APRUEBA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DE LA SUBSECRETARÍA PARA LAS FUERZAS ARMADAS.

RESOLUCION EXENTA N° 8028

Santiago, 17 octubre 2025

VISTOS:

a) DFL N°1/19.653, de 2001, del Ministerio Secretaría General de la Presidencia, que fija el texto refundido, coordinado y sistematizado de la Ley N°18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.

b) La Ley Nº19.880, que establece Bases de los Procedimientos Administrativos que rigen los actos de los órganos de la Administración del Estado.

c) DFL N°29, de 2005, del Ministerio de Hacienda, que fija texto refundido, coordinado y sistematizado de la Ley N°18.834, sobre Estatuto Administrativo.

d) La Ley Nº20.424, Estatuto Orgánico del Ministerio de Defensa Nacional.

e) La Ley N°19.799, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.

f) La Ley Nº19.628, sobre protección de la vida privada.

g) La Ley Nº21.719, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales.

h) La Ley Nº21.180, de Transformación Digital del Estado.

i) La Ley Nº21.464, modifica diversos cuerpos legales en materia de Transformación Digital del Estado.

j) La Ley Nº21.663, Marco de Ciberseguridad.

k) El Decreto Supremo N°83, de 2005, del Ministerio Secretaría General de la Presidencia, Aprueba norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos.

l) El Decreto Supremo N°164, de 2023, del Ministerio del Interior y Seguridad Pública, que aprueba Política Nacional de Ciberseguridad 2023-2028.

m) La Resolución Exenta N°8100, de 2018, que aprueba política general de seguridad de la información y revoca Resolución Exenta N°6180 de 2017, ambas de la Subsecretaría para las Fuerzas Armadas.

n) La Resolución Exenta N°8361, de 2019, de la Subsecretaría para las Fuerzas Armadas, que designa Encargado de Seguridad de la Información, Encargado de Ciberseguridad y Comité de Seguridad de la Información de la Subsecretaría para

las Fuerzas Armadas y deroga Resolución Exenta N°5952 del 04.ago.2015 y Resolución Exenta N°4412 del 22.jun.2017.

o) La Resolución N°36, de 2024, de la Contraloría General de la República, que fija normas sobre exención de toma de razón.

CONSIDERANDO:

1. Que, la revisión y análisis de la Política General de Seguridad de la Información corresponde a una tarea periódica, orientada al aseguramiento de la mejora continua del Sistema de Gestión de la Seguridad de la Información de la Subsecretaría para las Fuerzas Armadas, conforme a las buenas prácticas de gestión establecidas en las normas internacionales en la materia.

2. Que, en el marco de dicha revisión, se ha determinado la necesidad de actualizar la Política General de Seguridad de la Información vigente, a fin de fortalecer la gestión institucional y dar continuidad a las acciones de resguardo de la confidencialidad, integridad y disponibilidad de los activos de información.

3. Que, la entrada en vigor de las nuevas versiones de las normas internacionales en materia de Seguridad de la Información, en particular la norma ISO/IEC 27001:2022 y la norma ISO/IEC 27002:2022, así como su adopción oficial en Chile mediante la Norma Chilena NCh-ISO/IEC 27001:2023 y la NCh-ISO/IEC 27002:2022, exige la actualización de la Política General de Seguridad de la Información institucional, a fin de garantizar su plena alineación con los estándares actualmente reconocidos.

4. Que, la Subsecretaría para las Fuerzas Armadas debe dar cumplimiento a las disposiciones legales y reglamentarias vigentes que regulan la Seguridad de la Información en los órganos de la Administración del Estado, en especial aquellas referidas a la protección de datos personales, la seguridad de los documentos electrónicos y la prevención de delitos informáticos.

5. Que, en la gestión institucional se han realizado cambios organizacionales y tecnológicos significativos que impactan directamente en la gestión de la Seguridad de la Información, lo cual refuerza la necesidad de contar con una política actualizada y acorde a la realidad operativa actual.

6. Que, en mérito de lo expuesto, corresponde dejar sin efecto la Resolución Exenta Nº 8100, de fecha 14 de diciembre de 2018, y aprobar una nueva política General de Seguridad de la Información debidamente actualizada.

