EOI.IAIG.2019.02
Clasificación de la información

1. Authority: Esta Instrucción de la Oficina Ejecutiva (EOI) es promulgada por el Director del Grupo de Auditoría Interna e Investigaciones (IAIG) en virtud de la Directiva de la Oficina Ejecutiva sobre privacidad y seguridad de la información (ref. EOD.ED.2019.02) de conformidad con la delegación de autoridad del Director Ejecutivo.

2. Purpose: El propósito de esta Instrucción de la Oficina Ejecutiva es proporcionar instrucciones sobre cómo clasificar los datos de UNOPS en función de su grado de confidencialidad y cuantificar el nivel de protección de datos necesario.

3. Effective Date: Esta Instrucción de la Oficina Ejecutiva debe entrar en vigor inmediatamente.

4. Promulgation Date: 14 May 2022

[signature redacted]

Paul Lucas

Director, IAIG

Table of contents

- 1. Introducción (see page 1)
- 2. Nota sobre las actividades de documentación (research) (see page 2)
- 3. Niveles de clasificación (see page 3)
    - Públicos (see page 3)
    - No clasificados (see page 3)
    - Confidenciales (see page 3)
    - Estrictamente confidenciales (see page 4)
- 4. Resolución de conflictos entre la presente Instrucción de la Oficina Ejecutiva y otras normativas (see page 5)

1. Introducción

1.1 Los datos de UNOPS son información generada por o para UNOPS, de su propiedad o que se encuentra en su poder, y que está relacionada con las actividades de la organización.

1.2 Los datos de UNOPS pueden presentarse en cualquier formato (es decir, electrónico o en papel) e incluyen, entre otros, todos los datos estratégicos, tácticos, operacionales, administrativos y de actividades de documentación (research), así como la infraestructura de computación y el código de programa que sustentan la actividad de UNOPS.

1.3 Para proteger eficazmente estos datos, debemos disponer de un vocabulario que nos permita describirlos y cuantificar el nivel de protección necesario. La presente Instrucción de la Oficina Ejecutiva define cuatro categorías en las que se pueden clasificar todos los datos de UNOPS:

- Públicos
- No clasificados

- Confidenciales
- Estrictamente confidenciales

1.4 Los datos de UNOPS que se consideren públicos podrán divulgarse a cualquier persona, independientemente de su vinculación con UNOPS. El resto de datos de UNOPS se consideran información potencialmente sensible y deben protegerse adecuadamente; además, solo podrán divulgarse con cautela, de conformidad con la Instrucción Operacional de UNOPS sobre divulgación de información (ref. OI.LG.2019.02). En la sección 3 de este documento se ofrecen definiciones y ejemplos de cada una de las cuatro categorías.

1.5 Las distintas unidades y departamentos de UNOPS disponen de una gran variedad de tipos de documentos y datos. Aunque no es necesario que todos los documentos y datos se marquen físicamente como "Públicos", "No clasificados", "Confidenciales" o "Estrictamente confidenciales", cada unidad o departamento debe valorar en cuál de las categorías anteriores se encuadran sus documentos y datos, teniendo en cuenta el daño que podría causarse a las personas o a UNOPS en caso de divulgación involuntaria, modificación o pérdida. El Oficial Jefe de Seguridad de la Información (CISO) colaborará en este proceso para garantizar la coherencia en UNOPS. A la hora de abordar la clasificación de sus datos, cada departamento debe sopesar el riesgo que supone una divulgación involuntaria, modificación o pérdida frente a la necesidad de fomentar el debate abierto, mejorar la eficiencia y promover los objetivos de UNOPS en materia de creación y difusión del conocimiento. Los departamentos deben prestar especial atención a la protección de la información personal sensible, como los números de identificación nacional, los números del permiso de conducir y los números de cuentas bancarias, cuya divulgación podría suponer un riesgo de suplantación de identidad.

