Defensa | DIVRI | DIRECCIÓN DE VETERANOS Y REHABILITACIÓN INCLUSIVA

2025

PLAN CONTINUIDAD DEL NEGOCIO - TICS

Ministerio de Defensa Nacional
Dirección de Veteranos y Rehabilitación Inclusiva - DIVRI

Versión 1
2025

PLAN DE CONTINUIDAD DEL NEGOCIO - TICS

TABLA DE CONTENIDO

Contenido

INTRODUCCION

La Dirección de Veteranos y Rehabilitación Inclusiva, a través de la Oficina de las TICS y en atención a lo dispuesto por el decreto 1078 de 2015 en su artículo 2.2.17.6.6. Seguridad de la información, por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, donde se define que los actores que traten información, en el marco del presente título, deberán adoptar medidas apropiadas, efectivas y verificables de seguridad que le permitan demostrar el correcto cumplimiento de las buenas prácticas consignadas en el Modelo de Seguridad y Privacidad de la Información (MSPI), emitido por el MinTIC o un sistema de gestión de seguridad de la información certificable, con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información.

La implementación del MSPI requiere definir y aplicar procedimientos para proteger la información de la entidad ante eventos de desastre, que afecten la disponibilidad de los servicios críticos de la DIVRI, definiendo acciones que permitan reducir su impacto negativo, estas acciones permitirán una correcta gestión de la continuidad del negocio orientada a los servicios de tecnologías de la información y comunicación (TIC), por esto, la DIVRI decidide acatar los lineamientos que para este sentido contempla la Guía para la preparación de las TIC para la continuidad del negocio (BCP), emitida por MinTIC y la norma ISO 22301, que dicta las acciones, evidencias y resultado mínimo esperado para evitar que la operación misional del DIVRI se interrumpa.

1. OBJETIVO

1.1. OBJETIVO GENERAL

Establecer las actividades preventivas y reactivas que permitan mantener la capacidad de respuesta de la DIVRI, ante situaciones de interrupción de sus actividades misionales, mediante la creación y mejora continua del Análisis de Impacto al Negocio (BIA), el Plan de Continuidad del Negocio y el Plan de recuperación de desastres (DRP por sus siglas en ingles Disaster Recovery Plan).

Todo lo anterior asociado a documentos como la Política General de Continuidad del Negocio, el Programa de Continuidad del Negocio el cual, detalla los procesos y la fecha en la que se realizan pruebas de continuidad operativa y la documentación de estos resultados en el formato correspondiente.

1.2 OBJETIVOS ESPECIFICOS

- Disminuir el impacto ante la materialización de un riesgo que obligue a activar el Plan de Continuidad o el Plan de Recuperación ante el Desastre.
- Disminuir los tiempos de recuperación de la operación normal del DIVRI
- Establecer el cumplimiento de la copia de respaldo de información con el fin de que los puntos de recuperación operativa estén acordes con la necesidad de recuperación operativa y tecnológica del DIVRI
- Definir y documentar los cargos de los funcionarios que pertenezcan a los procesos críticos del DIVRI, con el fin de garantizar su pronta conectividad y gestión operativa y tecnológica.
- Asignar responsabilidades al personal designado.
- Identificar las actividades críticas, los recursos y los procedimientos necesarios para llevar a cabo las operaciones durante las interrupciones prolongadas del servicio.
- Asegurar una pronta recuperación en los servicios críticos para los Grupos de Valor y partes interesadas
- Proteger los activos de información de manera adecuada.

2. NORMATIVIDAD ASOCIADA

El artículo 2.2.17.6.6 del Decreto 1078 de 2015, que compila normas relacionadas con el sector de Tecnologías de la Información y las Comunicaciones (TIC) en Colombia, establece disposiciones específicas sobre la **gestión de riesgos de seguridad y privacidad de la información**. Este artículo hace parte del marco normativo que regula la implementación de políticas de seguridad digital en entidades públicas y privadas.

3. PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO (BCP)

El ciclo de funcionamiento del modelo de operación de continuidad del negocio y su funcionamiento, dentro del modelo de operación de seguridad y privacidad de la información, desarrolla cuatro (4) fases que comprenden el modelo de operación del MSPI definiendo objetivos, metas y herramientas que permiten que la continuidad del negocio sea un modelo sostenible dentro de la DIVRI. En la siguiente ilustración, se aprecian las fases del modelo de operación del MSPI, se debe tener en cuenta que la fase de diagnóstico no se tiene en cuenta en el BCP.