RESUELVO:

1.- APRUÉBASE la Política General de Seguridad de la Información de la Subsecretaría para las Fuerzas Armadas, la que forma parte íntegra de la presente resolución.

2.- IMPLEMÉNTESE la presente Política General de seguridad de la Información de la Subsecretaría para las Fuerzas Armadas, conforme a los roles y responsabilidades que en ella se asignan.

3.- DIFÚNDASE, la presente Política General de Seguridad de la Información a toda la comunidad funcionaria de la Subsecretaría para las Fuerzas Armadas y a terceros que interactúen de manera habitual u ocasional con esta Subsecretaría de Estado.

4.- PUBLÍQUESE en el sitio de Intranet Institucional para conocimiento de toda la comunidad funcionaria.

5.- **DÉJESE SIN EFECTO** la Resolución Exenta N°8100 de fecha 14 de diciembre de 2018, de la Subsecretaría para las Fuerzas Armadas, así como toda otra normativa anterior al 14 de diciembre de 2018, que diga relación con la política general de seguridad de la información.

Anótese, comuníquese y archívese

Firmado por
Galo Mauricio
Eidelstein
Silber
Fecha
17/10/2025
16:16:32 CLST

GALO EIDELSTEIN SILBER
SUBSECRETARIO PARA LAS FUERZAS ARMADAS

MAP/RQR/MBA/DAI//MCP/JVC

DISTRIBUCIÓN:
1. Gabinete MDN.
2. SS.FF.AA. Gabinete SS.FF.AA.
3. SS.FF.AA. Toda la Subsecretaría

Subsecretaría para las Fuerzas Armadas

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Código:	SSFFAA-SSI-CSI-POL-01
Versión:	5.0
Fecha de la versión	21-08-2025
Creado por:	Mauricio Arancibia Pino
Visado por:	Juan Vásquez Carrasco
Nivel de confidencialidad:	Uso interno

Tabla de contenido

I. DECLARACIÓN INSTITUCIONAL

La Subsecretaría para las Fuerzas Armadas establece esta política con el propósito de garantizar la **preservación de la confidencialidad, integridad y disponibilidad** de sus activos de información. A través de estos lineamientos, se promueve un entorno seguro que respalde la gestión de información crítica y la continuidad operativa de la institución.

Nota de confidencialidad

La información contenida en este documento es propiedad exclusiva de la Subsecretaría para las Fuerzas Armadas y está sujeta a políticas estrictas de confidencialidad. Su acceso, uso, reproducción o divulgación sin la debida autorización está estrictamente prohibido y podrá ser sancionado de acuerdo con las políticas internas de la Subsecretaría, así como con la legislación vigente en Chile sobre protección y seguridad de la información. Si alguna persona recibe este documento por error, le solicitamos eliminarlo de inmediato y notificarlo a la Subsecretaría para las Fuerzas Armadas a la brevedad.

II. OBJETIVOS DE LA POLÍTICA

La Política General de Seguridad de la Información establece los siguientes objetivos principales:

a) **Proteger los activos de información** mediante la implementación de medidas esenciales que resguarden su **confidencialidad, integridad y disponibilidad**, minimizando los riesgos de pérdida, mal uso o acceso no autorizado, y mitigando posibles impactos en la imagen institucional, la información sensible y la infraestructura tecnológica.

b) **Fortalecer la ciberseguridad institucional**, mediante la adopción de controles y prácticas que permitan prevenir, detectar y responder ante amenazas digitales, asegurando la continuidad de las operaciones frente a incidentes cibernéticos.

c) **Definir controles claros, eficientes y alcanzables**, que permitan gestionar la seguridad de la información de manera efectiva, en línea con las mejores prácticas y requisitos aplicables al contexto institucional.

d) **Fomentar una cultura de seguridad y ciberseguridad**, promoviendo acciones proactivas y sostenidas para el resguardo de los activos de información, a través de actividades de capacitación, difusión y sensibilización en todos los niveles de la organización.

