EVALUACION DEL PROCEDIMIENTO RESPALDO GENERAL DE INFORMACIÓN.

1. INTRODUCCIÓN

1.1 Origen.

El informe se desarrolla en cumplimiento del ejercicio de esta unidad, el marco normativo vigente relativo a control interno, administración de riesgo, gestión de las Tecnologías de Información y al Plan Estratégico de esta Auditoría Interna.

1.2. Aspectos objeto de estudio.

Comprobar el cumplimiento de la normativa relativa a control interno y gestión de las Tecnologías en el proceso denominado “Respaldo General de Información”.

1.3 Alcance.

Los periodos comprendidos entre 1° de enero de 2018 al 31 de diciembre del 2019, ampliándose en aquellos casos en que se consideró necesario.

El trabajo se realizó con sujeción al Manual de Normas generales de control interno para la Contraloría General de la República y las entidades y órganos sujetos a su fiscalización.

1.4 Exposición a la administración.

Según consta en el acta No. AI-001-2020 del veinte de febrero del año en curso, se presentan los resultados del presente estudio, al Director General y jefatura de la Unidad de Tecnologías de Información, ambos de este Instituto.

1.5 Marco de referencia

- Ley No. 8292 General de Control Interno.
- Ley No. 8204 sobre Estupefacientes, sustancias psicotrópicas, drogas de uso no autorizado, financiamiento al terrorismo, legitimación de capitales y actividades conexas y sus reformas.

- Manual de Normas de Control Interno para las entidades sujetas a las disposiciones de la Contraloría General de la República.
- Manual de Normas para el ejercicio de la Auditoría Interna promulgado por la Contraloría General de la República.
- Manual Técnico de Normas para las Tecnologías de Información de la Contraloría General de la República.
- COBIT 5 Marco referencial.

1.6 Limitación al alcance.

Carencia de contar con un Auditor de Sistemas en la unidad de Auditoría.

1.7 Generalidades.

El estudio responde a la necesidad de evaluar el estado actual de los procesos de la Unidad de Tecnologías de Información, con el fin de determinar el cumplimiento de los criterios básicos de control que deben observarse en la gestión de las tecnologías de conformidad con las “Normas Técnicas para la Gestión y el Control de las Tecnologías de Información” emitidas por la Contraloría General de la República Resolución R-CO-26-2007.

El presente informe contiene los resultados de la evaluación del procedimiento denominado “Respaldo General de Información”, enfocado en la seguridad física de la información que se genera en el Instituto Costarricense sobre Drogas (ICD) como parte de la ejecución de los alcances del Plan Anual de Trabajo de la Auditoría Interna para el presente periodo.

Incluye un apartado denominado resultados con la descripción de un conjunto de oportunidades de mejora determinadas que reflejan omisiones de control, igualmente contiene una conclusión general que expresa una opinión sobre la condición encontrada en los aspectos físicos del procedimiento objeto de estudio y por último menciona las recomendaciones que procuran orientar a la entidad para que subsane lo correspondiente en aras del fortalecimiento del Sistema de Control Interno, Sistema Específico de Valoración de Riesgo y Gestión Tecnológica.

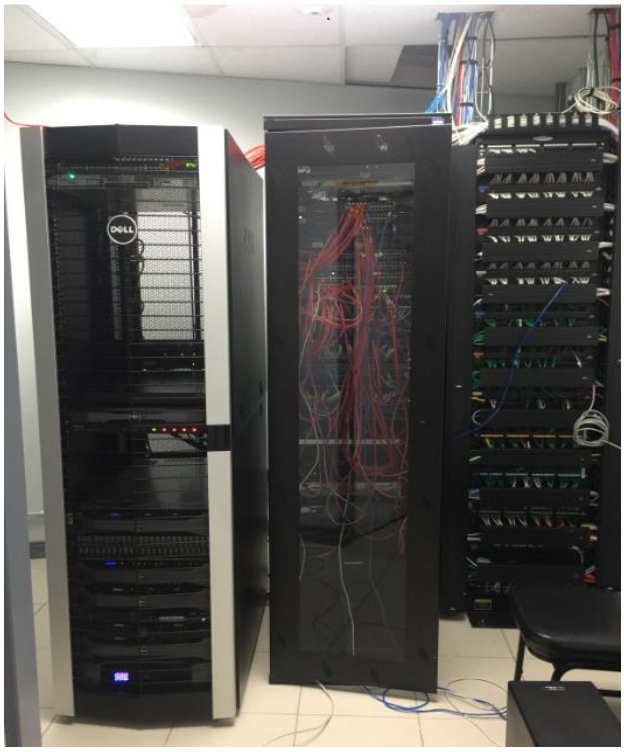
Parte de la responsabilidad de las Auditorías Internas es aportar valor agregado a las actividades de la administración activa, convirtiéndose en un órgano de advertencia, asesoramiento y garantía de que las actuaciones de los administrados se ejecutan en total apego al ordenamiento jurídico.