Modelo de operación seguridad y privacidad de la información.

4. METODOLOGIA

La DIVRI define la estrategia metodológica para establecer las políticas, objetivos, procesos y procedimientos pertinentes del (BCP), como punto clave se deben establecer los requerimientos de continuidad del negocio, los cuales son aprobados por la alta dirección.

4.1 Objetivos específicos del BCP

- Asegurar la continuidad de las aplicaciones críticas que son apoyadas por los servicios tecnológicos prestados por el proceso TICS, dentro de los márgenes de tiempo tolerables.
- Minimizar el tiempo de toma de decisiones durante un incidente que amenace la continuidad de las operaciones críticas del negocio.
- Mantener los servicios brindados a los ciudadanos y por ende la confianza en la entidad.
- Minimizar la pérdida de información crítica del negocio.
- Diseñar la estrategia del Plan de recuperación de desastres (DRP por sus siglas en ingles Disaster Recovery Plan) acorde a las necesidades de DIVRI, que le permita continuar su operación con el menor impacto posible.

4.2 Manejo de interrupciones

Se ha definido el manejo de interrupciones por su relación con la severidad y el impacto que las mismas pueden tener sobre los servicios de TI:

Tipo de evento	Características	Ejemplos	Respuesta
Desastre	Evento que inhabilita el Centro de Cómputo Principal (CCP) para prestar sus servicios. No permite seguir laborando en las instalaciones principales.	Terremotos, incendio general, fallo eléctrico en el sector.	DRP
Interrupción	Evento que requiere ser evaluado para ser tratado como desastre o como contingencia. Puede llegar a ser considerado como un desastre o una contingencia, dependiendo	Incendio localizado, atentado terrorista, huelga	DRP Planes de contingencia

	del impacto que se determine en el manejo de incidentes.	interno o externo.	
Contingencia	Evento que afecta puntualmente un recurso necesario para la prestación de los servicios de Informática. No impide el acceso al CCP. En ausencia de plan de contingencia, requiere evaluación que puede llevarla a categoría de desastre	Fallo de sistemas o servicio, ausencia de personal clave	Planes de contingencia

Las interrupciones catalogadas como desastre son las menos probables, pero de llegar a ocurrir representan riesgos de afectación a la vida humana, a las instalaciones, a proveedores y a la infraestructura de la entidad o de la ciudad, esta afectación, supone un grado de dificultad mayor para el cumplimiento de los tiempos de recuperación planteados.

4.3 Fases de una interrupción

Dentro del manejo de una interrupción se definen 5 fases que se detallan a continuación.

Prevención: Tareas de preparación y actividades que garanticen que, ante la necesidad de su activación, el servicio se preste en las condiciones esperadas.

Respuesta: Actividades encaminadas al manejo del incidente en cuanto a evaluación de daños y proyección de la restauración con el objeto de generar los soportes necesarios para la toma de decisión de activar el DRP. También hacen parte de esta fase la activación del DRP y su procedimiento de notificación.

Recuperación: Activar sitio alterno y plataformas para prestar servicios.

Reanudación: Reiniciar la prestación de los servicios de los diferentes aplicativos desde un sitio alterno.

Restauración: Reparar los daños en el sitio principal en busca de retornar a la normalidad.

4.4 Lineamientos la preparación de la continuidad de negocio de TI

- Se debe asegurar que las actividades descritas, sean asignados al personal idóneo para su atención.

- Se debe velar por que se socialice a todos los colaboradores involucrados, tanto titulares como contingencia, los roles y funciones que deben desempeñar en caso de un incidente.

- Se debe mantener contacto permanente con los proveedores de servicios críticos y conocer sus estrategias de continuidad de negocio.

- Se deben aprobar y asegurar los cambios significativos para los servicios de TI.

- Se debe aprobar toda interrupción programada de servicio.

- Se debe asegurar que toda acción preventiva o correctiva propuesta cumpla con las políticas de seguridad de la información.

