Políticas de Defensa y FONDEF

Las Políticas de Ciberdefensa sobre las Infraestructuras Criticas argentinas y su aplicación en el FONDEF.

Lic. Guillermo Enrique TORRES

Universidad de la Defensa

Diplomatura Internacional en Comunicación y Defensa

Diplomatura Internacional: Comunicación y Defensa Nacional. Cohorte 2021

Trabajo Integrador Final

Cursante: Lic. Guillermo Enrique TORRES.

Tema: Política de Defensa y la importancia del FONDEF.

Temática: Las Políticas de Ciberdefensa sobre las Infraestructuras Criticas argentinas y su aplicación en el ***FONDEF***.

Fundamento:

Porque el análisis y difusión de ésta temática de la política de defensa permite visualizar la relevancia de la Estrategia de Ciberdefensa sobre las Infraestructuras Criticas argentinas y su necesidad de apoyo en el FONDEF.

Porque permite entender la importancia de los temas relacionados a la problemática de la Ciberdefensa / Ciberseguridad.

Objetivos: Exponer y Difundir la importancia de asegurar la Ciberdefensa de los bienes y servicio que entregan las Infraestructuras Criticas argentinas en el contexto de la Seguridad Estratégica Nacional y su aplicación en el FONDEF.

Informe Periodístico Extendido: Informe de 10 fojas.

Público Objetivo: Publico en general y seguidores de noticias e información de Defensa - Ciberdefensa.

Medio / plataforma elegida para publicación: Medio gráfico / Revista **InfoDefensa**

Descripción de formato comunicacional: Pieza Comunicacional – Nota Periodística.

Partes de la noticia:

- **Volanta (Anticipa o complementa la información del título)**
- **Título (destaca lo más importante de la noticia).**
- **Copete (se encuentra debajo del título y es la síntesis de lo más importante del texto).**
- **Cuerpo de la noticia (se da la información completa, de mayor a menor importancia).**
- **Fotografía (de acuerdo al texto; puede ser opcional).**
- **Epígrafe (debe ubicar a la fotografía en la noticia y enunciar de qué trata la fotografía).**

Estructura de la Noticia

Esquema discursivo general:

Pieza comunicacional: Nota Periodística.

El artículo “Nota Periodística” presenta información actual y relevante sobre política de defensa de interés para personas profesionales, educadores, e investigadores seguidores de las temáticas de defensa junto con autoridades del ámbito político y militar.

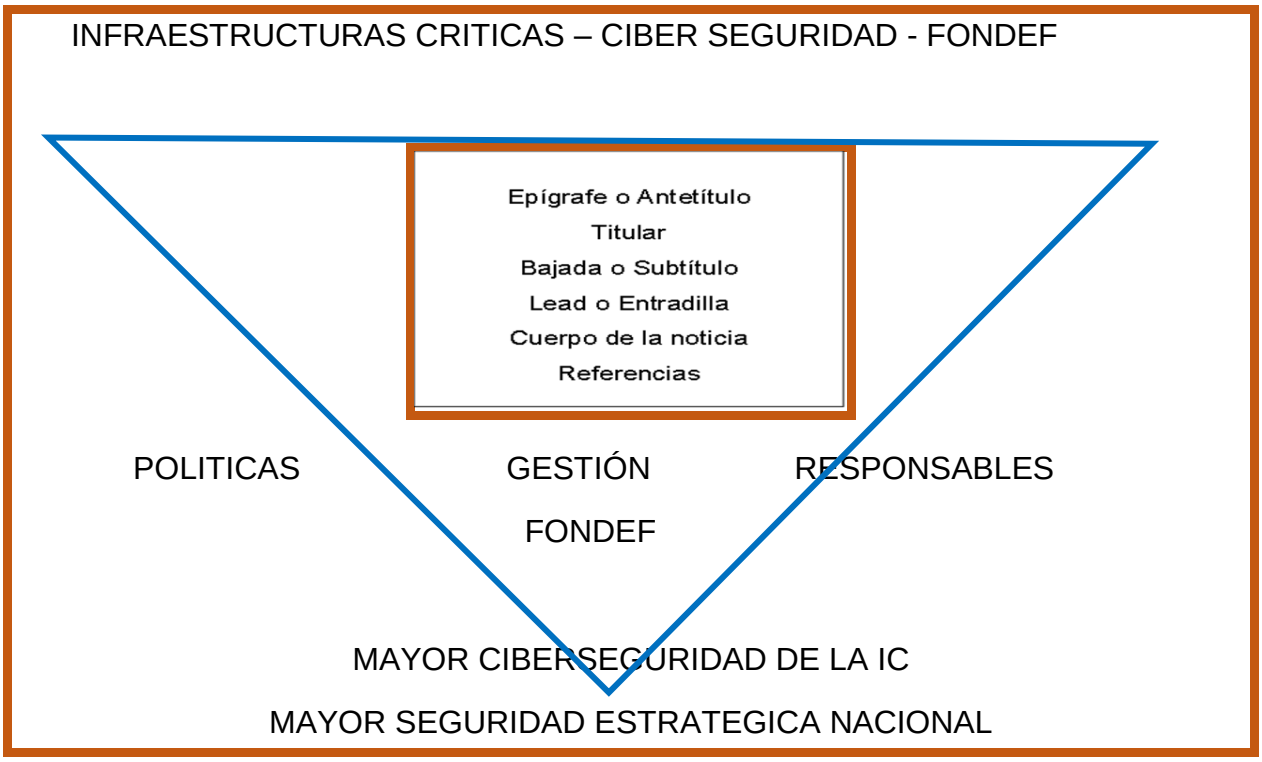
Es un texto descriptivo objetivo que se centra en brindar información sobre políticas de defensa, seguridad estrategia en el área de ciberdefensa concernientes a las Infraestructuras Criticas (IC) y su relación con la asignación de presupuestos del FONDEF.

