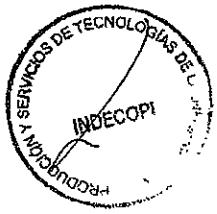
COMISIÓN DE DEFENSA DE LA LIBRE COMPETENCIA

INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE "SOFTWARE PARA ANÁLISIS FORENSE"

16 DE AGOSTO DE 2017

CONTENIDO



1. **NOMBRE DEL ÁREA**
Secretaría Técnica de la Comisión de Defensa de la Libre Competencia (en adelante, la Secretaría Técnica)

2. **RESPONSABLE DE LA EVALUACIÓN – CARGO**

Anthony Ramos Ramírez - Profesional en Ingeniería de Sistemas del Laboratorio Forense de la Secretaría Técnica.

3. **FECHA**
16 de Agosto de 2017

4. **ASUNTO**
Evaluación de software para análisis forense.

5. **ANTECEDENTES**

El presente informe se ha elaborado sobre la base del Decreto Supremo 024-2006-PCM, Reglamento de la Ley 28612 – Ley que norma el uso, adquisición y adecuación del software en la Administración Pública.

Mediante Memorando 041-2017/ST-CLC-INDECOPI del 2 de febrero de 2017, la Secretaría Técnica solicitó a la Gerencia General la adquisición de un programa informático (software) para el análisis forense de cantidades masivas de datos en alta velocidad.

6. **JUSTIFICACIÓN**

Mediante Ley de Represión de Conductas Anticompetitivas, aprobada por Decreto Legislativo 1034 y modificada por Decreto Legislativo 1205, se facultó a la Secretaría Técnica, según el numeral 15.3 literal c), a realizar visitas de inspección sorpresa en los locales de los agentes económicos[1]. En estos actos de inspección se suele tomar copia de cuantiosa información digital o electrónica, la cual es procesada posteriormente con la finalidad de realizar un análisis profundo e investigar prácticas anticompetitivas entre los agentes investigados.

Estas visitas de inspección se realizan simultáneamente, en promedio, a cuatro (4) agentes económicos en un día; y, por cada agente económico se inspecciona, en promedio, diez (10) ordenadores (computadora o laptop). De esta manera, la Secretaría Técnica inspecciona y recaba información, en promedio, de cuarenta (40) ordenadores en una visita de inspección, teniendo un promedio de 50 GB de información digital (entre correos electrónicos y archivos ofimáticos diversos) y un promedio de hasta 500 GB en los casos de copiado total de discos duros, por cada ordenador. De esta manera, el volumen de la información influye en el tiempo de procesamiento, factor directamente vinculado en la labor de detección de conductas anticompetitivas.

Asimismo, considerando que la información a recabar se encuentra vinculada con acciones de naturaleza ilegal, los agentes económicos suelen mantenerla en secreto y fuera del alcance regular de las autoridades, por ejemplo, mediante la eliminación de los registros de las computadoras, afectando el estado de los archivos recabados, factor relevante que influye sobre el tiempo de procesamiento. En efecto, la recuperación de la información

[1] **Ley de Represión de Conductas Anticompetitivas, aprobada mediante Decreto Legislativo 1034 y modificada por Decreto Legislativo 1205**
Artículo 15.- La Secretaría Técnica.-
15.3. Para el desarrollo de sus investigaciones, la Secretaría Técnica se encuentra facultada para:
(c) Realizar inspecciones, con o sin previa notificación, en los locales de las personas naturales o jurídicas, sociedades irregulares y patrimonios autónomos y examinar los libros, registros, documentación y bienes, pudiendo comprobar el desarrollo de procesos productivos y tomar la declaración de las personas que en ellos se encuentren. En el acto de la inspección podrá tomarse copia de los archivos físicos, magnéticos o electrónicos, así como de cualquier documento que se estime pertinente o tomar las fotografías o filmaciones que se estimen necesarias. Para ingresar podrá solicitarse el apoyo de la fuerza pública.
(...)

eliminada demanda un mayor tiempo (quince veces más) respecto del procesamiento usual, debido a que la ejecución se inicia primero con restituir el archivo a su formato original y seguidamente visualizarlo para su lectura.