- Se debe definir el procedimiento para el manejo de incidentes graves que permita: confirmar la naturaleza y grado del incidente, tomar control de la situación, contener el incidente y comunicar a las partes interesadas.

5. ESCENARIOS DE RIESGO

5.1 Desastre natural y Orden Publico

5.1.1 Análisis del contexto geográfico y de entorno

La entidad se encuentra en una zona estratégica de Bogotá, rodeada por:

- **Una base militar**, lo que implica presencia de armamento, personal armado y posibles objetivos de ataques o disturbios.
- **Industrias con manejo de elementos químicos**, con almacenamiento y manipulación de sustancias volátiles, lo que representa riesgo de explosiones, incendios o contaminación.
- **Empresa de almacenamiento de combustible**, con grandes volúmenes de material inflamable, aumentando el riesgo de incendios de gran magnitud.

5.1.2 Amenazas Potenciales

- **Desastres Naturales**
  - **Sismos**: Bogotá está en una zona sísmica moderada. Un terremoto podría dañar infraestructuras críticas, provocar fugas químicas o incendios.
  - **Inundaciones**: Aunque no frecuentes, lluvias intensas pueden afectar accesos, sistemas eléctricos y de comunicación.
- **Afectación del Orden Público**
  - **Protestas o disturbios sociales**: La cercanía a la base militar puede convertir la zona en foco de manifestaciones, con riesgo de enfrentamientos.
  - **Ataques terroristas o sabotajes**: La presencia de instalaciones estratégicas puede atraer amenazas dirigidas.
  - **Bloqueos o restricciones de movilidad**: Por razones de seguridad, el acceso a la zona puede ser restringido, afectando la operación normal.

5.1.3 Impactos Potenciales

- Interrupción total o parcial de operaciones.
- Evacuación del personal por seguridad.
- Daños a infraestructura física y tecnológica.
- Contaminación ambiental por químicos o combustibles.
- Pérdida de información o activos críticos.
- Afectación a la reputación institucional.

5.1.4 Medidas de Mitigación Recomendadas

- **Ejercicios sobre el plan de continuidad de negocio y recuperación ante desastres (BCP/DRP)** actualizados y probados.
- **Simulacros periódicos** de evacuación y respuesta ante emergencias.
- **Monitoreo constante** de condiciones ambientales y de seguridad pública.
- **Alianzas con autoridades locales** (bomberos, policía, defensa civil).
- **Infraestructura resiliente**: sistemas redundantes, respaldo de energía, almacenamiento seguro de datos.
- **Capacitación del personal** en manejo de crisis y primeros auxilios.

5.1.5 Ataque o fallo en la infraestructura tecnológica

5.1.5.1 Escenario de Riesgo por Fallo Tecnológico

Un fallo tecnológico puede generar una interrupción significativa en las operaciones de la entidad. Este tipo de fallo puede incluir:

- Caída de sistemas informáticos o redes de comunicación.
- Pérdida de acceso a bases de datos o información crítica.
- Fallos en sistemas de control de acceso, videovigilancia o sensores ambientales.
- Interrupción de servicios de energía o respaldo tecnológico.

Dado el entorno de alto riesgo, un fallo tecnológico puede desencadenar consecuencias graves como:

- Incapacidad para coordinar con autoridades de emergencia.
- Imposibilidad de activar protocolos de evacuación o confinamiento.
- Exposición a amenazas externas sin capacidad de respuesta tecnológica.
- Pérdida de trazabilidad de sustancias químicas o combustibles almacenados en el entorno.

5.2 Impactos Potenciales

- Interrupción total o parcial de las operaciones institucionales.
- Pérdida de información crítica o confidencial.
- Afectación a la seguridad física del personal y activos.
- Daños reputacionales y legales.
- Dificultades en la coordinación interinstitucional durante emergencias.

5.3 Medidas de Mitigación Recomendadas

- Implementación de sistemas redundantes de tecnología y energía.
- Copias de seguridad automáticas y almacenamiento externo seguro constante de infraestructura tecnológica.
- Simulacros de respuesta ante fallos tecnológicos.
- Capacitación del personal en manejo de crisis tecnológica con la base militar y empresas vecinas para protocolos conjuntos de emergencia.

