RESOLUCIÓN DIRECTORAL

Nº 023-2017-OTASS/DE

Lima, 13 de junio de 2017

Vistos, el Informe N° 53-2017-OTASS-OA-Hbustamante y el Memorándum N° 564-2017-OTASS/OA de la Oficina de Administración y el Informe N° 56-2017-OTASS/OPP de la Oficina de Planeamiento y Presupuesto;

CONSIDERANDO:

Que, de conformidad con el Decreto Legislativo N° 1280, Ley Marco de la Gestión y Prestación de los Servicios de Saneamiento, el Organismo Técnico de la Administración de los Servicios de Saneamiento - OTASS, en adelante OTASS, es el organismo público técnico especializado adscrito al Ministerio de Vivienda, Construcción y Saneamiento, con personería jurídica de derecho público interno, con autonomía funcional, económica, financiera y administrativa, con competencia a nivel nacional; el cual desarrolla su competencia en concordancia con la política general, objetivos, planes, programas y lineamientos normativos establecidos por el Ente Rector;

Que, la Norma Técnica Peruana NTP-ISO/IEC 27001:2008 EDI. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. Normativa Interna, en adelante la Norma Técnica, es el instrumento que especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de las organizaciones; así como establece los requisitos para la evaluación y tratamiento de los riesgos de seguridad de la información orientados a las necesidades de dichas organizaciones;

Que, los literales p) y q) del artículo 21 del Reglamento de Organización y Funciones – ROF del OTASS, aprobado por Decreto Supremo N° 017-2014-VIVIENDA, disponen que la Oficina de Administración tiene, entre otras, la función de gestionar las tecnologías de la información y comunicación, brindar el soporte técnico necesario a las distintas áreas del OTASS y usuarios externos, así como administrar y velar por la seguridad de la infraestructura y los servicios de comunicación del OTASS;

Que, en el marco de las funciones señaladas en el considerando precedente, mediante Informe N° 53-2017-OTASS-OA-Hbustamante y Memorándum N° 564-2017-OTASS/OA, la Oficina de Administración propone la aprobación de la "Directiva de Control de Acceso a los Recursos y Servicios de Tecnología de la Información y Medidas de Seguridad", la cual se encuentra alineada a la Norma Técnica y tiene por objeto definir y establecer las normas para el otorgamiento de acceso y utilización de los recursos y servicios de tecnología de la información que provee la Oficina de Administración a las unidades orgánicas del OTASS y la aplicación de las medidas de seguridad de la información respectivas;

Que, con Informe N° 56-2017-OTASS/OPP, la Oficina de Planeamiento y Presupuesto emite opinión técnica favorable al proyecto de "Directiva de Control de Acceso a los Recursos y Servicios de Tecnología de la Información y Medidas de Seguridad";

Que, con Resolución de Secretaría General N° 001-2016-OTASS/SG, se aprobó la Directiva N° 001-2016-OTASS "Directiva para la formulación, trámite, aprobación y actualización de directivas internas de gestión administrativa del OTASS", la cual tiene por objeto establecer criterios uniformes para la formulación, trámite, aprobación y actualización de directivas internas relacionadas a la gestión administrativa del OTASS;

Que, en tal sentido corresponde aprobar la "Directiva de Control de Acceso a los Recursos y Servicios de Tecnología de la Información y Medidas de Seguridad" propuesta por la Oficina de Administración;

Con el visado de la Secretaría General, la Oficina de Administración y la Oficina de Planeamiento y Presupuesto;

De conformidad con lo dispuesto en el artículo 11 del Reglamento de Organización y Funciones del OTASS, aprobado mediante Decreto Supremo N° 017-2014-VIVIENDA y la Norma Técnica Peruana NTP-ISO/IEC 27001:2008 EDI. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. Normativa Interna;

SE RESUELVE:

Artículo 1.- Aprobar la Directiva N° 006-2017-OTASS/DE "Directiva de Control de Acceso a los Recursos y Servicios de Tecnología de la Información y Medidas de Seguridad", la misma que en anexo forma parte integrante de la presente resolución.