De otro lado, el artículo 237-A de la Ley del Procedimiento Administrativo General (LPAG) introduce la regla de la caducidad de los procedimientos administrativos sancionadores, a efectos de que se archive de oficio toda actuación generada a partir de la imputación de cargos una vez cumplido el plazo legal sin que se haya emitido la decisión final en primera instancia administrativa. Adicionalmente, se señala que, una vez caducado, el plazo transcurrido durante la tramitación del procedimiento administrativo sancionador deberá ser computado dentro del plazo de prescripción de la infracción. Esta situación genera una gran preocupación a la Secretaría Técnica pues de no emitirse un pronunciamiento final dentro del plazo legal, deberá declararse de oficio la caducidad del procedimiento.

Para la aplicación de la caducidad prevista en el artículo 237-A de la Ley del Procedimiento Administrativo General (LPAG), la quinta disposición complementaria transitoria del Decreto Legislativo 1272, establece que los procedimientos administrativos sancionadores en trámite deben adecuarse en un plazo de un (1) año, contado desde la vigencia de la referida norma.

En ese sentido, es importante contar con una herramienta para el análisis forense de una gran cantidad de datos en un tiempo reducido, a fin de resolver los procedimientos sancionadores dentro de los plazos legales y evitar su caducidad.

7. ALTERNATIVAS

Entre las alternativas a evaluar se encuentran:

- Guidance Software: EnCase Forensic
- Nuix Investigation and Response

No se encontró alternativa en software libre[2].

8. ANÁLISIS COMPARATIVO TÉCNICO

El análisis comparativo técnico está basado en la metodología establecida en la Guía Técnica sobre Evaluación de Software para la Administración Pública, aprobada por Resolución Ministerial Nº 139-2004-PCM.

8.1. Propósito de la evaluación

REQUERIMIENTO ☒ TICKET Nº: Nro Ticket MONITOREO ☐

Producto final:

- Seleccionar un producto entre productos alternativos.
- Decidir cuándo mejorar o reemplazar un producto.

8.2. Tipo de producto

Software especializado para el análisis forense de información.

8.3. Modelo de Calidad

Se aplica el modelo establecido en la Guía Técnica sobre Evaluación de Software para la Administración Pública (R.M. Nº 139-2004-PCM).

8.4. Selección de métricas

La selección de métricas se obtuvo a partir de los atributos especificados en el Modelo de Calidad.

---

[2] El software libre comparado se obtiene de lo registrado en la página http://www.softwarepublico.gob.pe/ provista por la Oficina Nacional de Gobierno Electrónico e Informática – ONGEI.

8.5. Niveles/Escalas para las métricas

Cumplimiento de requerimientos

NIVEL DE CUMPLIMIENTO	VALOR
No	1
Poco	2
Medianamente	3
Casi todos	4
Completamente	5

Pesos

REQUERIMIENTO	PESO
Deseable	1
Necesario	2
Indispensable	3

8.6. Criterios de valoración

Los Atributos Internos, los Atributos Externos y la Calidad en Uso serán especificadas por el área solicitante.

8.7. Toma de medidas

Para la medición, las métricas seleccionadas se aplican al producto de software. Los resultados son valores expresados en las escalas de las métricas ya definidos.

- Puntaje máximo a obtener: 390

8.8. Comparación de criterios de calidad

a) A continuación, se presenta la evaluación de los atributos internos, atributos externos y la calidad en uso de las alternativas mencionadas:

ATRIBUTOS INTERNOS

				Valor		Puntaje	
	Valor	Peso	Puntaje Máx.	EnCase	Nuix	EnCase	Nuix
Funcionalidad. Compatibilidad e integración con Windows [3] 7 Professional - 32 y 64 bits.	5	3	15	5	5	15	15
Interoperabilidad. Reportes compatibles con Microsoft Office[4] 2003, 2007, 2010, 2016	5	3	15	5	5	15	15
Fiabilidad. Puede funcionar ininterrumpidamente (24x7)	5	3	15	5	5	15	15
Usabilidad. Interfaz gráfica intuitiva, con disponibilidad de manual de instalación y configuración.	5	2	10	5	5	10	10
Aprendizaje. Tutorial incluido en la aplicación o disponible para descarga.	5	2	10	5	5	10	10
Eficiencia. Requisitos mínimos de funcionamiento: Dual Core 2.4GHz, 8GB Ram, 1TB HD.	5	3	15	5	5	15	15
Comportamiento de tiempos. Proveer tiempos adecuados de respuesta y procesamiento, y ratios de rendimiento	5	3	15	3	5	9	15

