UNISHIELD
BY UNIPAGO

# POLÍTICA DE OPERACIÓN UNISHIELD

Versión: 2.0
Clasificación: Uso Institucional
Entidad Promotora: Unipago

## 1. Introducción

La presente Política de Operación UNISHIELD establece el marco institucional, operativo y de gobernanza para el funcionamiento de UNISHIELD, como mecanismo sectorial de análisis, coordinación e intercambio de información en ciberseguridad del Sistema Dominicano de la Seguridad Social (SDSS).

Esta política tiene como objetivo asegurar que la operación de UNISHIELD se realice de forma ordenada, segura, transparente y alineada con la estrategia de ciberseguridad de UNIPAGO, la normativa nacional vigente y las mejores prácticas internacionales aplicables a ISAC y CSIRT sectoriales.

## 2. ¿Qué es UNISHIELD?

UNISHIELD es un mecanismo sectorial de análisis, coordinación e intercambio de información en ciberseguridad, impulsado por UNIPAGO, que evoluciona hacia un CSIRT sectorial del ecosistema del Sistema Dominicano de la Seguridad Social (SDSS).

UNISHIELD opera como un espacio neutral, colaborativo y confiable, orientado a fortalecer la resiliencia digital del sector, mediante la compartición responsable de información sobre ciberamenazas, riesgos e incidentes relevantes.

UNISHIELD no es un ente regulador, ni sustituye las funciones de seguridad de las entidades participantes. Su rol es informativo, coordinador y preventivo, en articulación con las autoridades nacionales de ciberseguridad y, en particular, con el CSIRT-RD.

## 3. Objetivo de la Política

Esta política tiene como objetivo:

- Establecer las reglas de operación de UNISHIELD.
- Definir roles, responsabilidades y límites de actuación.
- Garantizar la confidencialidad, integridad y disponibilidad de la información compartida.
- Promover la confianza y colaboración entre los miembros.
- Asegurar la alineación estratégica con la visión sectorial y nacional de ciberseguridad.

## 4. Alcance

Esta política aplica a:

- Las entidades miembros de UNISHIELD.
- Los Puntos de Contacto (POC) designados por cada entidad.
- El Comité de UNISHIELD.
- El Coordinador de UNISHIELD / CSIRT Sectorial.
- Proveedores, aliados y terceros que participen de forma autorizada.

## 5. Principios Rectores de Operación

La operación de UNISHIELD se rige por los siguientes principios:

- **Gradualidad:** Las capacidades y servicios se desarrollan de forma progresiva y sostenible.
- **Confianza:** El intercambio de información se fundamenta en confidencialidad, transparencia y respeto mutuo.
- **Eficiencia:** Se prioriza el aprovechamiento de capacidades existentes y mecanismos de bajo costo.
- **Alineamiento nacional:** UNISHIELD se articula con la Estrategia Nacional de Ciberseguridad y el CSIRT-RD.
- **Valor demostrable:** Toda acción debe generar un beneficio tangible para el ecosistema del SDSS.

## 6. Servicios de UNISHIELD

UNISHIELD ofrece servicios de carácter informativo y colaborativo, entre ellos:

- Intercambio de alertas de ciberseguridad.
- Difusión de tendencias, riesgos e indicadores de compromiso (IoC).
- Coordinación informativa ante incidentes de impacto sectorial.
- Boletines y comunicaciones de concientización.

### 6.1 Exclusiones

UNISHIELD no:

- Audita, certifica o supervisa a los participantes.
- Representa legalmente a las entidades.

## 7. Comunidad Atendida

UNISHIELD estructura su comunidad en tres niveles de relación, con alcance y servicios diferenciados:

**Nivel 1 – Infraestructura Central**

- Sistemas y plataformas operadas por UNIPAGO para el SDSS.
- Coordinación directa y prioritaria.

**Nivel 2 – Accionistas del Ecosistema**

- Administradoras de Riesgos de Salud (ARS) y Administradoras de Fondos de Pensiones (AFP).
- Intercambio estructurado de información, alertas sectoriales e inteligencia.

**Nivel 3 – Ecosistema Extendido**

- Entidadades reguladores del SDSS, PSS y otros actores relevantes.
- Coordinación informativa y alertas de carácter general.

## 8. Membresía y Participación

La participación en UNISHIELD es voluntaria y requiere:

- Solicitud formal de adhesión.
- Designación de un Punto de Contacto (POC).
- Aceptación de esta política, código de conducta y de el acuerdo de confidencialidad aplicable.

## 9. Manejo de la Información – TLP

Toda la información compartida en UNISHIELD se clasifica conforme al Traffic Light Protocol (TLP):

- **TLP:RED** – Uso estrictamente limitado a destinatarios específicos.
- **TLP:AMBER** / AMBER+STRICT – Uso interno controlado.
- **TLP:GREEN** – Compartición dentro de la comunidad UNISHIELD.
- **TLP:CLEAR** – Información pública.

Si no se indica clasificación, la información se considera **TLP:AMBER** por defecto.

## 10. Canales Autorizados

La información se compartirá exclusivamente a través de canales oficiales autorizados, tales como:

- Correo institucional seguro.
- Plataforma de Ciberinteligencia (CTI).
- Canales colaborativos restringidos.
- Portal web UNISHIELD (solo información TLP:CLEAR).

El acceso es personal, autorizado e intransferible.

## 11. Gobernanza

UNISHIELD cuenta con un modelo de gobernanza que distingue:

- **Nivel Estratégico:** Comité de UNISHIELD, responsable de lineamientos, políticas y decisiones estratégicas.
- **Nivel Operativo:** Coordinador de UNISHIELD / CSIRT Sectorial, responsable de la ejecución diaria.

Las decisiones de carácter público, estratégico o de impacto sectorial requieren validación del Comité.

## 12. Escalamiento y Coordinación

El escalamiento de información se determina en función de:

- La clasificación TLP.
- El impacto potencial sectorial.

Cuando corresponda, UNISHIELD coordinará informativamente con el CSIRT-RD, conforme a los protocolos establecidos.

## 13. Seguridad de la Información

Todos los participantes deberán:

- Proteger la información recibida.
- Aplicar controles adecuados de acceso.
- Reportar cualquier uso indebido o incidente relacionado.

El incumplimiento podrá conllevar la suspensión o terminación de la participación.

## 14. Divulgación Responsable

La información compartida no deberá:

- Exponer datos personales o sensibles.
- Generar daño reputacional injustificado.
- Utilizarse con fines comerciales, legales o maliciosos.

## 15. Cumplimiento y Revisión

- Esta política es de cumplimiento obligatorio.
- Será revisada al menos una vez cada 2 años o ante cambios relevantes.
- El Comité y el Coordinador velarán por su aplicación.

**UNISHIELD** promueve una comunidad basada en la confianza, colaboración y responsabilidad, para fortalecer la ciberseguridad del Sistema Dominicano de la Seguridad Social.