III. DEFINICIONES

Para efectos de esta política, se adoptan las siguientes definiciones clave:

- **Activo de Información**: Todo recurso físico, digital o en la nube que contiene, procesa o respalda información crítica para la institución, como documentos, bases de datos, sistemas, hardware o software.

- **Ciberseguridad**: Conjunto de prácticas, procesos y medidas diseñadas para proteger los sistemas de información, activos digitales y redes frente a amenazas internas o externas que puedan comprometer su seguridad.
- **Confidencialidad**: Propiedad de la información que asegura que solo personas, procesos o sistemas autorizados puedan acceder a ella.
- **Disponibilidad**: Propiedad que garantiza que la información, los sistemas y servicios estén accesibles y operativos cuando sean requeridos.
- **Integridad**: Propiedad que asegura la exactitud y completitud de la información, evitando alteraciones no autorizadas en su contenido o formato.
- **Usuario Interno**: Personas que opera dentro de la institución bajo cualquier régimen contractual (planta, contrata, honorarios u otra modalidad).
- **Usuario Externo**: Personas o entidades que, en virtud de un contrato, convenio o cualquier otro tipo de relación formal, interactúa con los activos de información de la institución.
- **Vulnerabilidad**: Cualquier debilidad identificada en un sistema, procedimiento, control o infraestructura tecnológica que puede ser explotada por una amenaza para comprometer la seguridad de la información.
- **Incidente de Seguridad**: Evento no deseado o inesperado que puede afectar la confidencialidad, integridad o disponibilidad de los activos de información.
- **Política de Seguridad de la Información**: Conjunto de directrices generales definidas por la institución para proteger los activos de información y gestionar los riesgos asociados.

IV. ÁMBITO DE APLICACIÓN Y ALCANCE DE LA POLÍTICA

Esta política se aplica a toda la institución, incluyendo a las personas que forman parte de esta, bajo cualquier modalidad contractual (planta, contrata, honorarios, personal en comisión de servicio) y a todas las divisiones, departamentos, unidades, comités u otras estructuras funcionales de la Subsecretaría para las Fuerzas Armadas. Su alcance abarca los procesos, procedimientos, programas y planes relacionados con la seguridad de la información, así como todos los activos digitales, físicos y en la nube que la institución gestione o controle, sin importar su ubicación o forma de almacenamiento.

La supervisión e implementación de los procedimientos y estándares establecidos en esta política es responsabilidad del **Comité de Seguridad de la Información**, encargado de garantizar el desarrollo, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI). Este comité contará con la participación de actores clave provenientes de áreas estratégicas y transversales de la organización, asegurando una visión integral que permita abordar los desafíos asociados a la gestión de riesgos y la seguridad de la información de manera efectiva.

V. MARCO NORMATIVO

El cumplimiento de las leyes, normativas y estándares aplicables en materia de seguridad de la información y ciberseguridad es un pilar fundamental de esta política. Este marco

regula todas las actividades relacionadas con la protección de los activos de información, asegurando que los procesos institucionales se desarrollen conforme a las disposiciones legales y a las mejores prácticas reconocidas.

Esta política abarca todos los activos de información, independientemente de su formato, ubicación o método de almacenamiento, ya sea información impresa en papel, almacenada electrónicamente, transmitida por medios digitales, registrada en videos, audio o en cualquier otro soporte. Su aplicación incluye tanto los activos existentes como aquellos que puedan incorporarse en el futuro, asegurando una protección integral en línea con los requerimientos legales, normativos y contractuales aplicables a la institución.

Decreto 100	Constitución Política de la República de Chile: Capítulo 1, artículo 19, numeral 4º.- El respeto y protección a la vida privada y a la honra de la persona y su familia, y asimismo, la protección de sus datos personales.
Ley N°21.663/2024	Ley Marco de Ciberseguridad
Ley N°21.459/2022	Establece normas sobre delitos informáticos, deroga Ley N°19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest
Ley N°21.180/2022	Transformación Digital del Estado
Ley N°20.285/2008	Ley sobre acceso a la información pública
Ley N°17.336/2004	Propiedad intelectual
Ley N°19.927/2004	Modifica el código penal, el código de procedimiento penal y el código procesal penal en materia de delitos de pornografía infantil
Ley N°19.880/2003	Establece bases de los procedimientos administrativos que rigen los actos de los órganos de la administración del estado
Ley N°19.799/2002	Sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma
Ley N°19.628/1999	Sobre protección de la vida privada
DFL N°3/2021	Fija texto refundido, coordinado y sistematizado de la Ley N°19.496, que establece normas sobre protección de los derechos de los consumidores
D.S. N°164/2023	Aprueba Política Nacional de Ciberseguridad 2023-2028
D.S. N°7/2023	Establece Norma Técnica de Seguridad de la Información y Ciberseguridad conforme a la Ley N°21.180
D.S. N°273/2022	Establece obligación de reportar incidentes de Ciberseguridad
D.S. N°4/2020	Reglamento que regula la forma en que los procedimientos administrativos deberán expresarse a través de medios electrónicos, en las materias que indica, según lo dispuesto en la Ley N°21.180 sobre Transformación Digital del Estado
Resolución Exenta N°1.318/2020	Establece la Norma Técnica de Ciberseguridad para Proveedores de Servicios de Telecomunicaciones
D.S. N°83/2017	Promulga el convenio sobre la Ciberdelincuencia
D.S. N°1/2015	Aprueba norma técnica sobre sistemas y sitios web de los órganos de la administración del estado
D.S. N°533/2015	Crea el Comité Interministerial sobre Ciberseguridad

D.S. N°14/2014	Modifica Decreto N°181, de 2002, que aprueba reglamento de la ley N°19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma, y deroga los decretos que indica
D.S. N°93/2006	Aprueba norma técnica para la adopción de medidas destinadas a minimizar los efectos perjudiciales de los mensajes electrónicos masivos no solicitados recibidos en las casillas electrónicas de los órganos de la administración del estado y de sus funcionarios
D.S. N°83/2004	Aprueba norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos

VI. GESTIÓN DE RIESGOS

La gestión de riesgos en seguridad de la información es un proceso continuo y estratégico que busca identificar, evaluar y tratar amenazas que puedan comprometer la confidencialidad, integridad y disponibilidad de los activos de información. Este enfoque permite priorizar acciones para minimizar riesgos y garantizar la continuidad de las operaciones institucionales.

La institución aplicará metodologías reconocidas para evaluar los riesgos, estableciendo controles proporcionados según la criticidad y sensibilidad de los activos afectados. Las medidas adoptadas estarán alineadas con los marcos normativos vigentes y ajustadas a los cambios en el entorno tecnológico y regulatorio.

El Comité de Seguridad de la Información supervisará periódicamente la gestión de riesgos, promoviendo una mejora continua a través de revisiones regulares, monitoreo de indicadores clave y la implementación de medidas preventivas, correctivas o adaptativas cuando sea necesario.

VII. ROLES Y RESPONSABILIDADES

Para garantizar el cumplimiento de los objetivos de la Política General de Seguridad de la Información, se han definido roles y responsabilidades alineados con la estructura organizacional vigente, de acuerdo con la Ley N° 20.424 (Estatuto Orgánico del Ministerio de Defensa Nacional) y la normativa interna de la institución. Estas responsabilidades abarcan la aprobación, implementación, supervisión, actualización, difusión, cumplimiento y capacitación relacionadas con la seguridad de la información y la ciberseguridad.

1. Jefe/a del Servicio

- Aprobar la Política General de Seguridad de la Información.
- Establecer los lineamientos estratégicos para la gestión de la seguridad de la información y la ciberseguridad en la institución.

2. **Encargado/a de Seguridad de la Información**

- Actuar como asesor/a directo/a de la autoridad en materia de seguridad de la información.
- Presidir el Comité de Seguridad de la Información.
- Diseñar, gestionar y actualizar las políticas de seguridad de la información, supervisando su implementación.
- Coordinar la respuesta ante incidentes que puedan afectar los activos de información.

3. **Encargado/a de Ciberseguridad**

- Actuar como asesor/a directo/a de la autoridad en temas de ciberseguridad.
- Participar en el Comité de Seguridad de la Información.
- Gestionar análisis y planes de acción relacionados con vulnerabilidades y riesgos en ciberseguridad.
- Establecer vínculos con personas encargadas de ciberseguridad de otras entidades públicas para fomentar la cooperación y el intercambio de conocimientos.