Está escrito por personas asociadas al medio donde aparece publicado que producen información continua del área.

Los autores habitualmente son personas con experiencia y reconocimiento.

Las ideas que se exponen en ocasiones son polémicas y quieren provocar discusión o tendencia en la opinión pública.

Pieza comunicacional:



Estrategia de comunicación: Difundir información importante sobre las Infraestructuras Criticas (IC) en lo que respecta a la Ciberseguridad y cómo afecta o favorece su entendimiento sobre las vulneraciones, amenazas y o ataques a las que están expuesta dichas IC y como afectas la vida de las personas en relación a la Estrategia de Seguridad Nacional, además de su posible concreción por medio de la asignación del FONDEF.

Diplomatura Internacional: Comunicación y Defensa Nacional. Cohorte 2021

Trabajo Integrador Final

Viernes, 10 de diciembre del 2021 **Ciberseguridad / Ciberdefensa** **Revista InfoDefensa**

MÁS CIBER EN LAS INFRAESTRUCUTRAS CRITICAS CON MÁS FONDEF

EL FONDEF PERMITIRÁ INCORPORAR MAS POLITICAS DE CIBERSEGURIDAD SOBRE LAS INFRAESTRUCTURAS CRITICAS QUE ESTAN FUERA DEL PRESUPUESTA DE LAS FUERZAS

UNA TRIANGULACIÓN ENTRE:

CIBERDEFENSA / CIBERSEGURIDAD – LAS INFRAESTRUTURAS CRITICAS (IC) - FONDEF

"Debemos fortalecer las tareas de Ciberdefensa" palabras del Ministro de Defensa Jorge Taiana en una clase magistral en el acto por los 15 años de creación de la Escuela Superior de Guerra Conjunta.

Taiana en la Escuela Superior de Guerra

Las infraestructuras y los servicios críticos afrontan un gran reto en materia de ciberseguridad. Por eso, pensar en la protección de Infraestructuras Críticas requiere el rediseño de métodos técnicos y principalmente de gestión, para una administración segura en un mundo cibernético y lleno de amenazas, vulnerabilidades y ataques híbridos.

El jefe de la cartera defensa se refirió a la nueva Directiva de Política de Defensa Nacional y al inicio de la etapa de planeamiento estratégico de la misma. En ese marco, sostuvo que "*debemos fortalecer nuestras capacidades y reequipar nuestras Fuerzas Armadas*". "Sabemos que es un camino que abre una perspectiva de reconstrucción de nuestras capacidades y de alcanzar un desarrollo de la industria de la defensa acorde a las características de nuestro país", también destacó la necesidad de invertir en tecnología, "*somos un país que hace satélites, radares, y esa tecnología de primera calidad es la que tenemos que poner en primer lugar a la hora de pensar nuestro equipamiento es ciberdefensa, inteligencia artificial, aviones no tripulados y sistemas de guiado, con el objetivo de desarrollar una Defensa autónoma, cooperativa y multilateral*".