2. RESULTADOS.

2.1 Capacidad de espacio para respaldos de información.

Según el Manual de Procesos de TI, el objetivo del presente procedimiento es respaldar la información de los usuarios en un medio de almacenamiento persistente, para que pueda ser recuperada ante situaciones o interacciones excepcionales donde la integridad y consistencia se vea comprometida, haya supresión accidental o bien supresión malintencionada de los datos.

La unidad evaluada agrupa los equipos relativos a servidores, racks, switch, enrutadores, los cuales resguardan la información sensible en un área denominada cuarta de servidores ubicada en el segundo piso del edificio institucional, el cual cuenta con condiciones óptimas para albergar los equipos tecnológicos, situación que puede ser visualizado en las siguientes fotografías:



Dicho espacio comprende los servidores físicos y virtuales donde se almacena los datos que se generan de las unidades que conforman el ICD, detallándose de seguido:

Nombre	Tipo	Año adquirido	Sistema Operativo	Rol en la infraestructura
THANOS	Físico	2011	Windows server 2012 R2	Servidor de archivos institucionales
ARES	Físico	2014	Windows server 2012 R2	Servidor de archivos institucionales
GEA	Físico	2010	Windows server 2012 R2	Servidor de base de datos y archivos institucionales
ORION	Físico	2011	Windows server 2012 R2	Servidor de respaldos de datos institucionales
SAN	Físico	2016	EonOne	Sistema de almacenamiento
SEMX	Físico	2014	Windows server 2012 R2	Sistema de gestión de correo electrónico institucional
CENTAURUS	Virtual		Windows Server 2008 R2	Servidor de base de datos de sistemas institucionales
CODISA	Virtual		Windows Server 2003 R2	Servidor de base de datos Oracle para el sistema NAF
DB-SAB	Virtual		Windows Server 2008 R2	Servidor de base de datos de sistemas institucionales
DBA	Virtual		Windows Server 2008 R2	Servidor de base de datos de sistemas institucionales
GTE	Virtual		Windows Sister 2000	Sistema para generación de archivos de transferencias presupuestarias
NAF	Virtual		Windows Sister 2003 R2	Sistema administrativo contable utilizado por la UAFC, utiliza CODISA.

Del cuadro anterior se desprende que TI cuenta con un total de doce servidores de los cuales el 50% refiere a servidores virtuales y el otro 50% a servidores físicos, adquiridos entre los años 2011 y 2017, el servidor de respaldos de datos institucionales llamado Orión tiene una capacidad de 35000 GB.

Los respaldos de la información contenida en bases de datos de producción se ejecutan de forma automática y diaria, los archivos generados motivo del proceso de respaldo se almacenan en el mismo servidor donde se encuentran los ambientes de producción, sin embargo, existe una limitación en la capacidad de espacio, de tal forma que de presentarse alguna situación especial, según el jefe de TI, *"se perdería un día de información generada"*, opinión dada en entrevista formulada por esta auditoría y respaldada mediante el Acta de entrevista AI-044-2019 del pasado 11 de diciembre 2019.

Según el criterio[1] técnico de la jefatura de la unidad de Tecnologías de Información, la capacidad del servidor de respaldos de información debe ser el doble de la actual, 70.000 GB, para que permita establecer una política de respaldos y recuperación adecuada.

De lo anterior, se determina en el proceso objeto de evaluación que la capacidad de espacio para los respaldos de la información institucional es limitada,

[1] Correo electrónico 5 febrero 2020.

pues no se cuenta con un número de servidores suficiente para almacenar la información que manejan las unidades del ICD, pues solo se cuenta con un servidor, siendo un riesgo vulnerable en el almacenamiento de datos.