Artículo 2.- Disponer la publicación de la presente Resolución en la página web del OTASS (www.otass.gob.pe).

Regístrese y comuníquese.

FERNANDO LACA BARRERA
Director Ejecutivo
Organismo Técnico de la Administración
de los Servicios de Saneamiento

DIRECTIVA Nº 006 -2017-OTASS/DE

DIRECTIVA DE CONTROL DE ACCESO A LOS RECURSOS Y SERVICIOS DE TECNOLOGÍA DE LA INFORMACIÓN Y MEDIDAS DE SEGURIDAD

I. OBJETIVOS

Definir y establecer las normas para el otorgamiento de acceso y utilización de los recursos y servicios de tecnología de la información que provee la Oficina de Administración a las unidades orgánicas del Organismo Técnico de la Administración de los Servicios de Saneamiento – OTASS; y la aplicación de las medidas de seguridad de la información respectivas.

II. FINALIDAD

Brindar los recursos y servicios de tecnología de la información a los trabajadores del Organismo Técnico de la Administración de los Servicios de Saneamiento – OTASS, en el momento oportuno, asegurando su disponibilidad y operatividad.

III. BASE LEGAL

3.1 Ley N° 30045, artículo 3°, Ley de Modernización de los Servicios de Saneamiento.

3.2 Decreto Legislativo N° 1280, Decreto Legislativo que aprueba la Ley Marco de la Gestión y Prestación de los Servicios de Saneamiento.

3.3 Decreto Supremo N° 013-2016-VIVIENDA, Reglamento de la Ley de Modernización de los Servicios de Saneamiento.

3.4 Decreto Supremo N° 017-2014-VIVIENDA, Reglamento de Organización y Funciones - ROF del Organismo Técnico de la Administración de los Servicios de Saneamiento - OTASS.

3.5 Resolución de Contraloría General N° 320-2006-CG, Normas de Control Interno.

3.6 Resolución Ministerial N° 004-2016-PCM, Uso obligatorio de la Norma Técnica Peruana *"NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición"*, en todas las entidades integrantes del Sistema Nacional de Informática.

IV. ALCANCE

La presente Directiva es de aplicación de todas las Unidades Orgánicas que utilizan los recursos y servicios de tecnologías de la información que provee el OTASS.

V. DISPOSICIONES GENERALES

5.1 DEFINICIONES

a) RIESGO: Proximidad o posibilidad de un daño, peligro, amenaza, contingencia, emergencia, urgencia.

b) SEGURIDAD DE LA INFORMACIÓN: Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que en forma no autorizada, sea

accidental o intencionalmente, puedan ser modificados, destruidos o divulgados, así como la preservación de otras características como la autenticidad, no rechazo, responsabilidad y confiabilidad

c) DELITOS: Se puede citar fraudes, falsificación, venta de información.

d) PRIVACIDAD: Se define como el derecho que tienen los individuos y organizaciones para determinar, ellos mismos, a quién, cuándo y qué información referente a ellos serán difundidas o transmitidas a otros.

e) INTEGRIDAD: Se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema. El concepto de integridad abarca la precisión y la fiabilidad de los datos, así como la discreción que se debe tener con ellos.

f) DATOS: Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos. Los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y bases de datos, texto (colección de palabras), hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), video (secuencia de tramas), otros.

g) BASE DE DATOS: Una base de datos es un conjunto de datos organizados, entre los cuales existe una correlación y que además, están almacenados con criterios independientes de los programas que los utilizan.

h) ACCESO: Es la recuperación o grabación de datos que han sido almacenados en un sistema de computación. Cuando se consulta a una base de datos, los datos son primero recuperados hacia la computadora y luego transmitidos a la pantalla del terminal.

i) ATAQUE: Término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático o intento de obtener de modo no autorizado la información confiada a una computadora.

j) ATAQUE ACTIVO: Acción iniciada por una persona que amenaza con interferir el funcionamiento adecuado de una computadora, o hace que se difunda de modo no autorizado información confiada a una computadora personal. Ejemplo: El borrado intencional de archivos, la copia no autorizada de datos o la introducción de un virus diseñado para interferir el funcionamiento de la computadora.