En la misma medida en otra exposición el ministro dijo que se espera que $68.000 millones estén destinados al fomento y al desarrollo de la industria para la defensa nacional, así se duplicará la inversión a través del Fondo Nacional de Defensa (FONDEF)[1] lo que posibilita destinar fondos a la Ciberseguridad / Ciberdefensa de las Infraestructuras Criticas donde se canalizaron inversiones este año por $33.000 millones, mientras para 2022 se destinará más del doble. Taiana puso el acento en la posibilidad de generar empresas que pueden asociarse a los procesos vinculados con la producción para la defensa.

Estos recursos se utilizan prioritariamente para reparaciones del material, modernización y compra.

Nuevos criterios de Infraestructuras Criticas Nacionales

En los últimos años la argentina ha actualizado los criterios sobre las Infraestructuras Criticas (IC) Nacionales, la Resolución N° 1523/2019 de la Secretaría de Gobierno de Modernización, en el marco de la Estrategia Nacional de Ciberseguridad, estableció nuevas definiciones y criterios, a efectos de manejar los mismos conceptos ya definidos por otros estados potencia, para la protección de las infraestructuras que respaldan servicios críticos.

En el marco de la Estrategia Nacional de Ciberseguridad[2], la Secretaría de Gobierno de Modernización, con la colaboración del Comité de Ciberseguridad, sancionó la Resolución N°1523/2019[3] que define el concepto de infraestructuras críticas e infraestructuras críticas de la información.

Así, infraestructuras críticas se define como “aquellas que resultan indispensables para el adecuado funcionamiento de los servicios esenciales de la sociedad, la salud, la seguridad, la defensa, el bienestar social, la economía y el funcionamiento efectivo del Estado, cuya destrucción o perturbación, total o parcial, los afecte y/o impacte significativamente.”; mientras que, las infraestructuras críticas de información se definen como “las tecnologías de información, operación y comunicación, así como la información asociada, que resultan vitales para el funcionamiento o la seguridad de las infraestructuras críticas.”

La Normativa de Ciberseguridad Nacional vigente responde a[4]:

---

[1] Ley 27565. FONDO NACIONAL DE LA DEFENSA. http://servicios.infoleg.gob.ar/infolegInternet/anexos/340000-344999/342746/norma.htm

[2] A cargo del COMITÉ DE CIBERSEGURIDAD creado por el Decreto N° 577 del 28 de julio de 2017, se desplegarán las acciones para el uso seguro del Ciberespacio en nuestro país.

[3] https://www.boletinoficial.gob.ar/detalleAviso/primera/216860/20190918

[4] https://www.argentina.gob.ar/jefatura/innovacion-publica/direccion-nacional-ciberseguridad/normativa

Leyes relacionadas a la ciberseguridad

- **Ley 26.388 de Delito informático**
- **Ley 25.326 de Protección de Datos Personales**
- **Decreto Reglamentario N° 1558/2001**
- **Ley 25.506 de Firma Digital**
- **Decreto Reglamentario N° 2628/2002**
- **Ley 26.904 de Grooming**

Normativa vinculada a las funciones de la Dirección Nacional de Infraestructuras críticas de la información y ciberseguridad

- **Decisión Administrativa 641/2021. Establece los requisitos mínimos de seguridad de la información para organismos públicos**
- **Disposición 6/2021. Creación del Comité Asesor para el Desarrollo e Implementación de aplicaciones seguras.**
- **Disposición 1/2021. Centro Nacional de Respuestas a Incidentes Informáticos (CERT.ar) en el ámbito de la Dirección Nacional de Ciberseguridad.**
- **Resolución 580/2011. Creación del Programa Nacional de Protección de Infraestructuras Críticas de Información y Ciberseguridad.**
- **Disposición ONTI 3/2013. Aprobación de la Política Modelo de Seguridad de la Información.**
- **Resolución 1523/2019. Definición de Infraestructuras Críticas.**