En relación con el almacenamiento de información que resguarda el servidor actual, afirma el jefe de TI mediante el Acta No. AI-044-2019 del 11 de diciembre de 2019 lo siguiente:

> "Toda la información que se almacena en las carpetas de cada uno de los funcionarios y las carpetas de red que se almacena en cada una de las unidades institucionales, solamente no se contempla la carpeta "publico" y la carpeta "temporal.".

Actualmente se mantiene un respaldo de la información de la Institución, custodiado en un lugar externo a ésta[2], no obstante, las cintas de respaldo se envían una vez cada tres semanas al Banco de Costa Rica, entidad asignada para el resguardo de las cintas de respaldo, tal como lo detalla[3] la jefatura de TI, comprometiendo la información institucional ante un fallo técnico del servidor de respaldos, por cuanto no habría posibilidad de recuperar los datos de las ultimas tres semanas.

Por medio del correo electrónico del 29 de enero de 2020, el jefe de TI indica que la practica mencionada en el párrafo anterior obedece a que las cintas de respaldo son de alta capacidad aunado a la implementación de un método de respaldo incremental, donde se respaldan los cambios a la información a partir de la fecha del ultimo "back up", sin embargo, para esta Auditoría dicho hecho deviene en un riesgo importante ante la ocurrencia de una situación no deseada que pudiera afectar tales cintas, ya que se contaría únicamente con el resguardo externo el cual puede presentar sesgos en la información.

En relación con lo expuesto, los funcionarios, que ocupan las plazas Profesional de Informática 1A con puesto 501194 y el Profesional de Informática 1B, puesto 503891, son los responsables de brindar mantenimiento a los sistemas y bases de datos, llevan una bitácora de tareas de respaldo, donde se registra fecha, nombre del funcionario que lo realizó y el medio de almacenamiento, los registros quedan en la

[2] Caja de seguridad Banco de Costa Rica.
[3] Acta AI-044-2019, 11 diciembre 2019.

base de datos del sistema de respaldos y la ejecución es diaria de lunes a viernes según expresan dichos funcionarios a los cuales fueron entrevistados por esta auditoría.[4]

Por otra parte, no se evidencian pruebas de restauración de los respaldos generados, por lo que dicha condición establece una representativa omisión de control en virtud de la información de carácter sensible que se maneja, la cual puede perderse y no recuperarse, si fallará el servidor actual de respaldos.

En relación con lo anterior, las Normas Técnicas para la Gestión de Tecnologías de Información en el Dominio I: Normas de Aplicación General, indican al respecto:

> *"*1.4 Gestión de la seguridad de la información. 1.4.4 Seguridad en las operaciones y comunicaciones La organización debe implementar las medidas de seguridad relacionadas con la operación de los recursos de TI y las comunicaciones, minimizar su riesgo de fallas y proteger la integridad del software y de la información. Para ello debe: a. Implementar los mecanismos de control que permitan asegurar la no negación, la autenticidad, la integridad y la confidencialidad de las transacciones y de la transferencia o intercambio de información. b. Establecer procedimientos para proteger la información almacenada en cualquier tipo de medio fijo o removible (papel, cintas, discos, otros medios), incluso los relativos al manejo y desecho de esos medios. c. Establecer medidas preventivas, detectivas y correctivas con respecto a software "malicioso" o virus.".

Ante la ausencia de un marco de seguridad de la información actualizado, limita la posibilidad de establecer una estrategia para resguardar los datos de la institución, por cuanto dicho marco se formuló en el año 2012 (ocho años), situación que confirman que la institución podría eventualmente exponerse a la pérdida de uno de sus activos más valiosos-la información.

Por tanto, la continuidad de los servicios informáticos se apoya principalmente en la disponibilidad de las bases de datos; en función de esa necesidad,

[4] Actas de entrevistas No. AI-048-2019 y AI-049-2019 del 11 de diciembre de 2019.

por lo que reviste la importancia de respaldos continuos y funcionales, custodiados y administrados; y cumplir con la normativa aplicable.

