridad y montarlo como dispositivo de solo lectura en el directorio /mnt/USB_Evidencia.

Validar que la llave pública coincide con la llave pública indicada en el Acta de cadena de custodia.

6.2 Proceso de Validación de firmas

Validar las firmas de los artefactos firmados en el dispositivo con la llave pública fijada en el acta de cadena de custodia

Calcular los digeridos criptográficos con SHA256SUM de todos los artefactos y comparar con los registrados en el acta de cadena de custodia.

6.3 Proceso de Descifrado

Descifrar los artefactos cifrados identificados en el acta de cadena de custodia de evidencia digital utilizando el utilitario GPG #gpg -o file.txt.gpg –symmetric –cipher-algo AES256 file.txt

Colocar los primeros 16 (dieciséis) caracteres Smartmatic y los segundos 16 (dieciséis) caracteres del Correo Argentino

6.4 Proceso de Despliegue y validación

Cargar los artefactos binarios en la máquina dispuesta para la auditoria ejecutando el comando.

Validar los binarios extraidos y los binarios desplegados.

6.5 Proceso de Auditoria

Este proceso es realizado por entes externos al Correo Argentino a fin de corroborar la integridad y funcionalidades del sistema.

6.6 Proceso de emisión de informes

El proceso de auditoria debe generar un informe detallando los hallazgos y recomendaciones, posterior a la auditoria se debe resguardar nuevamente siguiendo el proceso de fijación de evidencia descrito en la sección anterior.

7 Anexo

7.1 Acta de Cadena de Custodia de Evidencia Digital

Acta de cadena de custodia de evidencia digital
Elecciones PASO Agosto 2019

Lugar y Fecha:	Buenos Aires, 07 de Agosto de 2019	Hora:	

DESCRIPCIÓN DE LA EVIDENCIA DIGITAL

El presente documento contiene los artefactos binarios recolectados de la solución electoral desplegada para las elecciones PASO, ubicados en el centro de datos del correo Argentino en Monte Grande accesado desde Barracas

DATOS DE LOS RECOLECTORES

NOMBRE Y APELLIDO	DNI/Pasaporte	CARGO
Jerry Rondon		Especialista Infraestructura Smartmatic
Juan Osio		Especialista Infraestructura Smartmatic

ARTEFACTOS RECOLECTADOS

Componente Relacionado	Nombre del Archivo	HASH	Ubicación Destino: Nombre/Serial
SDT	Smartmatic.SDT.1.exe	5e806e851271c3f9a50ba8b1fe0a69a1c0c5954759788d81ca5851fb9293f939	Pendrive CAP1 - Marca: SanDisk - Capacidad: 32GB - Serial: 0401aec9768e6c55491d998b5dfbaeb3d221cd38061c5ce150cf09556a6f10056db3000000000000000000000c81be7e001d7a18915581076a272a33
	Smartmatic.SDT.23.exe	82335e5dcaed49ca67fcea008a7932c10692f77e069bae487cdb989b56834161	
	SDT_1.0.23-1.0.22.zip	0f750a14daea75680d6b2f2af6e4be751760d03c5106217d9d7bc881e83b7bca	
RCL	rcl.war	611b4a9d58201d6c6b3173d8906b282f95f63ac474bf68463f71491a6138991e	
Listado de HASH	listado_hash_cnt1.txt	f3aa0e70f743b48ec227d616460ba2a8ef6ba02db5a66031f67452c5abe4e349	

Herramientas utilizadas para la recolección

Nombre	Versión	Función
SHA256SUM	8.28	Cálculo de digerido criptográfico SHA256
GPG	2.2.4	Cifrado y Firmado de artefactos
lshw	B.02.18	Utilitario Linux para obtener información del hardware
BASH	4.4.19	Utilitario Linux para la ejecución de instrucciones del sistema operativo

Aprobado por:	Entidad	Fecha:	Firma
Andrés Rombolá	Smartmatic	07/08/2019	

Recibido por:	Entidad	Fecha:	Firma
Esteban Di Sibio	Correo Argentino	07/08/2019	