k) ATAQUE PASIVO: Intento de obtener información o recursos de una computadora personal sin interferir con su funcionamiento, como espionaje electrónico, telefónico o la intercepción de una red. Todo esto puede dar información importante sobre el sistema, así como permitir la aproximación de los datos que contiene.

l) AMENAZA: Causa potencial de un incidente no deseado que pueda interferir con el funcionamiento adecuado de una computadora personal o sistema informático, así como causar la difusión no autorizada de información confiada en las mismas. Ejemplo: Fallas de suministro eléctrico, virus, saboteadores o usuarios descuidados.

m) INCIDENTE: Cuando se produce un ataque o se materializa una amenaza, se tiene un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de borrado de un archivo protegido. Tiene una gran probabilidad de comprometer las operaciones del negocio y de amenazar la seguridad de la información.

n) GOLPE (BREACH): Es una violación con éxito de las medidas de seguridad, como el robo de información, el borrado de archivos de datos valiosos, el robo de equipos, PC, entre otros.

o) USUARIO FINAL: Es la persona que tiene una vinculación con la Entidad y que utiliza los equipos y servicios informáticos ofrecidos por la misma.

p) RED: El conjunto de computadoras y otros equipos interconectados, que comparten información, recursos y servicios informáticos.

VI. DISPOSICIONES ESPECIFICAS

6.1 ACCESO A LOS SISTEMAS INFORMÁTICOS

La Oficina de Administración a través del Coordinador de Informática, proporcionará los accesos a los usuarios de acuerdo a las funciones que realizan y las características del entorno en el que trabajan, y que han sido debidamente solicitados por el Jefe / Director de la Unidad Orgánica a la que pertenecen. Los accesos que pueden otorgar son los siguientes:

a) Acceso a equipos informáticos para los usuarios.
b) Acceso a los sistemas de la entidad (sistemas externos adquiridos a proveedores o sistemas propios desarrollados por el OTASS).
c) Acceso a la base de datos (base de datos corporativa u otras bases de datos que utilizan las unidades orgánicas del OTASS).
d) Acceso a la red, correo electrónico, internet, carpetas compartidas, entre otros.

6.2 ADMINISTRACIÓN DE ACCESOS DE USUARIOS

6.2.1 Registro y anulación de cuentas de usuarios:

a) Cada Jefe / Director, será responsable de solicitar a la Oficina de Administración, a través del Coordinador de Informática, la creación de una cuenta de usuario de los recursos informáticos para el personal nuevo de la entidad, vía hoja de coordinación, la misma que deberá precisar el perfil de usuario requerido, es decir, las características necesarias para la elaboración de sus funciones, nivel de acceso a internet u otros. (Anexo 01).
b) La Oficina de Administración, a través del Coordinador de Informática deberá evaluar las solicitudes correspondientes a fin de dar respuesta a ellas en un plazo no mayor a veinticuatro (24) horas. En caso de aprobarlas, deberá proporcionar la cuenta de usuario, con su respectiva contraseña, para acceso a los recursos solicitados, junto con una relación de todos los derechos de accesos que poseen para la conformidad del usuario; asimismo el usuario final deberá firmar el Acta de Confidencialidad (Anexo 02). Las contraseñas de acceso a los equipos informáticos deberán tener una cadena mínima de 8 caracteres. El cambio de contraseña es responsabilidad del usuario y debe ser efectuada con una periodicidad de 90 días calendarios; asimismo lo podrá actualizar en cualquier otro momento, que por temas de seguridad considere necesario.
c) En caso de rechazar la solicitud, se deberá indicar los motivos de esta decisión y brindar recomendaciones para una correcta asignación del perfil al nuevo usuario. La atención a solicitudes rechazadas deberá darse en un periodo no mayor a veinticuatro (24) horas.
d) El Coordinador de Recursos Humanos de la Oficina de Administración deberá comunicar al Coordinador de Informática, el cese y/o los movimientos del personal, inmediatamente después de haberse producido a fin de que el Coordinador de Informática efectúe el mantenimiento de los sistemas de administración de usuarios dentro de las veinticuatro (24) horas siguientes. Los derechos de acceso para todos los usuarios de los sistemas informáticos serán removidos a la culminación del vínculo laboral, en caso de cambio de unidad orgánica se deberá ajustar los permisos y perfiles según corresponda