5.4 Escenario de Riesgo: Interrupción de Operaciones por Ausencia de Recursos

5.4.1 Técnicos y Tecnológicos

La falta de infraestructura tecnológica adecuada, fallos en sistemas de información, ausencia de conectividad o soporte técnico, puede generar interrupciones en los procesos críticos, especialmente en un entorno donde la respuesta rápida ante emergencias es vital.

5.4.2 Financieros

La insuficiencia de recursos financieros limita la capacidad de la entidad para adquirir insumos, contratar servicios especializados, mantener infraestructura operativa y responder ante contingencias. Esto puede afectar la continuidad de operaciones en situaciones de crisis.

5.4.3 Humanos

La ausencia de personal capacitado en los diferentes aspectos tecnológicos y de continuidad del negocio, así mismo cuando se presentan evacuaciones por emergencia dado el riesgo ambiental, también en importante tener en cuenta que los funcionarios categorizados como críticos para la operación sufran enfermedades o se ausentan por periodos muy prolongados, puede paralizar funciones esenciales.

En un entorno de alto riesgo, la disponibilidad de talento humano entrenado es fundamental para garantizar la seguridad y continuidad.

5.4.4 Impactos Potenciales

- Interrupción total o parcial de operaciones.
- Afectación de la capacidad de respuesta ante emergencias.
- Pérdida de información crítica y activos institucionales.
- Riesgo de accidentes mayores por falta de monitoreo o control.
- Deterioro de la imagen institucional y pérdida de confianza.

5.4.5 Medidas de Mitigación Recomendadas

- Implementar planes de continuidad de negocio con enfoque en resiliencia de recursos.

- Establecer convenios interinstitucionales para apoyo técnico y humano en caso de emergencia.
- Crear fondos de contingencia para asegurar disponibilidad financiera.
- Capacitar al personal en múltiples funciones para asegurar reemplazos operativos.

5.4.6 Monitorear constantemente el entorno y actualizar los planes de respuesta.

6. Responsables

La DIVRI, establecerá mecanismos de implementación del Plan de Continuidad de TI mediante la adopción de normas pertinentes y la designación de personal encargado de su gestión, estableciendo los mecanismos administrativos, técnicos y procedimentales que se requieran. La responsabilidad en la recuperación de los servicios tecnológicos se encuentra a cargo de:

- Responsable de la infraestructura tecnológica de la DIVRI
- Responsable de seguridad de la información
- Equipo de soporte Técnico.
- Proveedores de servicios activos
- Dueños de procesos
- Responsable de los activos de información afectados

7. Actualización

La Oficina de TIC, es responsable por el mantenimiento y la revisión del Plan de Continuidad de TI.

Se realizará una revisión, anualmente o las necesarias requeridas en respuesta a cualquier cambio que pueda afectar la base original de la evaluación de riesgos de continuidad, identificación, valoración de los activos de información (ej.: cambios de plataforma, nuevos procesos, cambio de estructura organizacional), valoración de riesgos, entre otras actividades.

8. ORGANIZACIÓN DEL PLAN DE CONTINUIDAD DE TI

Etapas del Plan de Continuidad y responsables

8.1 Antes Del Evento (Prevención Y Preparación)

El objetivo de esta etapa es reducir la probabilidad de interrupción y preparar al DIVRI para responder eficazmente.

8.2 Acciones Clave:

- Identificación y análisis de riesgos (geográficos, tecnológicos, operativos).
- Clasificación de procesos críticos.
- Diseño de estrategias de respaldo (infraestructura, datos, personal).
- Capacitación y simulacros.
- Coordinación con entidades externas (militares, bomberos, policía, industria vecina).

8.3 Responsables:

Lider de Seguridad y Riesgos:

- lidera el análisis de amenazas.
- diseña y actualiza el PCO.

Jefe de Tecnología (TI)

- Asegura respaldo de sistemas y datos.

Administrativa

- Coordina medidas preventivas con la base militar.

Dirección General

- Aprueba recursos y políticas.

8.4 Durante el Evento (Respuesta y Contención)

Objetivo:

Minimizar el impacto del evento y proteger vidas, activos y operaciones críticas.

Acciones Clave:

- Activación del Comité de Crisis.
- Ejecución de protocolos de evacuación, confinamiento o traslado.
- Comunicación interna y externa (autoridades, empleados, medios).