Ante lo señalado por el Jefe de TI,

> "Hay riesgo que son naturales, que se contemplan siempre, como inundaciones o incendios, también otros como daños en los equipos por su antigüedad o problemas eléctricos, y otros que pueden ser malintencionados, además de los riesgos por error humano.".[5]

Por tanto, es conveniente que el jerarca institucional en coordinación con el jefe de la unidad con el fin de obtener un servidor adicional con amplia capacidad de espacio que garantice seguridad razonable a los respaldos de información ejecutados y con ello minimice el riesgo de pérdida de información sensible.

2.2 Actualización del procedimiento.

La revisión del Manual de procesos y procedimientos determinó que se encuentra desactualizado, a la vez no fue posible conocer la política relativa a la revisión periódica de los procedimientos para mantener su vigencia.

El Manual de normas generales de control interno para la Contraloría General de la República y las entidades y órganos sujetos a su fiscalización en la norma 4.5, "Instrucciones por escrito", en lo de interés señala:

> "Las instrucciones que se impartan a todos y cada uno de los funcionarios de la institución deben darse por escrito y mantenerse en un compendio ordenado, actualizado y de fácil acceso que sea de conocimiento general.". (El subrayado es nuestro).

La desactualización de procedimientos en la unidad de TI afecta las sanas prácticas de control, pues el objetivo de este tipo de documentos es guiar de manera efectiva a los funcionarios para que asumen la labor de realizar respaldos de datos y cualquier otra función que se les asigne y se minimice el riesgo de pérdida de información ante un evento no deseado que afecte los sistemas institucionales.

[5] Acta AI-044-2019 11 diciembre 2019.

Sobre el particular, el procedimiento utilizado actualmente por la unidad de TI fue aprobado el 20 de diciembre del 2013 por la Jefatura de la Unidad de Planificación y la Directora General Adjunta de ese entonces. Posteriormente, el 07 de enero del 2014 bajo el oficio M-DG-006-2014 el jerarca informa que el Manual fue aprobado y publicado en la "carpeta publica/Manual de procesos y procedimientos".

En relación con este tema, a solicitud de esta Auditoría, la Contraloría General de la República indica en oficio No 1015 (FOE-PGA-37) del 06 de febrero del 2007, y entre lo que interesa señala:

> "En criterio de este órgano contralor, la competencia para la aprobación de este tipo de manual le corresponde al Consejo Directivo, toda vez que si bien no se trata de disposiciones con rango reglamentario, esos instrumentos mantienen importantes similitudes con este tipo de normativa, y al no existir una norma especial que atribuya expresamente su aprobación otra instancia, debería ser ese órgano colegiado dotado de la potestad reglamentaria interna el que los ponga en vigor; asimismo, debe tomarse en consideración que definir la estructura administrativa del Instituto, aspecto indisolublemente ligado a la emisión de ese tipo de instrumento es también potestad del Consejo Directivo.".

Los manuales son importantes porque contienen los procedimientos por escrito para regular las actividades de respaldo y validación de datos, que expliquen la forma en que la información debe ser resguardada, así como procedimientos formales para que los documentos fuente o información que hayan perdido vigencia, o que hayan superado el periodo de retención, sean removidos de almacenamiento y destruidos en concordancia con el marco jurídico que regula dicho fin.

El Decreto Ejecutivo No. 37549-JP señala en el artículo 11 que:

> "Cada Ministerio o Institución adscrita al Gobierno Central, elaborara manuales para el uso e instalación de programas de ordenador y velarán por el entrenamiento de todos los funcionarios de su dependencia, de acuerdo con las necesidades y el uso legal de los programas de cómputo, incluyendo la expedición de notas de advertencia, el establecimiento y la aplicación de medidas disciplinarias por incumplimiento de las disposiciones del presente Decreto.".

Conforme lo señala el decreto citado, toda organización debe poseer manuales que contengan regulaciones sobre la captura y conversión de datos,

formalidad de los documentos fuente o información que hayan perdido vigencia, o que hayan superado el periodo de retención, sean removidos de almacenamiento y destruidos.

En relación con este tema, no se cuenta con un manual que establezca las actividades y acciones a ejecutar en el tema de las pruebas de respaldo, punto a tratar en el siguiente apartado, lo que evidencia que los funcionarios de la unidad evaluada actúan sin estándares y metodología por escrito, situación que debe ser de atención en el sentido de establecer los pasos a seguir en las actividades asignadas para cada puesto. Procede reiterar que los procesos y procedimientos institucionales deben ser conocidos y aprobados por el órgano colegiado del ICD

En atención a lo expuesto, es prudente que la Dirección General de este instituto emita una directriz institucional sobre la formulación y revisión de manuales de procesos y procedimientos por parte de los administrados, se garantice su aprobación por parte del Consejo Directivo, se incorporen elementos de vigencia y utilidad en apego a las buenas prácticas y a la realidad institucional, con el propósito de evidenciar, medir y controlar las actividades de los funcionarios.