[3] Estandarizado mediante Resolución N° 201-2015-INDECOPI/GAF
[4] Estandarizado mediante Resolución N° 034-2016-INDECOPI/GAF

	Valor	Peso	Puntaje Máx.	Valor EnCase	Valor Nuix	Puntaje EnCase	Puntaje Nuix
Capacidad de mantenimiento. Opción de nuevas versiones, parches y actualizaciones.	5	2	10	5	5	10	10
Portabilidad. Capacidad de trasladado de un entorno a otro.	5	3	15	5	5	15	15
Coexistencia. Capacidad para coexistir con otros productos de software independientes dentro de un mismo entorno, compartiendo recursos comunes.	5	2	10	5	5	10	10

ATRIBUTOS EXTERNOS

	Valor	Peso	Puntaje Máx.	Valor EnCase	Valor Nuix	Puntaje EnCase	Puntaje Nuix
Compatibilidad con 32 y 64 bits	5	3	15	5	5	15	15
Interface con múltiples ventanas de búsqueda	5	3	15	1	4	3	12
Interface con ventana de detalle de procesamiento	5	3	15	4	4	12	12
Sistemas de archivo soportados: - FAT32 - NTFS - EXT2 - EXT3	5	3	15	5	5	15	15
Formatos forenses soportados: - E01 - L01 - AD1 - DD - VHD - XRY - UFD o UFDR	5	3	15	4	5	12	15
Tipos de archivos - Correos (pst, ost, msg, nsf, dbx, mbox, eml) - Documentos (doc, docx, xls, xlsx, ppt, pptx, html, pdf) - Imagen (png, jpg, jpeg, tiff, bmp, gif) - Compresión (zip, rar, tar) - Otros (iso, xml, vhd)	5	3	15	5	5	15	15
Procesamiento masivo de grandes volúmenes de datos a alta velocidad	5	3	15	2	5	6	15
Visualización detallada de estado de procesamiento	5	2	10	3	5	6	10
Recuperación de archivos borrados o eliminados	5	3	15	5	5	15	15
Exportar archivos, carpetas y correos a PDF, MSG, EML y adjuntos	5	3	15	5	5	15	15
Visualizaciones gráficas - Lista de archivos - Forma cronológica o línea de tiempo - Agrupación por dominio - Mapa de eventos - Diagrama de red	5	2	10	3	5	6	10
Identificación de datos duplicados	5	3	15	3	5	9	15

				Valor		Puntaje	
	Valor	Peso	Puntaje Máx.	EnCase	Nuix	EnCase	Nuix
Opción de agregar nuevas funcionalidades y automatización mediante codificación (scripting)	5	1	5	5	5	5	5
Reportes - Estadísticas de tipos de archivos analizados - Lista de palabras identificadas (indexadas) - Lista de direcciones electrónicas	5	2	10	3	4	6	8
Soporte y mantenimiento	5	3	15	5	5	15	15