Otras normativas relacionadas a la ciberseguridad

- **Decreto 577/2017. Creación del Comité de Ciberseguridad.**
- **Decreto 480/2019. Modificación del Decreto 577/2017.**
- **Resolución 829/2019. Aprobación de la Estrategia Nacional de Ciberseguridad.**
- **Resolución 141/2019. Presidencia del Comité de Ciberseguridad.**

Por qué incrementar los presupuestos y la determinación de las políticas de ciberseguridad sobre las Infraestructuras Criticas

Las Infraestructuras Críticas de todos los países estás expuestas a multitud de riesgos y amenazas fruto de sus vulnerabilidades. Las Infraestructuras Críticas son el objetivo más deseado de los atentados terroristas, los ataques cibernéticos de particulares e incluso ataques híbridos por parte de gobiernos y servicios de inteligencia, de ahí que necesiten una protección más avanzada, elevar esos estándares de seguridad nacional, no alcanzaría el presupuesto anual determinado año a año como parte del PBI, razón que fundamenta es uso de la herramienta presupuestaria que otorga el FONDEF.

Analizando los ataques terroristas del 11S en EEUU, las acciones cibernéticas de Anonymous o malwares diseñados por Servicios de Inteligencia como fue el caso de Stuxnet contra las Centrales Nucleares – Infraestructuras Criticas de Irán y del

escenario de la Seguridad Internacional[5], han provocado que la mayoría de los gobiernos establezcan líneas de acción estratégicas para garantizar la protección de sus Infraestructuras Críticas.

Por eso como argentino, conviene reconocer y saber qué es una Infraestructura Crítica de la que depende nuestra calidad de vida, conocer cómo y con qué criterios se protegen, nos permitirá proteger nuestros propios sistemas u organización nacional con la misma eficacia.

El fundamento del incremento de las estrategias de seguridad sobre las IC es su vinculación directa con las actividades humanas ya que a diario transportan electricidad, agua, transporte, transacciones bancarias, internet, telefonía, tramites gubernamentales online y otras actividades esenciales que dependen de centrales eléctricas o nucleares, plantas de aguas, centrales y terminales de transporte y tecnología satelital sobre sistemas de telecomunicaciones o de la Administración, además de ser esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población, cuya perturbación o destrucción afectaría gravemente a un Estado en todo tipo de contexto al no poder mantener esas funciones.

Cuando una infraestructura crítica es dependiente de otra, la caída de una infraestructura crítica supondría la paralización o menoscabo de los servicios de ambas, por lo que la protección de estas adquiere mayor importancia.

Áreas Estratégicas del ámbito nacional con IC que hacen a la Seguridad Estratégica Nacional.

- **Sistema Financiero y Tributario (entidades bancarias, información, valores e inversiones).**
- **Administración (servicios básicos, instalaciones, redes de información, principales activos y monumentos del patrimonio nacional).**

[5] ONU: "La SEGURIDAD es una situación en la que los Estados consideran que no hay peligro de un ataque militar, presión política ni coerción económica, con lo que pueden proseguir libremente su desarrollo y progreso"

- **Agua (embalses, almacenamiento, tratamiento y redes).**
- **Alimentación (producción, almacenamiento y distribución).**
- **Centrales y Redes de energía (producción y distribución).**
- **Instalaciones relacionadas con el Espacio Exterior.**
- **Centrales nucleares (producción, almacenamiento y transporte de mercancías peligrosas, materiales nucleares, radiológicos, etc.).**
- **Industria Química (producción, almacenamiento y transporte de mercancías peligrosas, materiales químicos, etc.).**
- **Investigación: laboratorios que por su idiosincrasia dispongan o produzcan materiales, sustancias o elementos críticos o peligrosos.**
- **Salud (sector e infraestructura sanitaria).**
- **Tecnologías de la Información y las Comunicaciones (TIC, ya sean infraestructuras críticas en sí mismas, como redes de telecomunicaciones, o den servicio de información y comunicaciones a otras infraestructuras críticas)**
- **Transportes (aeropuertos, puertos, instalaciones intermodales, ferrocarriles y redes de transporte público, sistemas de control del tráfico).**

El Centro Nacional de Protección de Infraestructuras Criticas es el órgano responsable del impulso, coordinación y supervisión de todas las políticas y actividades relacionadas con la protección de las infraestructuras críticas argentinas.