2.3 Validación de las pruebas de respaldo.

Los respaldos de seguridad son un método idóneo de protección de datos, sin embargo, existe la posibilidad de que la copia de datos no funcione correctamente y en caso de necesitar la restauración no se pueda realizar ya que la información de la copia de seguridad puede encontrarse violentada por diversos motivos. Por lo cual la administración debe considerar: que el medio en el que se realice la copia no se encuentre dañado, que las automatizaciones de copias se ejecuten correctamente.

La unidad de TI realizó un importante esfuerzo que se concretó con la elaboración de un marco de seguridad de la información denominado “Normas de seguridad de datos según la aplicación de los principios de PCI DSS (Payment Card Industry) elaborado en octubre 2012, dirigido por el jefe de Tecnologías de Información (TI) para que fuese puesto en ejecución, según consta en el documento ICD-UI-SD001-2012, no obstante, se reitera que dicho documento a la fecha se encuentra desactualizado, si se toman en cuenta el surgimiento de nuevas normas de calidad y seguridad como por ejemplo ISO, ITIL, COBIT 5 que deben ser adoptadas en la teoría y en la práctica.

A pesar de ese marco de seguridad instaurado en el pasado, no se obtuvo evidencia respecto de la planificación y ejecución de pruebas integrales a los respaldos que garanticen su funcionalidad en la recuperación de las bases de datos.

Dicho modelo de seguridad define las relaciones con proveedores y contratistas que manejen información sensible de la institución, medidas adicionales como lo son el respaldo de información que fortalezca la integridad de los datos y disminuya la vulnerabilidad de la plataforma tecnológica.

Para mayor validez por parte de esta unidad, se revisó el presente procedimiento en el SIGMA (Sistema de Gestión y Monitoreo de Actividades), el cual pertenece al proceso denominado Infraestructura Tecnológica condigo ICD-UI-0002-POSI, 2020 y no fue posible determinar en el Manual de Procesos de TI el procedimiento para la validación de las pruebas de respaldos pertinentes.

Aun cuando se han realizado importantes esfuerzos para minimizar el impacto negativo sobre la continuidad de las operaciones y pronta recuperación de las aplicaciones y datos de la institución ante eventos no deseados, esa comprobación periódica de la funcionalidad de los respaldos reviste vital importancia, pues es el medio que permite asegurar su efectividad, confiabilidad y pertinencia de la información.

Es conocido por esta Auditoría Interna mediante las entrevistas aplicadas a los funcionarios de TI que, para la ejecución de pruebas la disponibilidad de espacio en disco o equipo es un factor crítico, sin embargo, dicha condición no excluye la determinación de las posibles alternativas para cumplir con este requerimiento de control, cuando menos, en las bases de datos que se cataloguen como sensibles para la organización. La comprobación de pruebas procura, entre otros, minimizar el riesgo de eventuales fallas en los respaldos que afecten negativamente la recuperación de datos sensibles para la institución.

Por su parte, el jefe de TI al entrevistarlo[6] sobre el tema, señala:

> Se requiere robustecer la parte de almacenamiento de información institucional y también los medios de respaldo deben ser duplicados, así como también los dispositivos para poder realizar esos respaldos.

[6] Acta No. AI-044-2019 del 11 de diciembre 2019

La norma 1.3 Gestión de Riesgos de las normas técnicas para la gestión de las TI, señala al respecto:

> "La organización debe responder adecuadamente a las amenazas que puedan afectar la gestión de las TI, mediante una gestión continua de riesgos que esta integrada al sistema especifico de valoración del riesgo institucional y considere el marco normativo que le resulte aplicable.".

Cabe rescatar que las instituciones son vulnerables al ataque inminente de virus informáticos, en unos casos desde el punto de vista de terrorismo, implantación de identidad, hurto de datos con gran valor, todos contribuyen a una amenaza para la organización, por lo que generan dependencia sobre copias de seguridad satisfactorias y oportunas.