CALIDAD EN USO

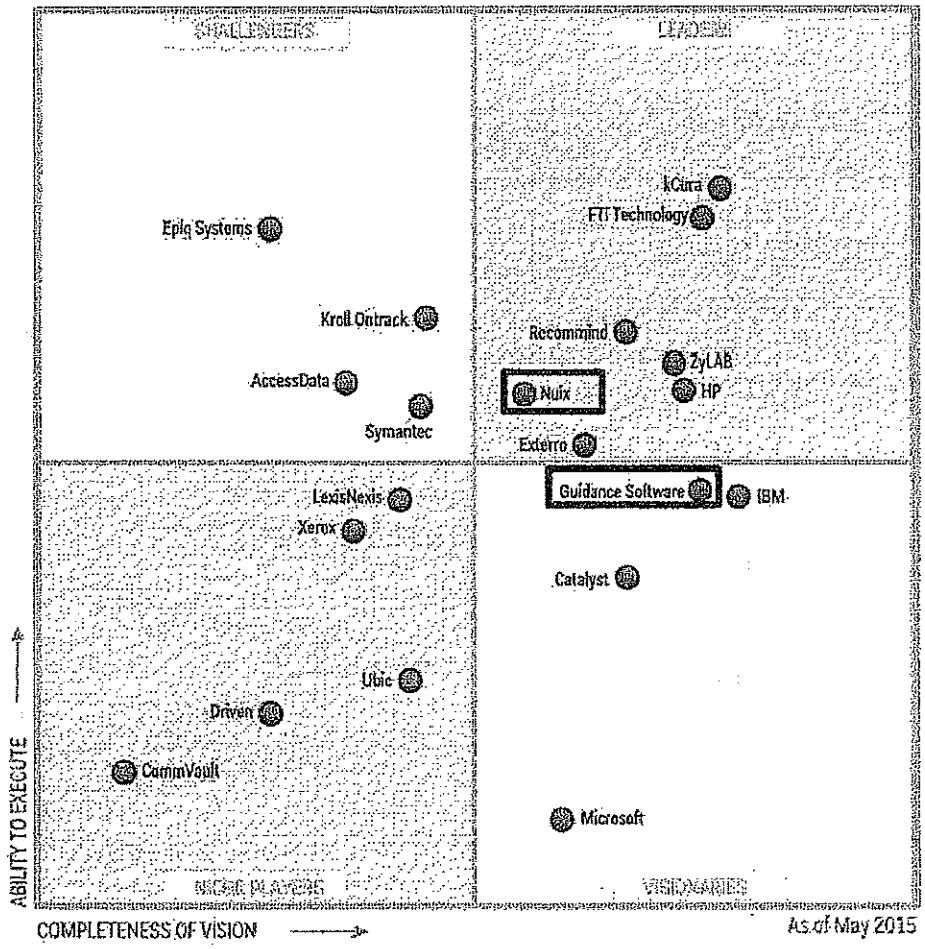
				Valor		Puntaje	
	Valor	Peso	Puntaje Máx.	EnCase	Nuix	EnCase	Nuix
CALIDAD EN USO							
Eficacia	5	3	15	5	5	15	15
Productividad	5	3	15	3	4	9	12
Seguridad	5	3	15	5	5	15	15
Satisfacción	5	3	15	4	5	12	15

PUNTAJE FINAL

	Puntaje Total	
Puntaje Máx.	EnCase	Nuix
390	330	379
100%	85%	97%

b) A continuación, se presenta un gráfico de posicionamiento en el mercado:

Figure 1. Magic Quadrant for E-Discovery Software



Fuente: Gartner, Mayo de 2015

En el gráfico se observa que el fabricante Nuix está posicionado en el cuadrante[5] de líderes, superando a Guidance Software, donde se han evaluado cuatro características importantes:

- Funcionalidad y características acordes con las buenas prácticas.
- Modelo de negocio enfocado en el desarrollo de software, lo que garantizaría una mejora constante (mantenimiento) y soporte para el software.
- Usabilidad, al contar con firmas de abogados entre su cartera de clientes, lo que demostraría la aceptación del producto sobre todo en el mercado para el que fue diseñado.
- Respaldo financiero y perspectiva de crecimiento.

c) Adicionalmente se presentan los resultados de un informe comparativo de software forense comercial[6], que mide las capacidades de procesamiento de grandes volúmenes de datos, realizado por los especialistas Knut Kröger y Reiner

[5] Cuadrantes mágicos Gartner http://www.mercadeo.com/blog/2010/01/cuadrantes-magicos-gartner/

[6] Para la elaboración del informe se realizaron cuatro pruebas usando diferentes escenarios (tipo de archivo de evidencia y tamaño) en un mismo equipo de cómputo, es decir, cada software evaluado tuvo las mismas condiciones de hardware para el procesamiento en cada escenario de prueba.

Creutzburg, del Departamento de Informática y Medios de la Universidad Brandenburg de Ciencias Aplicadas[7], de Alemania.

Forensic image	Nuix 4.2	Guidance Encase Forensic 7	AccessData FTK 4.2	X-Ways Forensics 16.9
Windows 7 image E01 89 GB	1,06 hours	10,5 hours	4,29 hours	5,04 hours
Mac OS X 10.8.2 E01 133 GB	3,17 hours	16,4 hours	5,43 hours	5,44 hours
Outlook pst file 101 MB	9 seconds	16 seconds	7 seconds	8 seconds
Windows 001 image 125 MB	3 seconds	4 seconds	5 seconds	3 seconds

Fuente: Brandenburg University of Applied Sciences

En el recuadro se puede apreciar que, en todas las pruebas el software Nuix obtiene un mejor tiempo de respuesta en el procesamiento de la información, frente a las demás alternativas, llegando a ser hasta un 90% más rápido que EnCase Forensic. Esto se debe a que Nuix cuenta con un motor de procesamiento paralelo patentado, lo que le permite procesar datos a nivel binario, indexando grandes volúmenes de datos en poco tiempo.