4. **Jefaturas de División**

- Garantizar la aplicación de la política en sus respectivas áreas.
- Liderar y promover el compromiso del nivel directivo en la implementación de medidas y mejoras relacionadas con la seguridad de la información.

5. **Jefaturas de Departamento**

- Supervisar la correcta aplicación de la política por parte de las personas a su cargo.
- Promover el uso adecuado de los controles de seguridad establecidos.
- Informar cualquier incumplimiento o incidente que afecte los activos de información de la institución.

6. **Personas usuarias internas**

- Aplicar la política en el uso de sistemas y el tratamiento de la información en sus actividades diarias.
- Participar en actividades de sensibilización y capacitación para fortalecer la cultura de seguridad de la información.

7. **Personas usuarias externas**

Las personas usuarias externas que presten servicios a la institución, ya sea consultores, proveedores u otras figuras similares, estarán sujetos a los lineamientos establecidos en la Política General de Seguridad de la Información. Estas deberán:

- Cumplir con las normativas internas y estándares de seguridad de la información aplicables durante la prestación de sus servicios.
- Garantizar la protección y correcto uso de los activos de información a los que tengan acceso, evitando su divulgación o uso indebido.

- Participar en actividades de inducción y sensibilización organizadas por la institución, en caso de ser requerido.
- Informar de inmediato cualquier incidente de seguridad o vulnerabilidad detectada en el marco de sus actividades.

La institución establecerá los acuerdos y contratos necesarios para regular estas responsabilidades, asegurando la protección de los activos de información mediante cláusulas específicas de seguridad.

8. Comité de Seguridad de la Información

- Supervisar la implementación de procedimientos y controles establecidos en la política.
- Proponer estrategias y soluciones específicas para mitigar riesgos y garantizar la protección de los activos de información.
- Revisar y actualizar periódicamente la política, asegurando su difusión en la institución.
- Sensibilizar a las personas de la institución sobre la importancia de la seguridad de la información y arbitrar conflictos relacionados con esta materia.

VIII. GESTIÓN DE ACTIVOS DE INFORMACIÓN

La Subsecretaría para las Fuerzas Armadas reconoce la importancia de tratar los activos de información como recursos estratégicos esenciales para su operación y cumplimiento de objetivos. En este marco, los activos serán gestionados con un enfoque integral, garantizando que su identificación, clasificación y protección respondan a su nivel de sensibilidad, criticidad y los riesgos asociados a su uso.

Para ello, se establecerán responsabilidades claras en la administración de los activos, asegurando su resguardo frente a amenazas internas y externas. Este tratamiento incluirá la adopción de controles adecuados y adaptativos que permitan minimizar los riesgos y garantizar la continuidad operativa.

El manejo de los activos se realizará conforme a los principios establecidos en esta política, considerando las disposiciones normativas aplicables, con la flexibilidad necesaria para adaptarse a futuros requerimientos y desafíos tecnológicos. Los procedimientos específicos que detallen su gestión serán desarrollados en documentos complementarios que alineen la práctica operativa con los objetivos estratégicos de la institución.

IX. CIBERSEGURIDAD

La ciberseguridad se establece como un pilar estratégico en la protección de los sistemas, redes y activos digitales de la institución frente a amenazas internas y externas. Este enfoque abarca la implementación de medidas preventivas, reactivas y de detección que aseguren la confidencialidad, integridad y disponibilidad de la información, garantizando la continuidad operativa y la resiliencia tecnológica.

Las acciones de ciberseguridad estarán alineadas con normativas vigentes, estándares internacionales y mejores prácticas reconocidas. Estas incluirán controles adaptativos para mitigar vulnerabilidades, monitoreo continuo de los sistemas críticos, y respuestas efectivas a incidentes que puedan comprometer la seguridad de los activos digitales.

Asimismo, se promoverá la capacitación periódica de las personas de la institución para fortalecer sus competencias en materia de ciberseguridad, junto con la implementación de mecanismos de cooperación con entidades públicas y privadas para gestionar riesgos de manera coordinada y compartir conocimientos relevantes.