6.2.2 Administración de contraseñas de usuario:

a) Los usuarios son responsables del cambio de contraseña de sus cuentas, la cual deberá realizarse al ser recibidas y con una periodicidad de 90 días calendarios; asimismo, deberán mantener secretas las contraseñas asignadas y evitar guardarlas en papel, archivos u otros dispositivos. Bajo ningún concepto está permitido compartir cuentas de usuarios con otros trabajadores, bajo responsabilidad.
b) Las contraseñas serán entregadas, por seguridad, de manera personal a cada usuario, previa verificación de la identidad del usuario, con una relación de los derechos otorgados y un compromiso para no compartir su contraseña a otros usuarios, dicha entrega será recibida y firmada en señal de conformidad (Anexo 01).
c) En caso algún usuario olvide su clave de acceso, la solicitará al Coordinador de Informática mediante correo electrónico a la cuenta informatica@otass.gob.pe asimismo el usuario al recibir su nueva clave de acceso deberá modificarla.

6.2.3 Administración de contraseñas críticas:

Para el caso de las contraseñas de los servidores y base de datos se deberá realizar lo siguiente:

Claves de acceso a los servidores del Centro de Datos del OTASS:

La Oficina de Administración a través del Coordinador de Informática deberá actualizar periódicamente las claves de acceso para el ingreso a los servidores que son administrados por el OTASS que se encuentran en su Centro de Datos, las cuales se deberán efectuar con una periodicidad de seis (06) meses, dentro de los primeros quince (15) días hábiles de cada periodo semestral del año; asimismo se deberá actualizar en cualquier otro momento que se considere necesario previa evaluación e informe técnico por parte del Coordinador de Informática, como en el caso de la ocurrencia del cese o cambio de unidad orgánica del trabajador que se le hizo entrega de la última clave actualizada, para lo cual se procederá de la siguiente manera:

a) La Oficina de Administración a través del Coordinador de Informática, deberá:

- Coordinar el cambio de la clave de acceso a los servidores, la misma que no deberá repetirse con ninguna clave anterior utilizada, una vez recibida la nueva clave las mantendrá en custodia en un sobre lacrado hasta el próximo cambio y/o para la posterior entrega al personal asignado a esta función.
- Entregar al especialista responsable de la administración del Centro de Datos del OTASS, las claves de acceso a los servidores en un sobre lacrado a través de un documento para que realice el cambio respectivo. Asimismo, dicho personal deberá firmar un acuerdo de confidencialidad en el cual se compromete a no revelar, comentar, suministrar o transferir de cualquier forma, tal información a terceros, puesto que esta clave permite el acceso a datos e información confidencial y privilegiada (Anexo 03).
- Como medida de contingencia el Jefe de la Oficina de Administración deberá mantener en custodia en un sobre lacrado las claves de acceso a los servidores como medida de contingencia.

b) De requerirse el acceso a los servidores del Centro de Datos para otro especialista informático, deberá ser solicitado al Jefe de la Oficina de

OFICINA DE ADMINISTRACIÓN

Administración para su aprobación; de ser aprobado, el Coordinador de Informática entregará la clave en sobre lacrado y el documento de acuerdo de confidencialidad para la firma respectiva. (Anexo 03).

Claves de acceso a la Base de Datos para configuración de los aplicativos del OTASS:

La Oficina de Administración a través del Coordinador de Informática deberá actualizar periódicamente las claves de los usuarios para la conexión a las Bases de Datos de los aplicativos desarrollados por el OTASS, las cuales se deberán efectuar con una periodicidad de seis (06) meses, dentro de los primeros quince (15) días hábiles de cada semestre del año; asimismo se deberá actualizar en cualquier otro momento que se considere necesario, como en el caso de la ocurrencia del cese o cambio de área de algún personal al cual se le hizo entrega de la última clave actualizada, para lo cual se procederá de la siguiente manera:

a) El Coordinador de Informática, deberá:

- Gestionar el cambio de la(s) clave(s) de conexión a la(s) base(s) de dato(s) relacionales del OTASS, la misma que no deberá repetirse con ninguna clave anterior utilizada, una vez recibida las nuevas claves las mantendrá en custodia en un sobre lacrado hasta el próximo cambio y/o para la posterior entrega al personal asignado a esta función.
- Entregar al especialista informático a cargo de la administración de la Base de Datos del OTASS, las claves de acceso correspondientes en un sobre lacrado y a través de un documento para que realice el cambio respectivo. Dicho personal deberá firmar un acuerdo de confidencialidad en el cual se compromete a no revelar, comentar, suministrar o transferir de cualquier forma, tal información a terceros puesto que esta clave permite el acceso a datos e información confidencial y privilegiada. (Anexo 03).
- Entregar al Jefe de la Oficina de Administración en un sobre lacrado las claves de acceso respectivas como medida de contingencia.

b) El Coordinador de Informática comunicará mediante un informe al Jefe de la Oficina de Administración respecto a la actualización de la nueva clave en los aplicativos.

c) De requerirse el acceso de la clave para otro especialista informático de la Oficina de Administración, el Coordinador de Informática deberá solicitar al Jefe de la Oficina de Administración para su aprobación; de ser aprobado, el Coordinador de Informática entregará a dicho personal la clave en sobre lacrado y el documento de acuerdo de confidencialidad para la firma respectiva. (Anexo 03).

6.2.4 Revisión de Derechos de Acceso de Usuarios de los Trabajadores

La Oficina de Administración a través del Coordinador de Informática revisará periódicamente el sistema de administración de acceso a la red y sistemas externos o adquiridos, a fin de obtener la relación de usuarios, perfiles y permisos actualizados. Deberá coordinar y comunicar a todas las unidades orgánicas sobre los usuarios activos en el sistema, a fin de que sean depurados los que no correspondan, las cuales se deberán efectuar con una periodicidad de seis (6) meses dentro de los primeros quince (15) días hábiles de cada

semestre. Asimismo, las unidades orgánicas deberán proporcionar la información que les sea solicitada para dicho fin.

6.2.5 Responsabilidades de los usuarios:

a) Los servicios de acceso a la red, sistemas, correo electrónico, internet y documentos que existen en los equipos informáticos son de responsabilidad de los usuarios asignados y solo podrán utilizarse para propósitos lícitos, responsables y en cumplimiento de sus funciones.
b) Los usuarios que tengan acceso a internet deberán acceder a sitios seguros y no descargarán contenido ni programas no autorizados, sin licencias o de procedencia no confiable.
c) Está prohibido utilizar los recursos informáticos de la entidad para fines que no estén relacionados con el desarrollo de sus funciones, así como, la creación e introducción de virus o cualquier otro software perjudicial o nocivo que puedan ser utilizados para atacar los sistemas informáticos de la entidad.
d) Los usuarios de la entidad cuidarán que las contraseñas o claves de acceso se mantengan en estricta confidencialidad, ya que estos son la principal protección contra el ingreso no autorizado a los servicios de red y sistemas.
e) Todos los trabajadores que tengan asignados recursos informáticos y acceso a sistemas son únicos responsables de todos los efectos del uso que se derive de ellas; por tal motivo deberá cerrar la sesión o bloquear su estación de trabajo al momento de ausentarse.
f) La divulgación de la información y la manipulación indebida de las claves de acceso de los sistemas y los daños de información que pudiera ser generado será responsabilidad directa de los usuarios autorizados de dicha información, tal hecho será sancionado de acuerdo a la normativa vigente.
g) Cuando los usuarios detecten cualquier incidente, acceso indebido o problema de seguridad de información que surjan en el uso de los equipos de la entidad deben comunicar a la Oficina de Administración.