Cabe precisar que, considerando que el tamaño de los archivos que procesa la Secretaría Técnica es similar al usado en las pruebas realizadas, los resultados obtenidos del Nuix resultan ser representativos y guardan correspondencia con la necesidad requerida actualmente en el laboratorio forense.

9. EVALUACIÓN DE RIESGOS

Para la evaluación de riesgos se ha aplicado el Procedimiento de Evaluación y Tratamiento de Riesgos[8] y la Guía de Amenazas y Vulnerabilidades[9] del Sistema de Gestión de Seguridad de la Información – SGSI del INDECOPI.

Las marcas de software de que se están comparando cumplen con los estándares de desarrollo del ciclo de vida del software, lo que garantiza productos maduros y estables, minimizando considerablemente las amenazas y vulnerabilidades ocasionadas por software.

7 "A practical overview and comparison of certain commercial forensic software tools for processing large-scale digital investigations" - Knut Kröger and Reiner Creutzburg, Brandenburg University of Applied Sciences (http://docplayer.net/docview/53/31421465/#file=/storage/53/31421465/31421465.pdf)

8 Ver https://www.indecopi.gob.pe/documents/474320/626167/PG-SIG-03.pdf

9 Ver https://www.indecopi.gob.pe/documents/474320/626469/SGSI-GU-001.pdf

ANÁLISIS DE ENCASE FORENSIC

IDENTIFICACIÓN			ANÁLISIS										ESTIMACIÓN				
Activo			Amenaza		Vulnerabilidad		Consecuencia / Riesgo		Pilares de Seguridad								
Nº	Nombre del Activo	Tipo de Activo	Código	Descripción	Código	Descripción	Código	Descripción	Confidencialidad	Integridad	Disponibilidad	GRADO DE AFECCION	PROBABILIDAD	IMPACTO	RESULTADO = P * I	TOLERANCIA	COMENTARIOS
1	EnCase	Activo de Software	AME-033	Procesamiento ilegal de datos	VUL-042	Uso impropio / no controlado	-	Procesamiento ilegal de datos por Uso impropio / no controlado	3	4	4	3			3	MO	Mitigar, asumir, evitar, compartir o transferir el riesgo
			AME-038	Accesos no autorizados al sistema	VUL-039	Control de acceso inadecuado	-	Accesos no autorizados al sistema por Control de acceso inadecuado	3	4	4	3	2		6	IM	Mitigar, evitar, compartir o transferir el riesgo
			AME-048	Ruptura de la mantenibilidad del sistema de información	VUL-061	Falta de conciencia de los fabricantes de actualizaciones	-	Ruptura de la mantenibilidad del sistema de información por Falta de conciencia de los fabricantes de actualizaciones	3	4	4	3			1	TR	Asumir el riesgo
			AME-046	Saturación del sistema de información	VUL-104	Falta de mecanismos de monitoreo	-	Saturación del sistema de información por Falta de mecanismos de monitoreo	3	4	4	3	2	2	4	MO	Mitigar, asumir, evitar, compartir o transferir el riesgo

