	Digital Partner (DIPA) & Information Security Officer (ISO)
Reporta a:	Como ISO: Director de país (para informes de gestión) CISO / ISM-T (para temas técnicos) Como DIPA: Al /a la LFA directamente
Diputado:	--

1. Antecedentes

Usted es responsable de todos los asuntos relacionados con la transformación digital y la seguridad de la información dentro de su área de responsabilidad. Usted sirve como punto de contacto central para la gerencia y el personal en temas relacionados con la gestión de la información, la seguridad de TI y la protección de datos, tanto para los aspectos organizativos internos como para la infraestructura digital local.

Como socio digital (DIPA), proporciona orientación técnica a los equipos y garantiza la calidad de los resultados en los procesos digitales. Facilita una comunicación clara de objetivos, condiciones y limitaciones, y desempeña un papel activo en el desarrollo y fortalecimiento de la red digital de la organización. Apoya a los usuarios locales en la introducción y el uso de nuevos sistemas digitales, proporciona orientación sobre futuras soluciones tecnológicas y promueve la colaboración con la sede. Además, coordina y responde a las solicitudes dentro de su equipo, lo que garantiza un procesamiento oportuno y eficiente, al tiempo que contribuye al intercambio de conocimientos y la documentación.

Como responsable de seguridad de la información (ISO), usted es responsable de implementar y mantener el Sistema de Gestión de Seguridad de la Información (ISMS por sus siglas en inglés) de acuerdo con ISO/IEC 27001: 2022, Este sistema tiene como objetivo proteger toda la información valiosa procesada por la organización en todo el mundo.

En este rol, usted sirve como punto focal para la gestión local de la seguridad de la información, asegurando la implementación de políticas, controles y evaluaciones de riesgos. Trabaja en estrecha colaboración con el Director de Seguridad de la Información (CISO) y el equipo de ISMT, que proporcionan liderazgo técnico global, mientras que la supervisión disciplinaria es proporcionada por el nivel de gestión local.

El/la ISO también colabora con profesionales de TI, socios de digitalización (DIPA), jefes de unidades y la gerencia de la oficina de país, asegurando una estrecha coordinación entre los procesos digitales y las medidas de seguridad de la información. Es importante tener en cuenta que, para evitar conflictos de intereses, el rol ISO no se puede desempeñar simultáneamente con los puestos de Profesional de TI, Jefe de Unidad de TI.

Contribuye a la mejora continua de los procesos digitales y de seguridad de la información, desempeñando un papel activo en el avance de la transformación digital y protegiendo los activos de información de la organización.

2. Requisitos y funciones DIPA

- **Conocimiento de procesos:** Conocer y hacer seguimiento a los procesos digitalizados y documentados dentro de la oficina, identificar las necesidades de los procesos que aún son analógicos y proponer mejoras organizativas.
- **Cumplimiento y gestión de la información**: Brindar asesoría independiente de sistemas sobre el manejo conforme (PuR y legislación aplicable) de la información sujeta a conservación, estructuras de archivo, almacenamiento, archivado y gestión de permisos.
- **Asesoría digital:** Brindar orientación en la interfaz con los socios de la GIZ, en coordinación con las áreas técnicas de la sede, sobre el uso y desarrollo de herramientas digitales específicas.
- **Supervisión de procesos**: Monitorear los procesos digitalizados y proponer ajustes a flujos de trabajo existentes.
- **Integración y apoyo**: Garantizar que la transformación digital esté plenamente integrada en las operaciones de la oficina y cuente con recursos adecuados.
- **Desarrollo de capacidades**: Participar en actividades de formación y fortalecimiento de competencias digitales de acuerdo con las directrices de la GIZ.

3. Requisitos y funciones ISO

- **Independencia**: Reportar directamente al/la Director/a de País y al/la LFA .
- **Apoyo organizativo:** Contar con recursos y presupuesto adecuados para implementar eficazmente las políticas de seguridad.
- **Roles definidos**: Los roles y responsabilidades deben estar claramente establecidos y comunicados por la dirección local.
- **Integración**: Asegurar que la seguridad de la información esté integrada en todos los procesos (Finanzas, RR.HH., Contrataciones, TI, etc.).
- **Auditorías internas**: Realizar auditorías internas de cumplimiento de políticas y procedimientos de seguridad.
- **Informes**: Presentar reportes periódicos al/la la Director/a de País, al/la LFA y al CISO/ISM-T sobre el estado de la seguridad de la información.
- **Desarrollo profesional**: Mantener y actualizar competencias mediante formación y experiencia continua.
- **Sensibilización**: Fortalecer las iniciativas de concienciación y programas de seguridad de la información en la oficina.

4. Responsabilidades – DIPA e ISO

4.1 DIPA

- Actuar como punto focal de transformación digital.
- Promover la digitalización de procesos y recomendar mejoras.
- Alinear la implementación de sistemas digitales con los estándares globales de la GIZ.
- Brindar asesoría en gestión de datos, archivado y gobernanza de la información.
- Promover la alfabetización digital y la formación del personal.
- Coordinar con TI y la sede sobre sistemas, herramientas y procesos.
- Asegurar la documentación y comunicación de actividades digitales y buenas prácticas.
- Contribuir a la integración de la transformación digital en todas las áreas operativas y de proyectos.

4.2 ISO

- Ser el punto focal de la seguridad de la información.

- Implementar, monitorear y mejorar el ISMS (por sus siglas en inglés) conforme a ISO/IEC 27001:2022.
- Coordinar políticas, normas y prácticas de gestión de riesgos.
- Realizar auditorías internas y recomendar medidas correctivas.
- Gestionar e informar incidentes de seguridad.
- Presentar informes periódicos al/la Director/a de País, al/la LFA y al CISO/ISM-T.
- Colaborar con profesionales de TI, DIPA, SRMO y equipos de proyecto.
- Promover campañas de concienciación y formación en seguridad.
- Garantizar la confidencialidad, integridad y disponibilidad de la información.
- Apoyar procesos de certificación y mejora continua.

5. Tareas

Además de las responsabilidades mencionadas anteriormente, la/el ISO – DIPA tiene las siguientes tareas:

5.1 ISO

- Implementar, coordinar y mejorar continuamente el SGSI local.
- Coordinar, elaborar y revisar políticas y subconceptos de seguridad.
- Planificar y coordinar medidas de seguridad de la información con HQ-ISMT, TI, Protección de Datos y SRMO.
- Supervisar la efectividad del programa de seguridad y proponer mejoras.
- Apoyar la gestión de incidentes, incluyendo evaluación, comunicación y seguimiento.
- Asesorar y reportar a la dirección sobre el desempeño del SGSI.
- Desarrollar planes de auditoría interna y apoyar auditorías externas.
- Ser punto de contacto ante no conformidades.

5.2 DIPA

- Promover la transferencia de conocimientos mediante capacitaciones y talleres.
- Mantenerse actualizado sobre soluciones digitales y coordinar con DIGITS/Global IT Services.
- Difundir buenas prácticas y aspectos clave de la transformación digital.
- Actuar como multiplicador/a de herramientas y soluciones digitales (por ejemplo, LSS S4GIZ).
- Crear contenido para comunicación multicanal y capacitación del personal nuevo.
- Asesorar a los usuarios sobre herramientas, sistemas de gestión documental (M365 y Sharepoint) y cumplimiento normativo.
- Ser el primer punto de contacto para temas básicos de clasificación, etiquetado y protección de datos.
- Participar activamente en los canales de comunicación con la sede sobre protección de datos.
- Traducir las recomendaciones de DIGITS en materiales comprensibles para usuarios finales.
- DIPA reporta sólo al/la LFA

Desempeñar las tareas adicionales que le asigne su superior jerárquico, de acuerdo con las necesidades operativas y organizacionales.

6. Cualificaciones

El/la titular del puesto deberá contar con:

- 5 años de experiencia laboral en una organización internacional con un mínimo de 1000 empleados, familiarizado con las estructuras y procesos organizacionales
- Título universitario en sistemas de información, informática, administración o áreas afines.
- Conocimientos sólidos en seguridad de la información, ISO/IEC 27001:2022, gestión de riesgos, vulnerabilidades y auditorías.
- Experiencia en procesos de digitalización, gestión documental y protección de datos.
- Habilidades de comunicación, asesoría y trabajo en equipo.
- Alto grado de integridad, discreción y pensamiento analítico.
- Actitud proactiva, orientación a resultados y compromiso con la mejora continua.
- Dominio de inglés C1, opcional alemán

En coherencia con nuestra política de inclusión, estrategia de género y nuestro compromiso con la diversidad, valoramos la multiplicidad de perspectivas y el enriquecimiento que aportan equipos diversos. En GIZ Colombia fomentamos activamente la participación en todas las etapas de los procesos de selección y contratación de mujeres, personas pertenecientes a la comunidad LGTBIQ+, personas con discapacidad y personas con pertenencia étnica y les invitamos a enviar sus postulaciones.

Las personas interesadas están invitadas a enviar su hoja de vida en español, junto con la carta de motivación y aspiración salarial, a HR-GIZColombia@giz.de hasta el día 19 de enero de 2026