1.6 Es necesario resaltar que cierta información podría clasificarse de forma diferente en distintos momentos. Por ejemplo, los datos que en su momento se consideraron "Confidenciales" pueden pasar a ser "Públicos" una vez que se hayan divulgado de forma adecuada. Todas las personas que tengan acceso a los datos de UNOPS deben actuar con buen criterio al gestionar información sensible y solicitar orientación a la dirección cuando sea necesario.

2. Nota sobre las actividades de documentación (research)

2.1 UNOPS está comprometida con la transparencia en las actividades de documentación (research): el libre acceso de todas las personas interesadas a los datos subyacentes, a los procesos y a los resultados finales de las actividades de documentación. En general, las actividades de documentación que se lleven a cabo en UNOPS deben publicarse de forma amplia y abierta y ponerse a disposición del público mediante una amplia difusión o publicación de los resultados de las mismas. Los datos de las actividades de documentación se consideran, por regla general, datos públicos, salvo que existan requisitos específicos para mantener su confidencialidad, como cuando la persona a cargo de las actividades de documentación está obligado/a a proteger la información confidencial de un Gobierno colaborador o una organización asociada, o cuando los datos se refieren a sujetos humanos.

3. Niveles de clasificación

Públicos

3.1 Los datos públicos son aquella información que puede divulgarse a cualquier persona, independientemente de su relación con UNOPS. La clasificación "Públicos" no se limita a los datos que son de interés público o destinados a su difusión entre el público; dicha clasificación se aplica a los datos que no requieren ningún nivel de protección frente a su divulgación. Aunque puede ser necesario proteger los documentos originales (fuente) frente a modificaciones no autorizadas, los datos públicos pueden compartirse con un público amplio, tanto dentro como fuera de la comunidad, y no es necesario tomar medidas para impedir su difusión.

3.2 Entre los ejemplos de datos públicos se incluyen: comunicados de prensa, información de directorios, formularios de solicitud y otra información general que se difunde de forma abierta. El tipo de información que un departamento de la organización decide publicar en su página web es un buen ejemplo de datos públicos.

No clasificados

3.3 Los datos no clasificados son información que puede ser sensible y que no está destinada a ser compartida con el público. Por regla general, los datos internos no deben divulgarse fuera de UNOPS sin el permiso de la persona o el grupo que los haya elaborado. Es responsabilidad de la persona titular de los datos clasificarlos como "No clasificados" cuando proceda. En caso de duda sobre si la información es de carácter no clasificado o sobre cómo tratar los datos de carácter no clasificado, se debe poner en contacto con Seguridad de la Información o con la persona responsable del departamento.

3.4 Entre los ejemplos de datos no clasificados se incluyen algunos memorandos, correspondencia y actas de reuniones; listas de contactos que contienen información que no es de dominio público; y documentación sobre procedimientos que debe mantenerse en privado.

Confidenciales

3.5 Los datos confidenciales son aquella información que, de llegar a manos de personas no autorizadas, podría afectar negativamente a las personas o a la actividad de UNOPS. Esta clasificación también incluye los datos que UNOPS tiene la obligación de mantener confidenciales, ya sea por ley o en virtud de un acuerdo de confidencialidad con un tercero, como un proveedor. Esta información debe protegerse contra su divulgación o modificación no autorizadas. Los datos confidenciales solo deben utilizarse cuando sea necesario con fines comerciales y deben protegerse tanto mientras se utilizan como cuando se almacenan o se transmiten.

3.6 Cualquier divulgación no autorizada o pérdida de datos confidenciales deberá comunicarse a la persona responsable del departamento correspondiente. El/La jefe/a de departamento deberá decidir

si debe notificar la divulgación no autorizada o la pérdida de datos confidenciales al CISO a través de la dirección ciso@unops.org.

3.7 Entre los ejemplos de datos confidenciales se incluyen:

- Información sujeta a los marcos jurídicos en materia de privacidad y protección de datos en todas las operaciones de UNOPS y en otras jurisdicciones (por ejemplo, el RGPD de la UE, la HIPAA, etc.).
- La información de carácter personal que se nos ha confiado y que no sea de carácter estrictamente confidencial, como la información relativa a oficiales públicos, donantes actuales, donantes potenciales o hijos/as de empleados/as actuales o antiguos/as.
- El identificador de UNOPS (CSID), cuando se almacena junto con otros datos identificativos, como el nombre o la dirección de correo electrónico.
- Registros financieros.
- Información laboral individual, incluyendo el salario, las prestaciones y las evaluaciones de desempeño del personal actual, antiguo y potencial.
- Información protegida por el secreto profesional.
- Información que está sujeta a un acuerdo de confidencialidad.

Estrictamente confidenciales

3.8 Los datos estrictamente confidenciales incluyen cualquier información que UNOPS tenga la obligación contractual o fiduciaria de proteger de la forma más rigrosa. En algunos casos, la divulgación no autorizada o la pérdida de estos datos obligaría a UNOPS a notificarlo a la persona afectada y a las autoridades estatales o federales. En algunos casos, la modificación de los datos requeriría informar a la persona afectada.

3.9 Las obligaciones de UNOPS dependerán de los datos concretos y del contrato o la legislación aplicables. Los estándares mínimos de seguridad establecen un nivel básico para todos los datos estrictamente confidenciales. Los sistemas y procesos destinados a proteger los siguientes tipos de datos deben cumplir con ese nivel mínimo:

- Información de salud que permita identificar a una persona.
- Información de carácter personal, incluyendo el nombre de una persona, así como su número de identificación nacional, número de permiso de conducir, datos del pasaporte o número de cuenta bancaria.
- Datos no cifrados que se utilizan para autenticar o autorizar a las personas a utilizar recursos electrónicos, como contraseñas, claves y otros tokens electrónicos.
- "Datos sobre antecedentes penales" que puedan recopilarse como parte de un formulario de solicitud o de una verificación de antecedentes.

3.10 Existen requisitos más estrictos para algunos tipos de datos estrictamente confidenciales. Las personas que trabajen con los siguientes tipos de datos deben cumplir las políticas de UNOPS que regulan dichos tipos de datos y consultar con Seguridad de la Información para asegurarse de que cumplen todos los requisitos correspondientes a su tipo de datos:

- Información de salud protegida. La información de salud protegida incluye toda la información de salud que permita identificar a una persona, incluidos los datos demográficos, los historiales

médicos, los resultados de pruebas, la información sobre seguros y cualquier otro dato que se utilice para identificar a un/a paciente o para prestar servicios de salud o cobertura de salud.
- Números de cuentas financieras sujetos al estándar de seguridad de los datos de la industria de tarjetas de pago, que regula la forma en que se acepta, utiliza y almacena la información de las tarjetas de crédito.
- Información sobre asociaciones de la Unión Europea y los países del Grupo de Estados de África, el Caribe y el Pacífico (ACP).
- Datos clasificados del Gobierno de los Estados Unidos de América.

3.11 Los datos estrictamente confidenciales solo deben utilizarse cuando no exista ninguna alternativa y deben protegerse con sumo cuidado. Toda divulgación no autorizada, modificación no autorizada o pérdida de datos estrictamente confidenciales debe comunicarse al CISO a través de la dirección ciso@unops.org.

4. Resolución de conflictos entre la presente Instrucción de la Oficina Ejecutiva y otras normativas

4.1 Algunos datos pueden estar sujetos a requisitos específicos de protección en virtud de un contrato o un subsidio, o de conformidad con una ley o normativa que no se describe en el presente documento. En esas circunstancias, deben aplicarse los requisitos de protección más estrictos. Para más información se ruega ponerse en contacto con el CISO a través de la dirección de correo electrónico ciso@unops.org.

[Nota: En caso de discrepancia entre el documento en inglés y la traducción, prevalecerán las disposiciones del documento en inglés].