ANÁLISIS DE NUIX INVESTIGATION AND RESPONSE

IDENTIFICACIÓN			ANÁLISIS										ESTIMACIÓN				
Activo			Amenaza		Vulnerabilidad		Consecuencia / Riesgo		Pilares de Seguridad								
N°	Nombre del Activo	Tipo de Activo	Código	Descripción	Código	Descripción	Código	Descripción	Confidencialidad	Integridad	Disponibilidad	GRADO DE AFECCIÓN	PROBABILIDAD	IMPACTO	RESULTADO = P.I.	TOLERANCIA	COMENTARIOS
2	Nuix	Activo de Software	AME-033	Procesamiento ilegal de datos	VUL-042	Uso impropio / no controlado	-	Procesamiento ilegal de datos por Uso impropio / no controlado	3	4	4	3			3	MO	Mitigar, asumir, evitar, compartir o transferir el riesgo
			AME-038	Accesos no autorizados al sistema	VUL-039	Control de acceso inadecuado	-	Accesos no autorizados al sistema por Control de acceso inadecuado	3	4	4	3	2	3	6	IM	Mitigar, evitar, compartir o transferir el riesgo
			AME-048	Ruptura de la mantenibilidad del sistema de información	VUL-061	Falta de conciencia de los fabricantes de actualizaciones	-	Ruptura de la mantenibilidad del sistema de información por Falta de conciencia de los fabricantes de actualizaciones	3	4	4	3			1	TR	Asumir el riesgo
			AME-046	Saturación del sistema de información	VUL-104	Falta de mecanismos de monitoreo	-	Saturación del sistema de información por Falta de mecanismos de monitoreo	3	4	4	3	2	2	4	MO	Mitigar, asumir, evitar, compartir o transferir el riesgo

10. ANÁLISIS COMPARATIVO DE COSTO BENEFICIO

A continuación, se presenta el análisis de costo beneficio de las dos herramientas en evaluación:

CONCEPTO	Cant.	EnCase	Nuix
		Monto en S/. Inc IGV	Monto en S/. Inc IGV
Licenciamiento	1	12,616.95	15,484.44
Soporte y mantenimiento (anual)	3	6,193.78	11,927.49
TOTAL		**18,810.72**	**27,411.93**

Los montos están expresados es Soles e incluyen el IGV (T.C. S/ 3.2401[10] al 20/07/2017).

Del comparativo se observa que los costos asociados a EnCase Forensic son menores a los costos de Nuix Investigation and Response.

11. CONCLUSIONES

- Para poder cumplir con la necesidad que tiene el área, vinculado a la gran cantidad de datos que se requiere procesar en un reducido tiempo y considerando los cambios normativos respecto a los plazos legales de los procedimientos administrativos sancionadores, se identificaron dos posibles alternativas de software: EnCase Forensic del fabricante Guidance Software y Nuix Investigation and Response del fabricante Nuix. De estas alternativas evaluadas, el software Nuix cubrió en mayor porcentaje los requerimientos establecidos en los criterios de calidad.
- En cuanto al posicionamiento en el mercado, la empresa Nuix aparece como líder en el rubro de software forense, superior a Guidance Software, alineando las funcionalidades a las buenas prácticas y estándares internacionales, garantizando una mejora continua en el desarrollo de software reflejado en el mantenimiento y soporte de sus productos y, teniendo entre sus clientes a importantes entidades de gobierno e instituciones legales.
- En las pruebas de laboratorio a las que fueron sometidos ambos productos, donde se evaluó el rendimiento (tiempo de respuesta) de las computadoras durante el análisis de evidencia, Nuix Investigation and Response del fabricante Nuix, demostró un procesamiento más rápido, superando a EnCase Forensic en cada uno de los 4 escenarios, llegando a ser hasta un 90% más rápido.
- Las pruebas de laboratorio mostraron también que, Nuix Investigation and Response presenta funcionalidades adicionales como filtros avanzados y opciones gráficas de visualización de gran cantidad de información, destacándose de las demás herramientas evaluadas. Estas funcionalidades mejoran las actividades de análisis de la información disminuyendo el tiempo de revisión de los casos.
- Finalmente, según el análisis comparativo de costo beneficio, EnCase Forensic requiere menor inversión que Nuix Investigation and Response en la adquisición de la licencia y el soporte y mantenimiento anual; sin embargo, para la necesidad requerida de la Secretaría Técnica, la velocidad de procesamiento demostrada por Nuix Investigation and Response, evidencia un ahorro considerable en el tiempo de procesamiento y análisis de la información.

[10] SBS http://www.sbs.gob.pe/app/stats/tc-cv.asp

12. FIRMAS

ELABORADO POR: Anthony Ramos Ramírez Profesional en Ingeniería de Sistemas	REVISADO POR: Enith Matías Ejecutivo 1 de GTI Sofía Castillo Especialista 2 de GTI	APROBADO POR: Jesús Espinoza Secretario Técnico CLC Hernán Urrutia Gerente de TI (e)
FIRMA:	FIRMA:	FIRMA: