

## DIRECTIVA GENERAL N°001 -2024-PRODUCE-SG

### DISPOSICIONES PARA LA ADMINISTRACIÓN DE ACCESO A LAS PLATAFORMAS INFORMÁTICAS Y SISTEMAS DE INFORMACIÓN DEL MINISTERIO DE LA PRODUCCIÓN

Formulada por: Oficina General de Tecnologías de la Información (OGTI)

#### I. OBJETIVO

Establecer las disposiciones para la administración de accesos a las plataformas informáticas y sistemas de información del Ministerio de la Producción (en adelante, PRODUCE).

#### II. FINALIDAD

Fortalecer los medios de autenticación de acceso seguro a las plataformas informáticas y sistemas de información, que asegure la confidencialidad, integridad y disponibilidad de la información de PRODUCE.

#### III. ALCANCE

Las disposiciones contenidas en la presente Directiva General son de obligatorio cumplimiento para los usuarios de los órganos, unidades orgánicas y programas de PRODUCE.

#### IV. BASE LEGAL

- 4.1 Ley N° 29158, Ley Orgánica del Poder Ejecutivo, y sus modificatorias.
- 4.2 Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado.
- 4.3 Decreto Legislativo N° 1047, Decreto Legislativo que aprueba la Ley de Organización y Funciones del Ministerio de la Producción.
- 4.4 Decreto Supremo N° 066-2001-PCM, que aprueba los "Lineamientos de Políticas Generales para promover la masificación del acceso a Internet en el Perú".
- 4.5 Decreto Supremo N° 002-2017-PRODUCE y su modificatoria, que aprueba el Reglamento de Organización y Funciones del Ministerio de la Producción.
- 4.6 Resolución de Contraloría N° 320-2006-CG, Aprueban Normas de Control Interno.
- 4.7 Resolución Secretarial N° 00026-2022-PRODUCE, que aprueba la Directiva General N° 002-2022-PRODUCE-SG denominada "Disposiciones para la formulación, aprobación y modificación de Directivas en el Ministerio de la Producción".
- 4.8 Resolución Secretarial N° 041-2018-PRODUCE, que aprueba la Directiva General N° 002-2018-PRODUCE-SG "Disposiciones que regulan la administración y el uso del correo electrónico institucional en el Ministerio de la Producción".
- 4.9 Resolución Directoral N° 022-2022-INACAL/DN, Aprueban Normas Técnicas Peruanas sobre turismo, acuicultura y otros.
- 4.10 Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD, Establecen la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las entidades públicas.

#### V. DISPOSICIONES GENERALES

##### 5.1 Abreviaturas

- ✓ OGTI: Oficina General de Tecnologías de la Información.
- ✓ OGA: Oficina General de Administración.
- ✓ MFA: Multi Factor Authentication.



## 5.2 Definiciones

- a) **Autenticación:** Proceso mediante el cual se comprueba la identidad de un usuario.
- b) **Contraseña:** Cadena de caracteres que un usuario o servicio utiliza para verificar su identidad con el objetivo de tener acceso a un servicio, sistema informático, estación de trabajo, punto de red, entre otros.
- c) **Contratista:** Persona natural y/o jurídica autorizada para realizar actividades o labores que requiere un órgano, unidad orgánica o programa de PRODUCE para el desarrollo y cumplimiento de sus funciones y fines.
- d) **Cuenta de Usuario:** Es un perfil que tiene asignado un conjunto de privilegios mediante el cual se puede tener acceso a recursos informáticos como el servicio de internet, VPN, entre otros.
- e) **Mesa de Ayuda:** Equipo de recursos humanos y tecnológicos para atender solicitudes de servicios de manera integral, utilizando las Tecnologías de Información y Comunicaciones (TIC).
- f) **Multi Factor Authentication:** La autenticación multifactor (MFA) es un proceso de registro en varios pasos que requiere que los usuarios ingresen algo más de información que simplemente una contraseña, agrega una capa de protección al proceso de inicio de sesión.
- g) **Plataforma Informática:** Es precisamente el basamento, ya sea de hardware o software, sobre el cual un programa puede ejecutarse. Ejemplos típicos incluyen: arquitectura de hardware, sistema operativo, lenguajes de programación y sus librerías de tiempo de ejecución.
- h) **Servidor:** Un servidor es un recurso informático que almacena, distribuye y suministra información. Los servidores funcionan basándose en el modelo "cliente-servidor". El cliente puede ser tanto un ordenador como una plataforma informática que requiere información del servidor para funcionar. Por tanto, un servidor ofrecerá la información demandada por el cliente siempre y cuando el cliente esté autorizado. Los servidores pueden ser físicos o virtuales Existen servidores de Desarrollo, Calidad y Prueba.
- i) **Símbolo especial:** Se considera como símbolo especial a los siguientes caracteres: #, \$, %, @, \*, etc.
- j) **Sistemas de Información:** Es un conjunto de elementos orientados a la administración de datos e información organizada para ser usados y son generados para cubrir un objeto o necesidad de PRODUCE.
- k) **Usuario:** Persona que tiene vínculo laboral o contractual con la entidad y utiliza los bienes, servicios informáticos y de telecomunicaciones proporcionados por PRODUCE.
- l) **Usuario de red:** Es una cuenta de usuario que tiene un conjunto de permisos y de recursos asignados como parte de un dominio institucional. Cada usuario de red este asignado a un trabajador y/o plataforma informática.





- m) **Usuario Privilegiado:** Usuario que dentro de una plataforma informática o sistema de información posee los más altos privilegios que le permiten realizar actividades sin restricciones.
- n) **Usuario administrador local del servidor:** Usuario que cuenta con privilegios y acceso a funciones y configuraciones en un servidor. Pueden instalar y desinstalar programas, configurar permisos de archivos y carpetas, administrar usuarios y grupos, y realizar otras tareas importantes en el sistema.
- o) **VPN:** Red privada virtual, una conexión VPN permite a un usuario de red acceder de forma segura a recursos informáticos dentro de una red local a través de internet.

### 5.3 Actores del procedimiento

5.3.1 La OGTI, en su calidad de órgano de apoyo de PRODUCE, responsable de implementar el gobierno electrónico; planificar, diseñar e implementar soluciones de tecnologías de información del Ministerio; realizar la innovación y el desarrollo tecnológico, así como del soporte y las telecomunicaciones, realiza lo siguiente:

- 1) Controla el proceso de otorgamiento de cuentas de acceso, en el marco de la presente Directiva.
- 2) Controla el proceso de otorgamiento de accesos, validando las solicitudes recibidas y atendiendo aquellas debidamente autorizadas por la oficina solicitante.
- 3) Realiza el seguimiento a la aplicación de los lineamientos contenidos en la presente Directiva General.

5.3.2 El funcionario responsable del órgano, unidad orgánica o programa de PRODUCE, es responsable de lo siguiente:

- 1) De los accesos requeridos a sus usuarios y los cuales, están debidamente autorizados.
- 2) De la aplicación de los lineamientos contenidos en la presente Directiva General.

5.4 La presente Directiva regula el correcto uso de contraseñas para el acceso a las plataformas informáticas y/o sistemas de información de PRODUCE.

5.5 La OGTI administra adecuadamente los accesos de los usuarios a las plataformas informáticas y/o sistemas de información de PRODUCE, tomando las acciones que sean necesarias para asegurar la confiabilidad del mismo, en función a los recursos y capacidades disponibles.

5.6 La administración realizada por la OGTI no implica ningún control sobre el contenido de la información proveniente del acceso a las cuentas de usuarios o de quien la genere; por cuanto, el usuario que accede a las plataformas informáticas y/o sistemas de información de PRODUCE, es responsable por cualquier información o acción efectuada a la que se haya podido acceder por medio de su cuenta y contraseña de acceso, inclusive de aquellas que se realicen durante su ausencia.

5.7 El funcionario responsable del órgano, unidad orgánica o programa de PRODUCE deberá informar mediante documento formal (memorando) dirigido a la OGTI o a



través del correo electrónico [mesadeayuda@produce.gob.pe](mailto:mesadeayuda@produce.gob.pe) el término del vínculo laboral o contractual de los usuarios para que se proceda con el retiro de los accesos a las diferentes plataformas informáticas y/o sistemas de información.

- 5.8 Se prohíbe al usuario, bajo responsabilidad, compartir o exponer la contraseña con otras personas, independientemente de la jerarquía del solicitante. Las cuentas son intransferibles y de uso personal.

## VI. DISPOSICIONES ESPECÍFICAS

### 6.1 Contraseña de acceso a la red

- 6.1.1 Toda cuenta de usuario debe ser creada y otorgada únicamente a usuarios de PRODUCE para el cumplimiento de sus funciones a solicitud del funcionario responsable del órgano, unidad orgánica o programa de PRODUCE y con la autorización adicional del Director general de la OGTI. Estas cuentas deberán ser creadas de acuerdo a lo establecido en la Directiva General "Disposiciones que regulan la administración y el uso del correo electrónico institucional en el Ministerio de la Producción".
- 6.1.2 Toda cuenta debe tener asociada obligatoriamente una contraseña de acceso, exigida en el proceso de autenticación, con ocho (08) caracteres como mínimo, de los que debe contener al menos una letra en mayúscula, una letra en minúscula, un número y un símbolo especial, mientras el sistema lo permita.
- 6.1.3 El acceso de los equipos informáticos a la red de PRODUCE, tendrá como mecanismo de seguridad lógico, la utilización de un usuario de red y contraseña.
- 6.1.4 La OGTI brindará la primera contraseña para que los usuarios puedan ingresar a la red institucional de PRODUCE, dicha contraseña deberá ser cambiada por el usuario al realizar el primer ingreso.
- 6.1.5 La contraseña deberá ser cambiada periódicamente, pudiendo ser modificada en cualquier momento por el usuario. La vigencia máxima de la contraseña es de tres (03) meses.
- 6.1.6 Recién después de utilizar cinco (05) contraseñas diferentes se puede reutilizar una contraseña con un tiempo de antigüedad mayor a doce (12) meses salvo mejor parecer.
- 6.1.7 La contraseña de acceso a la red se bloqueará después de cinco (05) intentos de acceso fallido. El desbloqueo es automático después de cinco (05) minutos.
- 6.1.8 La contraseña de usuario de red y el correo electrónico están sincronizadas; por lo que, si el usuario cambia su contraseña de acceso a la red, automáticamente también se cambiara su contraseña de todas las herramientas colaborativas de Microsoft Office 365.
- 6.1.9 Se deberá revisar periódicamente los usuarios con acceso a la red institucional.





**6.2 Contraseña de acceso a las plataformas informáticas y/o sistemas de información**

- 6.2.1 Para el acceso de las plataformas informáticas y/o sistemas de información de PRODUCE deberán de iniciar sesión mediante el MFA o equivalente, siempre que la tecnología lo permita.
- 6.2.2 Se creará una contraseña temporal, la misma que se solicitará ser cambiada la primera vez que el usuario acceda a las plataformas informáticas y/o sistemas de información.
- 6.2.3 La contraseña deberá de tener como mínimo una longitud de ocho (08) caracteres hasta un máximo de quince (15) caracteres, de los que debe contener al menos una letra en mayúscula, una letra en minúscula, un número y un símbolo especial.
- 6.2.4 Los accesos a las diferentes plataformas informáticas y/o sistemas de información de PRODUCE, deben ser solicitados por el funcionario responsable del órgano, unidad orgánica o programa de PRODUCE mediante documento formal (memorando) dirigido a la OGTI.
- 6.2.5 La contraseña deberá ser cambiada periódicamente, pudiendo ser modificada en cualquier momento por el usuario. La vigencia máxima de la contraseña es de tres (03) meses, luego de dicho periodo la plataforma informática y/o sistema de información deberá solicitar el cambio obligatorio de la contraseña.
- 6.2.6 Recién después de utilizar cinco (05) contraseñas diferentes se puede reutilizar una contraseña con un tiempo de antigüedad mayor a doce (12) meses salvo mejor parecer.
- 6.2.7 El acceso a la plataforma informática y/o sistemas de información se bloqueará después de cinco (05) intentos de acceso fallido.
- 6.2.8 Ante el bloqueo de la plataforma informática y/o sistema de información, el usuario externo deberá ingresar a la indicación de "olvido su contraseña" y seguir los pasos indicados, y el usuario interno deberá de comunicarse a Mesa de Ayuda.
- 6.2.9 En el caso de utilizar contraseñas o PiN's (Personal Identification Numbers) generados automáticamente, el programa o algoritmo de generación deberá estar específicamente protegido.
- 6.2.10 La conexión sólo permitirá al usuario acceder a las plataformas informáticas y/o sistemas de información a los cuales está autorizado según lo solicitado por el funcionario responsable del órgano, unidad orgánica o programa de PRODUCE mediante documento formal (memorando) dirigido a la OGTI y/o solicitud por medio de formulario digital través del correo electrónico [mesadeayuda@produce.gob.pe](mailto:mesadeayuda@produce.gob.pe).
- 6.2.11 Las plataformas informáticas y/o sistemas de información, siempre que la tecnología lo permita, deberá controlar los terminales inactivos de forma que proceda la desconexión automática luego de diez (10) minutos de permanecer en inactividad.



- 6.2.12 Las plataformas informáticas y/o sistemas de información, siempre que la tecnología lo permita, deberá controlar la conectividad de los usuarios, por lo que no deberá permitir que un usuario se encuentre conectado en dos equipos diferentes al mismo tiempo.
- 6.2.13 Se deberá revisar periódicamente los derechos de acceso, los perfiles en los servicios de tratamiento de información y la vigencia de las credenciales.
- 6.2.14 Los usuarios ante cualquier incidente presentado con los accesos a las plataformas informáticas y/o sistemas de información deberán comunicarlo inmediatamente a la OGTI a través del correo electrónico [mesadeayuda@produce.gob.pe](mailto:mesadeayuda@produce.gob.pe) y/o formulario digital para el reporte de incidentes disponible en el servicio de mesa de ayuda de la institución.

### 6.3 Contraseña de acceso a los Servidores (Windows, Linux, etc.)

- 6.3.1 El acceso a los Servidores (Windows, Linux, etc.) de PRODUCE, deberá ser únicamente por el personal encargado de la administración de servidores y servicios de la OGTI. De requerir el ingreso a los servidores de PRODUCE, de algún otro personal, este deberá ser solicitado con un adecuado sustento y con la autorización del Director General de la OGTI.
- 6.3.2 El acceso a los servidores de los ambientes de Desarrollo, estará restringido solamente a los programadores que lo requieran, únicamente mientras se encuentre vigente el proyecto en que se encuentren laborando. La solicitud de este acceso debe ser confirmada por el coordinador del equipo de Desarrollo de la OGTI, el cual deberá comunicar el momento en que dicho acceso debe ser desactivado.
- 6.3.3 La contraseña deberá de tener como mínimo una longitud de diez (10) caracteres hasta un máximo de quince (15) caracteres, de los que debe contener al menos una letra en mayúscula, una letra en minúscula, un número y un símbolo especial.
- 6.3.4 La contraseña deberá ser cambiadas por el usuario administrador local del servidor como máximo cada seis (06) meses, pudiendo ser modificada en cualquier momento por mantenimiento preventivo, cuando haya cambio de administrador de servidores o por indicación del Director General de la OGTI.
- 6.3.5 El acceso a los servidores se bloqueará después de tres (03) intentos de acceso fallido.
- 6.3.6 No se deberá realizar la reutilización de una contraseña anterior.
- 6.3.7 Se deberá revisar periódicamente los derechos de acceso y la vigencia de las credenciales.

### 6.4 Contraseña de acceso a las Bases de Datos

- 6.4.1 El acceso a las Bases de Datos del ambiente de Calidad y Producción de PRODUCE, estará restringido únicamente a los administradores de la Base de Datos de la OGTI y solo en modo de consulta por el personal que cuente con un adecuado sustento, con la autorización del jefe de proyecto y del encargado del área funcional de Soluciones TI de la OGTI. Para los





casos en que el contrato del usuario solicitante no incluya un acuerdo de confidencialidad de Base de Datos, deberá llenar un formulario con el mismo.

- 6.4.2 El acceso a la Base de Datos deberá de tener como mecanismo de seguridad lógica, la utilización de una contraseña.
- 6.4.3 Las contraseñas deberán de tener como mínimo una longitud de diez (10) caracteres hasta un máximo de quince (15) caracteres, de los que debe contener al menos una letra en mayúscula, una letra en minúscula, un número y un símbolo especial.
- 6.4.4 La contraseña deberá ser cambiada como máximo cada cuatro (04) meses, pudiendo ser modificada en cualquier momento por mantenimiento preventivo, cuando haya cambio de administrador de Base de Datos o por indicación del director de la OGTI.
- 6.4.5 La contraseña de acceso a la Base de Datos se bloqueará después de cinco (05) intentos de acceso fallido.
- 6.4.6 No se deberá realizar la reutilización de una contraseña anterior.
- 6.4.7 Se deberá revisar periódicamente los derechos de acceso y la vigencia de las credenciales.

#### 6.5 Contraseña de acceso a la VPN

- 6.5.1 El acceso a la VPN de PRODUCE, debe ser solicitado por el funcionario responsable del órgano, unidad orgánica o programa de PRODUCE mediante documento formal (memorando), con el adecuado sustento, dirigido a la OGTI.
- 6.5.2 El acceso a la VPN deberá de tener como mecanismo de seguridad lógica, la utilización de una contraseña, la cual será habilitada por la OGTI.
- 6.5.3 El acceso a la VPN es mediante las credenciales del usuario de red (usuario y contraseña).
- 6.5.4 Las contraseñas deberán de tener como mínimo una longitud de ocho (08) caracteres hasta un máximo de quince (15) caracteres, de los que debe contener al menos una letra en mayúscula, una letra en minúscula, un número y un símbolo especial.
- 6.5.5 La contraseña de acceso a la VPN se bloqueará después de cinco (05) intentos de acceso fallido. El desbloqueo es automático después de cinco (05) minutos.
- 6.5.6 Se deberá revisar periódicamente los derechos de acceso y la vigencia de las credenciales.



#### 6.6 Contraseña de acceso a equipos de comunicaciones

- 6.6.1 El acceso a los equipos de comunicaciones de PRODUCE deberá ser únicamente por el personal de la OGTI que cuente con la autorización del Director General de la OGTI.



- 6.6.2 El acceso a los equipos de comunicaciones deberá de tener como mecanismo de seguridad lógica, la utilización de una contraseña.
- 6.6.3 El mecanismo de seguridad lógica para acceso a los equipos de comunicaciones deberá ser de dos tipos, uno deberá ser el acceso mediante credenciales locales (nombre de usuario y contraseña) establecida en la base de datos del equipo de comunicaciones y el otro deberá ser el acceso mediante credenciales de dominio establecida a través del directorio activo de PRODUCE.
- 6.6.4 Las contraseñas locales deberán de tener como mínimo una longitud de diez (10) caracteres hasta un máximo de quince (15) caracteres, de los que debe contener al menos una letra en mayúscula, una letra en minúscula, un número y un símbolo especial.
- 6.6.5 Las contraseñas locales deberán ser cambiadas como máximo cada cinco (05) meses, pudiendo ser modificada en cualquier momento por mantenimiento preventivo, cuando haya cambio de administrador de redes o por indicación del director de la OGTI.
- 6.6.6 La contraseña de acceso a los equipos de comunicaciones se bloqueará después de tres (03) intentos de acceso fallido, debiendo notificar (mediante correo electrónico o algún otro medio) al administrador de redes a fin de identificar la causa y realizar la acción correctiva.
- 6.6.7 No se deberá realizar la reutilización de una contraseña anterior.
- 6.6.8 Se deberá revisar periódicamente los derechos de acceso y la vigencia de las credenciales.
- 6.7 Contraseña de acceso a equipos de seguridad perimetral y de interconexión**
- 6.7.1 El acceso a los equipos de seguridad perimetral de PRODUCE, deberá ser únicamente por el personal de la OGTI que cuente con la autorización del Director General de la OGTI.
- 6.7.2 El acceso a los equipos de seguridad perimetral deberá de tener como mecanismo de seguridad lógica, la utilización de una contraseña.
- 6.7.3 Las contraseñas deberán de tener como mínimo una longitud de diez (10) caracteres hasta un máximo de quince (15) caracteres, de los que debe contener al menos una letra en mayúscula, una letra en minúscula, un número y un símbolo especial.
- 6.7.4 La contraseña deberá ser cambiada como máximo cada cinco (05) meses, pudiendo ser modificada en cualquier momento por mantenimiento preventivo, cuando haya cambio de administrador de seguridad informática o por indicación del director de la OGTI.
- 6.7.5 La contraseña de acceso a los equipos de comunicaciones y seguridad perimetral se bloqueará después de tres (03) intentos de acceso fallido.
- 6.7.6 No se deberá realizar la reutilización de una contraseña anterior.
- 6.7.7 Se deberá revisar periódicamente los derechos de acceso y la vigencia de las credenciales.





## 6.8 Administración de accesos

- 6.8.1 El usuario solo podrá acceder a las plataformas informáticas y/o sistemas de información a los cuales se encuentre debidamente autorizado, de conformidad con los requerimientos efectuados por el funcionario responsable del órgano, unidad orgánica o programa de PRODUCE.
- 6.8.2 Se debe autenticar a todos los usuarios antes que éstos accedan a las plataformas informáticas y/o sistemas de información asignados, en caso no haya sido debidamente autenticado se restringirá totalmente el acceso.
- 6.8.3 En la medida que las plataformas informáticas y/o sistemas de información lo permitan, los intentos infructuosos de conexión se deberán contabilizar, estableciéndose hasta un máximo de cinco (05) intentos para proceder al bloqueo del usuario inutilizando su conexión por cinco (05) minutos, luego el usuario se desbloquea automáticamente. Estos intentos infructuosos deberán ser registrados como eventos de seguridad.
- 6.8.4 En la medida que las plataformas informáticas y/o sistemas de información lo permitan, los intentos infructuosos de conexión se deberán contabilizar, estableciéndose hasta un máximo de cinco (05) intentos para proceder al bloqueo del usuario inutilizando su conexión por cinco (05) minutos, luego el usuario se desbloquea mediante un correo al titular del acceso y/o uso de PIN mediante SMS.
- 6.8.5 Los usuarios son los únicos responsables de la información y el contenido que envíen mediante el uso de la cuenta de usuario.
- 6.8.6 El usuario debe desconectarse al término de su sesión. Asimismo, siempre que la tecnología lo permita, el sistema deberá controlar los terminales inactivos de forma que proceda a su desconexión automática luego de cinco (5) minutos de permanecer sin actividad.
- 6.8.7 El usuario deberá cambiar las contraseñas de acceso iniciales que les han sido asignadas la primera vez que ingresan.
- 6.8.8 El acceso a las funciones de administración de las plataformas informáticas y/o sistemas de información (usuario privilegiado) deberán estar restringidos únicamente al personal autorizado. En estos casos, en la medida que las herramientas disponibles lo permitan, se debe tener un control más detallado del acceso a las plataformas informáticas y/o sistemas de información mediante dichas cuentas.
- 6.8.9 El usuario al identificar cualquier incidente o sospecha de que otro usuario está utilizando sus contraseñas de acceso deberá proceder con el cambio de su contraseña de acceso y reportar inmediatamente a la OGTI a través del correo electrónico [mesadeayuda@produce.gob.pe](mailto:mesadeayuda@produce.gob.pe) y/o formulario digital para el reporte de incidentes disponible en el servicio de mesa de ayuda de la institución.
- 6.8.10 Todo usuario que identifique el uso indebido de cuentas y contraseñas de acceso de otros usuarios por parte de terceros, con o sin su conocimiento, deberá reportar inmediatamente a la OGTI a través del correo electrónico [mesadeayuda@produce.gob.pe](mailto:mesadeayuda@produce.gob.pe) y/o formulario digital para el reporte de incidentes disponible en el servicio de mesa de ayuda de la institución.



## 6.9 Auditoría y revisión de las solicitudes de acceso a usuarios

- 6.9.1 La OGTI debe verificar cada solicitud de acceso antes que la misma sea atendida, monitorear los accesos y las actividades realizadas por los usuarios con el objetivo de identificar actividades sospechosas que pudieran evidenciar un uso inadecuado de los privilegios asignados.
- 6.9.2 La OGTI debe verificar mediante un mecanismo de registro de eventos (logs) el acceso a las plataformas informáticas y/o sistemas de información. Este mecanismo debe permitir recopilar datos y estadísticas que faciliten el monitoreo del acceso a los distintos servicios mediante el uso de credenciales.

## VII. RESPONSABILIDADES

- 7.1. Los órganos, unidades orgánicas y programas de PRODUCE, son responsables de la aplicación de las disposiciones contenidas en la presente Directiva General.
- 7.2. La OGTI es responsable de realizar el seguimiento a la aplicación de las disposiciones contenidas en la presente Directiva General.

## VIII. DISPOSICIONES COMPLEMENTARIAS

- 8.1 Para la contratación de los contratistas, la OGA debe establecer una cláusula de confidencialidad y responsabilidad que garantice el uso adecuado de los accesos a las plataformas informáticas y/o sistemas de información otorgadas, siendo responsables de las consecuencias que podrían generar un mal uso del acceso otorgado, acorde con lo dispuesto con la normatividad de la materia.
- 8.2 Los aspectos no contemplados en la presente Directiva General, serán resueltos por la OGTI, en el marco de la normatividad vigente sobre la materia.