Entre sus principales objetivos se destacan las siguientes:

- **Obliga a que todas las infraestructuras críticas cuenten con un responsable de seguridad que haga de enlace con el Centro Nacional de Protección de las Infraestructuras Críticas en caso de que sea necesario.**
- **Fomenta el intercambio de información entre las diversas empresas e instituciones afectadas por esta catalogación.**
- **Define las medidas resolutivas que deben de poner en marcha las infraestructuras críticas en caso de ser víctimas de un ataque.**
- **Recoge los dictámenes y directivas que sigue el Estado para movilizar sus capacidades operativas frente a ataques deliberados, así como los mecanismos de coordinación establecidos con los operadores críticos en estos casos.**
- **Líneas de Acción Estratégicas de la Seguridad Nacional para las Infraestructuras Críticas.**
- **Determina presupuestos adicionales en este caso en coordinación con el FONDEF.**

Para fortalecer las infraestructuras críticas, la Estrategia de Seguridad Nacional ha establecido siete líneas de acción que son las siguientes:

1. Responsabilidad compartida y cooperación público-privada.
2. Planificación escalonada.
3. Equilibrio y eficiencia.
4. Resiliencia.
5. Coordinación.

6. Cooperación internacional.
7. Garantía en la seguridad de las infraestructuras críticas.

Conclusiones y propuesta

La prioridad que tiene para la nación la Seguridad Estratégica sobre las Infraestructuras Criticas a través de la Ciberseguridad es fundamental para el desenvolvimiento social de los argentinos, hemos podido analizar que son varios actores, públicos y privados, los que están comprometidos con dicha situación.

Principales responsables de la protección de las Infraestructuras Críticas

1. Gobiernos – Son los principales interesados en la generación e implantación de iniciativas de Protección de Infraestructuras Críticas

2. Organismos competentes – Es muy común que los gobiernos deleguen las tareas de difusión, elaboración y gestión de iniciativas en organismos públicos, privados o combinación de ambos.

Los organismos competentes son:

- **La Secretaría de Modernización.**
- **El Centro Nacional para la Protección de las Infraestructuras Críticas.**
- **Los Ministerios y la Jefatura de Gabinete.**
- **Las Provincias, Ciudades Autónomas y Municipios.**
- **Las Corporaciones Locales mediante la asociación de Entidades Locales de mayor implantación a nivel nacional.**
- **La Comisión Nacional para la Protección de las Infraestructuras Críticas.**

3. Operadores de infraestructuras críticas – Son los que tienen más interés en que sus infraestructuras sean seguras, funcionen de manera adecuada y no sufran daños, interrupciones ni ataques. Las principales funciones de los operadores críticos en materia de seguridad son:

Analizar sus organizaciones de ciberseguridad.

- **Diseñar nuevas políticas.**
- **Establecer nuevas estructuras de gobierno y o privadas para el control.**
- **Educación e información.**
- **Analizar los riesgos y las amenazas no previstos con anterioridad.**
- **Llevar a cabo estudios de las consecuencias y el impacto que supondría la interrupción y no disponibilidad de los servicios esenciales.**
- **Concientizar al personal sobre la importancia del cumplimiento de los procedimientos y recomendaciones de seguridad.**

4. Terceras partes – No se ven afectadas de manera directa por las exigencias legales, pero sí de manera indirecta.

Amenazas y vulnerabilidades de las infraestructuras críticas a las que están expuestas las infraestructuras críticas argentinas:

- **Terrorismo – Cada vez tiene mayores dimensiones.**
- **Crimen organizado – Es una amenaza de carácter transnacional, flexible y opaca. Tiene una gran capacidad desestabilizadora, cuyo fin es el ánimo de lucro, pero debilitando el Estado y corrompiendo la buena gobernanza económica.**
- **Proliferación de armas de destrucción masiva – Supone una gran amenaza para la paz y la seguridad internacional, afectando de manera directa a la Seguridad Nacional.**
- **Espionaje – Es una amenaza de primer orden para la seguridad tanto por el espionaje de otros países como por el realizado por empresas extranjeras.**
- **Vulnerabilidad del ciberespacio – Las amenazas en el ciberespacio han adquirido una dimensión global que va mucho más allá de la tecnología.**
- **Vulnerabilidad del espacio marítimo – Este espacio es de gran relevancia para Argentina por su litoral atlántico, pues reviste un gran valor estratégico.**
- **Amenazas derivadas de actos intencionados y de naturaleza delictiva (la piratería, el terrorismo, los tráficos ilícitos, etc)**
- **Amenazas accidentales derivadas de las condiciones naturales del propio medio (accidentes marítimos y las catástrofes naturales).**
- **Vulnerabilidad del espacio aéreo y ultraterrestre – El espacio aéreo puede ser comprometido por parte de actores estatales y no estatales.**
- **Causas naturales – El impacto de las catástrofes perjudica la vida de las personas, así como a los bienes patrimoniales, al medioambiente y al desarrollo económico.**
- **Otros – Cualquier tipo de perturbación en los servicios ofrecidos por estas infraestructuras de sectores estratégicos y esenciales.**

REFERENCIAS

1. Portal Web AMBITO FINANCIERO. ECONOMIA. Jorge Taiana indicó que se duplicará la inversión a través del Fondo Nacional de Defensa. 02 de noviembre del 2021.

   https://www.ambito.com/economia/inversion/jorge-taiana-indico-que-se-duplicara-la-traves-del-fondo-nacional-defensa-n5309845

2. Portal Web Argentina.gob.ar. Taiana brindó una clase magistral en el acto por los 15 años de creación de la Escuela Superior de Guerra Conjunta. Lunes 06 de septiembre de 2021

   https://www.argentina.gob.ar/noticias/taiana-brindo-una-clase-magistral-en-el-acto-por-los-15-anos-de-creacion-de-la-escuela

3. INFOLEG – LEY 27565 HONORABLE CONGRESO DE LA NACION ARGENTINA. 17-sep-2020. FONDO NACIONAL DE LA DEFENSA. CREACION. Publicada en el Boletín Oficial del 01-oct-2020 Número: 34487 Página:4.

   http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do;jsessionid=78025BE9139B12459AF0BFF7F6D8F296?id=342746

4. TECNOLOGIA SUR SUR - TSS AGENCIA DE NOTICIAS TECNOLÓGICAS Y CIENTÍFICAS.UNIVERSIDAD NACIONAL DE SAN MARTIN. 24 SEPTIEMBRE 2020. NOTA “Agustín Rossi: - Con el FONDEF se podrá planificar a futuro” Por Matías Alonso.

   https://www.unsam.edu.ar/tss/agustin-rossi-con-el-fondef-se-podra-planificar-a-futuro/

5. Argentina.gob.ar. Jorge Taiana juró como nuevo ministro de Defensa. Publicado el miércoles 11 de agosto de 2021.

   https://www.argentina.gob.ar/noticias/jorge-taiana-juro-como-nuevo-ministro-de-defensa

6. Ciberseguridad Industrial e Infraestructuras Críticas. Editorial : Editorial Ra-Ma; 1er edición (9 Mayo 2021). Idioma : español. Tapa blanda : 346 páginas. ISBN-10 8418551364. ISBN-13 : 978-8418551369.

7. JEFATURA DE GABINETE DE MINISTROS. SECRETARÍA DE INNOVACIÓN PÚBLICA. Resolución 36/2020. RESOL-2020-36-APN-SIP#JGM.

   http://servicios.infoleg.gob.ar/infolegInternet/anexos/335000-339999/338378/norma.htm

8. Miranzo, Mónica; del Río, Carlos La protección de infraestructuras críticas Universidad Complutense de Madrid (UNISCI) Discusión Papers, núm. 35, mayo-agosto, 2014, pp. 339-352. Madrid, España. ISSN: 1696-2206

   https://www.redalyc.org/pdf/767/76731410018.pdf

9. Sánchez Manuel. Infraestructuras Críticas y Ciberseguridad. Paper. Publicado el 6 julio, 2011.

10. VALIENTE PÉREZ, JOSÉ COORD./PAREDES TAMARGO, IGNACIODIR. /LINARES FERNÁNDEZ, SAMUELREV. La protección de infraestructuras críticas y la ciberseguridad industrial. EDITORIAL: Industrial. España. ISBN: 978-84-616-6330-9. FECHA PUBLICACIÓN: 01-10-2013