X. DIFUSIÓN DE LA POLÍTICA

La responsabilidad de difundir la Política General de Seguridad de la Información recae en el **Comité de Seguridad de la Información** que, a través del Encargado de Seguridad de la Información utilizará medios institucionales como el correo electrónico y la intranet para garantizar su accesibilidad y comprensión. Este comité contará con el apoyo de los/as Jefes/as de Divisiones y Departamentos para asegurar su efectiva divulgación en toda la institución.

La última versión de la política estará disponible en el apartado del **Sistema de Gestión de Seguridad de la Información** en la intranet institucional, junto con actualizaciones y otros documentos relacionados con la seguridad de la información.

Para facilitar su comprensión, se realizarán actividades periódicas de difusión, como charlas informativas dirigidas a todos los grupos relevantes, incluyendo a las personas internas y externas que interactúe con los activos de información de la institución.

XI. MEDIDAS DISCIPLINARIAS

El incumplimiento de la Política General de Seguridad de la Información será evaluado conforme a los procedimientos internos de la institución, como investigaciones sumarias u otras medidas administrativas que permitan verificar los hechos, determinar responsabilidades y aplicar las sanciones correspondientes.

Las acciones disciplinarias estarán orientadas a proteger los activos de información y garantizar la continuidad operativa, considerando la gravedad de la infracción. En el caso de las personas usuarias externas, las medidas se aplicarán según los términos contractuales establecidos.

Todas las sanciones serán ejecutadas con apego a los principios de proporcionalidad, objetividad y transparencia, promoviendo una cultura organizacional basada en la protección de la seguridad de la información

XII. EVALUACIÓN Y AUDITORÍA

La institución llevará a cabo evaluaciones periódicas y auditorías internas para garantizar la efectividad de las medidas establecidas en la Política General de Seguridad de la Información. Estas actividades permitirán verificar el cumplimiento normativo, identificar

brechas de seguridad, y proponer acciones correctivas y preventivas para fortalecer la protección de los activos de información.

Las auditorías estarán alineadas con los estándares internacionales aplicables y serán realizadas por personas internas capacitadas o entidades externas autorizadas, según corresponda. Los resultados obtenidos serán revisados por el Comité de Seguridad de la Información, que se encargará de priorizar e implementar las mejoras necesarias

XIII. ACTUALIZACIÓN DE LA POLÍTICA

La Política General de Seguridad de la Información será revisada periódicamente para garantizar su alineación con los objetivos institucionales, los marcos normativos vigentes y las mejores prácticas en materia de seguridad de la información. El **Comité de Seguridad de la Información** realizará una revisión anual del documento y propondrá las actualizaciones necesarias para reflejar cambios normativos, tecnológicos o estratégicos que impacten la gestión de la seguridad de la información.

Adicionalmente, se contempla una revisión extraordinaria de la política una vez que se publiquen los reglamentos derivados de la **Ley Marco de Ciberseguridad (Ley N° 21.663/2024)**. Este proceso permitirá adaptar las disposiciones de la política para asegurar su cumplimiento y coherencia con las nuevas exigencias legales.

Todas las modificaciones serán aprobadas siguiendo los procedimientos internos establecidos y difundidas oportunamente a todas las personas de la institución.

XIV. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS			
Versión	**Fecha**	**Autor**	**Descripción**
1.0	03.12.2012	Comité de Seguridad de la Información	Elaboración inicial
2.0	14.06.2013	Comité de Seguridad de la Información	Aplicación de formato, ámbitos, definiciones, disposiciones de la política
3.0	03.10.2016	Igor Carrasco N.	Revisión completa de la política
4.0	14.09.2017	Mauricio Arancibia P.	Aplicación de formato, cambio en los objetivos, revisión roles y responsabilidades, revisión de difusión de la política
4.1	15.09.2017	Juan Pablo Silva R.	Cambio en acciones especiales de seguridad, difusión de la política, definiciones
5.0	27.08.2025	Comité de Seguridad de la Información	Revisión completa, cambios normativos y aplicación de nueva estructura