- Activación de sitios alternos o trabajo remoto si aplica.
- Protección de activos críticos (infraestructura, información, personal).

8.5 Responsables:

Comité de Crisis: toma decisiones estratégicas en tiempo real.

Coordinador de Emergencias: ejecuta protocolos de respuesta.

Jefe de Comunicaciones: maneja la información oficial.

Jefe de Recursos Humanos: gestiona el bienestar del personal.

Enlace Militar o de Defensa Civil: Coordina con fuerzas armadas y socorro.

8.6 Después del Evento (Recuperación y Mejora)

Objetivo: restaurar operaciones normales, evaluar daños y fortalecer el plan.

Acciones Clave:

- Evaluación de impacto y daños.
- Activación del Plan de Recuperación ante Desastres (DRP).
- Reinstalación de servicios y procesos.
- Apoyo psicológico y logístico al personal.
- Revisión y mejora del Plan de Continuidad del Negocio basado en lecciones aprendidas.

8.7 Responsables

Lider de Seguridad con responsabilidades sobre la Continuidad de Negocio: Lidera la recuperación operativa.

Jefe de Infraestructura y Tecnología: Restablece sistemas y servicios.

Auditor Interno / Control Interno: Verifica cumplimiento y efectividad.

Dirección General: Aprueba mejoras y recursos.

8.8 Equipo de Seguridad y Salud en el Trabajo (SST)

Apoya recuperación humana.

En la DIVRI, frente al Plan de Continuidad de TI, se desempeñarán los siguientes roles:

8.9 Responsabilidad especifica de la infraestructura tecnológica de la DIVRI
Quien tiene a su cargo la responsabilidad de la infraestructura tecnológica de la DIVRI, Esto con el fin de brindar a la entidad la gestión necesaria para recuperar el ambiente de producción a fin de restituirlo a su estado normal.
Es responsable de:

Antes:

- Realizar análisis de riesgo al proceso
- Establecer el grado de criticidad del proceso.
- Evaluar el impacto que la indisponibilidad de los servicios críticos de la entidad.
- Estimar los tiempos de recuperación de los sistemas de información que soportan el proceso.
- Determinar en qué punto del tiempo se deben retomar los datos de las aplicaciones (es decir, qué tanta información se puede perder sin afectar significativamente la actividad de la entidad).
- Adelantar las gestiones necesarias para que los servicios tecnológicos puedan recuperarse después de un fallo Alto con las mismas características de calidad y desempeño que se tenían antes del incidente.
- Proponer y facilitar la realización de pruebas de recuperación con su respectiva información.
- Designar las funciones que sus colaboradores deban desarrollar antes y después de un desastre.
- Canalizar ante la Dirección los proyectos y gastos relacionados con el mantenimiento y preparación de la plataforma tecnológica de la entidad.
- Coordinar la ejecución de las pruebas de recuperación y actualizar el soporte de los procesos.
- Implementar los planes de recuperación de desastres tecnológicos.

Durante:

- Identificar causas de la indisponibilidad de los servicios.
- Identificar los servicios afectados.
- Comunicar a las partes interesadas los avances del cierre del incidente disruptor.

- Evaluar la eficacia de los controles y actividades realizadas para recuperar la operatividad del DIVRI

Después:

- Verificar el adecuado funcionamiento de la operación.
- Coordinar el retorno a normalidad.
- Presentar a la Dirección el reporte sobre la recuperación de operaciones.
- Verificar que el ambiente de contingencia, en caso de que aplique, continúa operando según lo establecido y que la protección permanece.

9. PREMISAS DEL PLAN DE CONTINUIDAD DE TI

El proceso TICS, ha determinado evaluar la estrategia de contingencia para los servicios tecnológicos determinados en la matriz activos de informacion_DIVRI_2025_TIC.xlsx.
De igual forma, se establece que los lineamientos del presente plan se encuentran basados en las siguientes premisas:

- Los snapshot sobre las máquinas virtuales de la DIVRI, solo se realizan cuando se solicitan al administrador, por ende, no son programados.
- Las copias de respaldo se realizan de acuerdo con el plan de copias de seguridad de la vigencia y el instrumento de infraestructura critica.
- Existe una redundancia de canales de internet con el mismo proveedor.
- Los equipos de usuarios finales, así como los servidores, cuentan con seguros contra daños, los cuales permiten solicitar nuevos equipos en caso de que estos sufran fallas irreversibles, por lo que el plan de continuidad del negocio del DIVRI se enfoca en la infraestructura tecnológica de prestación de servicios.

9.1 Centro de Cómputo

El proceso TICS, ha establecido que su esquema de recuperación de los servicios críticos tecnológicos se realizará en el mismo centro de cómputo de la Entidad y la estrategia se enfoca en la recuperación vía copias de respaldo e instalación manual de los equipos.

Es responsabilidad del proceso TICS, gestionar el mantenimiento a la plataforma tecnológica dispuesta en el Centro de Cómputo, así como las actualizaciones, reconfiguraciones o renovación que sean necesarias para mantener un servicio estable y seguro.
Cuando exista activos que presenten fallo o cuando se requiera actualización, tal necesidad se comunicará de manera inmediata por parte de los encargados de estos al responsable de la infraestructura, quien autorizará los proyectos necesarios o elevará requerimiento a la Dirección General para que sean aprobados.

9.2 Aplicaciones críticas

Resultado de aplicar un análisis de los procesos de la entidad, se concluye que se requiere un Plan de Continuidad para los equipos que soportan los servicios priorizados de tecnología. Lo anterior con base en los valores definidos en la Matriz de activos en la ruta activos de informacion_DIVRI_2025_TIC.xlsx
, que permite determinar los tiempos de recuperación y de restauración para los servicios críticos de la entidad.

9.3 Tiempos y Momentos de recuperación

La DIVRI ha establecido que los tiempos y momentos para la recuperación de los servicios (RTO y RPO) materia del alcance, deben ser iguales o inferiores a lo desplegado en la matriz de levantamiento de activos de información, en la sección de continuidad del negocio, acorde con lo valorados del activo de información y la gestión del riesgo. activos de informacion_DIVRI_2025_TIC.xlsx,
Los servicios críticos son catalogados como aquellos que tienen la clasificación del impacto en niveles Grave o Critico
Una vez se realice la recuperación de los servicios críticos/priorizados, se debe iniciar con la recuperación de los servicios no críticos, los cuales están clasificados con nivel de Impacto Marginal, Leve o Minimo

9.4 Medidas de Seguridad Efectivas para recuperación tecnológica

9.4.1 Medidas de Gobierno de seguridad

- **Evaluación y Monitoreo de Riesgos junto con análisis de amenazas y vulnerabilidades** actualizado periódicamente.
- **Monitoreo ambiental y estructural** (sensores de gases, temperatura, vibraciones, etc.).
- **Sistema de videovigilancia** con cobertura total y análisis inteligente.

- **Copias de seguridad automáticas** en servidores externos o en la nube.
- **Ciberseguridad robusta**, especialmente si se manejan datos sensibles.

9.4.2 Infraestructura Resiliente

- **Diseño antisísmico** y resistente al fuego.
- **Barreras físicas** (muros, cercas, control de accesos).
- **Protocolos de evacuación y confinamiento** claros y conocidos por todo el personal.
- **Sistemas redundantes** de energía, comunicaciones y respaldo de datos.

9.4.3 Planes de Emergencia y Continuidad

- **Plan de Continuidad de Operaciones (BCP)** y **Plan de Recuperación ante Desastres (DRP)**.
- **Simulacros regulares** con participación de todos las partes interesadas.

9.4.4 Gestión de Seguridad Física y Electrónica

- **Control de accesos biométrico o con credenciales seguras**.
- **Guardias entrenados en manejo de crisis** y primeros auxilios.
- **Sistema de alarmas** conectado con autoridades locales.

9.4.5 Coordinación Interinstitucional

- **Alianzas con la base militar cercana, bomberos, policía y defensa civil**.
- **Protocolos de comunicación rápida** en caso de emergencia.
- **Participación en redes locales de gestión del riesgo**.
- **Sistema de comunicación interna de emergencia** (radios, apps, etc.).

9.4.6 Capacitación y Cultura de Seguridad

- **Entrenamiento constante** del personal en seguridad, manejo de químicos, incendios y evacuación.
- **Campañas internas de concientización** sobre riesgos y prevención.
- **Manual de seguridad** accesible y actualizado.