UNISHIELD
BY UNIPAGO

CÓDIGO DE CONDUCTA Y ÉTICA

1. Introducción

El presente Código de Conducta y Ética establece los principios, valores y normas que rigen el comportamiento de todas las personas y organizaciones que participan en el Centro de Intercambio y Análisis de Información (ISAC – UNISHIELD).

El ISAC se fundamenta en la confianza, la colaboración segura, la confidencialidad y el intercambio responsable de información de ciberseguridad, con el objetivo de fortalecer la resiliencia del ecosistema digital del sector.

Este Código busca garantizar que todas las interacciones se desarrollen en un entorno de respeto, integridad, responsabilidad compartida y cumplimiento normativo, promoviendo el intercambio oportuno de inteligencia sin comprometer la reputación, privacidad o información sensible de los participantes.

2. Propósito

Este Código tiene como propósito:

- Establecer normas claras de conducta ética y profesional para los miembros del ISAC – UNISHIELD.
- Garantizar el uso responsable, seguro y legítimo de la información compartida.
- Promover un ambiente de confianza, cooperación y defensa colectiva.
- Proteger la confidencialidad, integridad y correcto uso de la información intercambiada.
- Asegurar el cumplimiento de las leyes, regulaciones y buenas prácticas aplicables.

3. Alcance

Este Código aplica a:

- Organizaciones miembros del ISAC – UNISHIELD.
- Representantes designados por las organizaciones participantes.
- Directivos, personal operativo y colaboradores del ISAC.
- Proveedores, contratistas o terceros autorizados.
- Invitados y asistentes a reuniones, foros, talleres o plataformas del ISAC.

Aplica a todas las interacciones realizadas a través de:

- Plataformas de intercambio de información.
- Reuniones técnicas y grupos de trabajo.
- Eventos, talleres, foros y cumbres.
- Comunicaciones electrónicas.
- Espacios colaborativos virtuales o presenciales.

4. Principios Éticos y de Conducta

Los participantes del ISAC deberán regirse por los siguientes principios:

4.1 Confianza
La confianza es la base del intercambio de información. Los miembros deberán actuar con integridad, cumplir los compromisos asumidos, respetar las políticas de privacidad, confidencialidad y manejo de información, y fomentar relaciones basadas en reciprocidad, igualdad y respeto.

4.2 Confidencialidad y Seguridad
Toda información compartida deberá manejarse con el máximo nivel de protección, aplicando controles adecuados y respetando los esquemas de clasificación definidos por el ISAC.

4.3 No Atribución
La información compartida dentro del ISAC no deberá atribuirse a la organización fuente sin autorización expresa. Este principio fomenta la transparencia y facilita la divulgación temprana de amenazas.

4.4 Responsabilidad
Los miembros son responsables del uso adecuado de la información recibida y deberán utilizarla exclusivamente para fines legítimos de ciberseguridad, gestión de riesgos y resiliencia institucional.

4.5 Colaboración Activa

Se promueve una cultura de cooperación voluntaria que permita:

- Compartir amenazas, incidentes, indicadores de compromiso y aprendizajes.
- Participar en la detección temprana y respuesta coordinada.
- Fortalecer la resiliencia del ecosistema digital.

4.6 Respeto e Integridad
Los participantes deberán mantener un comportamiento profesional y respetuoso, evitando cualquier forma de discriminación, acoso, intimidación o conducta inapropiada, y compartir información veraz y no manipulada.

5. Uso Responsable de la Información

Los miembros del ISAC se comprometen a:

- Utilizar la información compartida únicamente para fines de seguridad y gestión de riesgos.
- Respetar las clasificaciones de información establecidas.
- Proteger la confidencialidad de la información recibida.
- No divulgar información a terceros sin autorización expresa del emisor o del ISAC.
- Aplicar medidas razonables para proteger la información dentro de sus organizaciones.

El uso indebido de la información constituye una violación grave de este Código.

6. Clasificación y Manejo de Información (TLP)

El ISAC utiliza el Traffic Light Protocol (TLP) para clasificar la información:

- **TLP:RED** – Información altamente sensible, compartida solo con destinatarios específicos.
- **TLP:AMBER** – Información de uso interno limitado dentro de la organización receptora.
- **TLP:GREEN** – Información compartible dentro de la comunidad del sector.
- **TLP:CLEAR** – Información que puede hacerse pública.

Los miembros deberán respetar estrictamente las restricciones de distribución asociadas a cada nivel.

7. Conducta en Reuniones y Plataformas

Durante su participación en actividades del ISAC, los miembros deberán:

- Mantener discusiones profesionales y orientadas a la seguridad.
- Contribuir de forma constructiva al intercambio de conocimiento.
- Respetar las opiniones y participación de otros miembros.
- Evitar la divulgación de información sensible fuera de los canales autorizados.

No se permitirá el uso de los espacios del ISAC para:

- Promoción comercial, marketing o ventas no autorizadas.
- Competencia desleal.
- Difusión de información no relacionada con ciberseguridad.
- Actividades que afecten la confianza o reputación de la comunidad.

8. Propiedad Intelectual

- No se podrá utilizar, copiar o distribuir propiedad intelectual del ISAC – UNISHIELD o de terceros sin la debida autorización.

9. Conflictos de Interés

Los participantes deberán declarar cualquier situación que pueda representar un conflicto de interés y gestionarlo de manera transparente para no afectar la confianza entre los miembros.

10. Cumplimiento Legal y Normativo

Las actividades del ISAC deberán cumplir con:

- Las leyes y regulaciones nacionales aplicables.
- Normativas de protección de datos personales.
- Regulaciones sectoriales.
- Políticas internas del ISAC y de las organizaciones miembros.

El ISAC no podrá utilizarse para actividades contrarias a la ley o a principios éticos.

11. Conductas Prohibidas

Se consideran conductas prohibidas, entre otras:

- Acoso, discriminación o intimidación.
- Divulgación no autorizada de información o datos personales.
- Compartir credenciales o accesos no autorizados.
- Publicación de malware, exploits o contenido malicioso.
- Uso indebido de información de terceros.

12. Reporte de Incumplimientos

Cualquier posible infracción a este Código deberá ser reportada a través de los canales oficiales del ISAC – UNISHIELD.

Los reportes serán tratados con confidencialidad y evaluados de forma objetiva.

13. Medidas y Consecuencias

Las violaciones a este Código podrán resultar en:

- Advertencia formal.
- Restricción o suspensión temporal de acceso.
- Prohibición permanente de participación.
- Notificación a la organización miembro correspondiente.
- Acciones legales, cuando aplique.

La medida dependerá de la gravedad e impacto de la infracción.

14. Gobierno y Supervisión

El ISAC – UNISHIELD mantiene una estructura de gobierno conformada por un Comité de Gestión y un Coordinador, responsables de supervisar el cumplimiento de este Código.

15. Revisión del Código

Este Código será revisado periódicamente para asegurar su alineación con:

- Buenas prácticas internacionales de intercambio de inteligencia.
- Evolución del panorama de amenazas.
- Cambios legales, regulatorios u operativos.

16. Aceptación

La participación en el ISAC – UNISHIELD implica la lectura, comprensión y aceptación plena de este Código de Conducta y Ética, así como el compromiso de contribuir activamente a un entorno de confianza, colaboración y seguridad.