Por lo anterior, algunas organizaciones normalmente relegan sobre terceras personas o soluciones independientes el testeo, validación, optimización y el hacerse cargo de sus operaciones de copia de seguridad.

De la opinión externada por la jefatura de la unidad objeto de estudio, el cual indica que los recursos humanos y monetarios son muy limitados, no es compartida por esta Auditoría, por cuanto no es justificante para no proporcionar al jerarca el panorama sobre las dificultades que existen y se puedan tomar decisiones en beneficio de la protección de la información.

En lo concerniente, la norma 1.4.6 Seguridad en la implementación y mantenimiento de software e infraestructura tecnológica reza:

> "La organización debe mantener la integridad de los procesos de implementación y mantenimiento de software e infraestructura tecnológica y evitar el acceso no autorizado, daño o perdida de información…".

De lo expuesto, es prudente que la jefatura de la unidad de Tecnologías de Información formule un procedimiento para la realización de pruebas de respaldo de información, y que dicha validación se documente, con el propósito de asegurar que los funcionarios tienen las indicaciones claras sobre el respaldado de datos de forma correcta y oportuna, disminuyendo el riesgo de omisiones en la validación de datos.

3. CONCLUSIONES.

Se determina en el proceso objeto de evaluación que la capacidad de espacio para los respaldos de la información institucional es limitada, pues no se cuenta con un número de servidores suficiente para almacenar la información que manejan las unidades del ICD, pues solo se cuenta con un servidor, siendo un riesgo vulnerable en el almacenamiento de datos.

Según el criterio[7] técnico de la jefatura de la unidad de Tecnologías de Información, la capacidad del servidor de respaldos de información debe ser el doble de la actual, 70.000 GB, para que permita establecer una política de respaldos y recuperación adecuada.

Se mantiene un respaldo de la información de la Institución, custodiado en un lugar externo a ésta[8], no obstante, las cintas de respaldo se envían una vez cada tres semanas al Banco de Costa Rica, entidad asignada para el resguardo de las cintas de respaldo.

Por otra parte, no se evidencian pruebas de restauración de los respaldos generados, por lo que dicha condición establece una representativa omisión de control en virtud de la información de carácter sensible que se maneja, la cual puede perderse y no recuperarse, si fallará el servidor actual de respaldos.

El manual de procesos determinó que se encuentra desactualizado el procedimiento, a la vez no fue posible conocer la política relativa a la revisión periódica de los procedimientos para mantener su vigencia.

No se obtuvo evidencia respecto de la planificación y ejecución de pruebas integrales a los respaldos que garanticen su funcionalidad en la recuperación de las bases de datos y además no fue posible determinar en el Manual de Procesos de TI el procedimiento para la validación de las pruebas de respaldos pertinentes.

4. RECOMENDACIONES.

A LA DIRECCIÓN GENERAL.

1. Es conveniente se gestione con las áreas competentes administrativas y Jefe de TI, las acciones para adquirir un servidor con amplia capacidad de espacio que

[7] Correo electrónico 5 febrero 2020.
[8] Caja de seguridad Banco de Costa Rica.

garantice seguridad razonable a los respaldos de información ejecutados y con ello minimice la eventual pérdida de información sensible**.(léase punto 2.1 de este informe).**

2. Es prudente que la Dirección General de este instituto emita una directriz institucional sobre la formulación y revisión de manuales de procesos y procedimientos por parte de los administrados, se garantice su aprobación por parte del Consejo Directivo, se incorporen elementos de vigencia y utilidad en apego a las buenas prácticas y a la realidad institucional, con el propósito de evidenciar, medir y controlar las actividades de los funcionarios. **(Véase el punto 2.2 de este informe).**

3. Girar instrucciones a la jefatura de la unidad de Tecnologías de Información con el fin de que se formule un procedimiento para la realización de pruebas de respaldo y validación, con el propósito de asegurar que los funcionarios tengan indicaciones claras sobre el respaldado de datos de forma correcta y oportuna. **(Ver punto 2.3 de este informe)**

DEYANIRA BERMUDEZ CALDERON (FIRMA)

Firmado digitalmente por DEYANIRA BERMUDEZ CALDERON (FIRMA)
Fecha: 2020.04.23 08:39:14 -06'00'