6.2.6 Medidas de Seguridad en los Sistemas Informáticos:

a) La Oficina de Administración a través del Coordinador de Informática es el único autorizado para la instalación de software en los equipos de cómputo de la entidad. Los programas informáticos deben contar con licencia o autorización del uso válido a nombre de la entidad.
b) Está prohibido cualquier retiro de equipo de cómputo de la entidad salvo autorización expresa del Jefe de la Oficina de Administración.
c) La Oficina de Administración a través del Coordinador de Informática es responsable del mantenimiento de los equipos de cómputo, el mismo que se efectuará de forma periódica en las diferentes unidades orgánicas de la entidad, este mantenimiento podrá efectuarse a través de terceros, cuando corresponda.
d) La Oficina de Administración a través del Coordinador de Informática es responsable de realizar los backups o respaldos de la información relevante almacenados en el Centro de datos del OTASS; debiendo almacenarlos en lugares adecuadamente preparados para dicho fin.

OFICINA DE ADMINISTRACIÓN

VII. DISPOSICIONES COMPLEMENTARIAS

7.1 Todos los trabajadores del OTASS con acceso a los sistemas informáticos deberán cumplir lo establecido en la presente Directiva desde el momento en que hacen uso de los recursos informáticos ofrecidos por la entidad.

7.2 Los aspectos no contemplados en la presente directiva, serán resueltos por la Oficina de Administración.

7.3 El OTASS aplicará las sanciones correspondientes de acuerdo con lo establecido en el Reglamento Interno de Trabajo, cuando el usuario incumpla con las medidas de seguridad establecida en la presente Directiva.

VIII. DISPOSICIÓN FINAL

La presente directiva entrará en vigencia a partir del día siguiente de su publicación en la página web del OTASS (www.otass.gob.pe).

IX. ANEXOS

ANEXO 01: Formato de Solicitud de Acceso a los Servicios de Tecnologías de la Información

ANEXO 02: Acuerdo de Confidencialidad para Personal / Locador del OTASS

ANEXO 03: Acuerdo de Confidencialidad para Personal / Locador que tenga la función o preste un servicio relacionado a sistemas o informática en la Oficina de Administración.

OFICINA DE ADMINISTRACIÓN

San Isidro, Junio de 2017.

ANEXO 01:

Formato de Solicitud de Acceso a los Servicios de Tecnologías de la Información

OTASS
Organismo Técnico de la Administración de los Servicios de Saneamiento

OFICINA DE ADMINISTRACION

La columna *"No"* se utiliza para la eliminación de los accesos. De no marcar con una "X" en el casillero *"SI"*, se asumirá que no se autorizan dichos accesos.

Formato de Solicitud de Acceso a los Servicios de Tecnología de la Información

Versión 1.0

N° DE SOLICITUD
(Llenado por el Coordinador de Informática)

Fecha:

DATOS DEL ÁREA SOLICITANTE:

Oficina / Dirección: (Siglas) | Apellidos y Nombres del Director / Jefe:

DATOS DEL USUARIO A ASIGNAR/RETIRAR SERVICIOS:

Apellido Paterno: | Apellido Materno:

Nombres: | DNI / Pasaporte:

Cargo: | Anexo :

Equipo de Cómputo Propio: ☐ SI

Condición Laboral: ☐ CAS ☐ Practicante | Indique Usuario de Red:

☐ Otro tipo de Contrato o Modalidad Laboral

ACCESO/RETIRO DE RECURSOS INFORMÁTICOS:

Requerimiento: CREACIÓN Y/O MODIFICACIÓN ☐ ELIMINACIÓN ☐

Servicios a solicitar:	SI	No		SI	No
Acceso a Red	☐	☐			
Correo electrónico	Acceso Correo OTASS ☐	☐	Acceso Correo mediante el Celular ☐	☐	
Acceso Telefónico	Salida Externa ☐	☐	Llamada a Celular ☐	☐	Número de anexo telefónico ☐
Internet Alámbrico ☐			Internet Inalámbrico ☐		

Marque con una "X" los accesos a incluir o retirar. Puede marcar más de una opción:

4:Director.	3:Coordinador.	2:Especialista	1:Secretaria.

La solicitud de acceso a Internet se asigna a base de las necesidades del área solicitante y cargo que la requiere. Los accesos marcados como 4 y 3 serán aprobados por la Oficina de Administración.

ASIGNACIÓN/RETIRO DE ACCESOS A SISTEMAS DE INFORMACIÓN (DESARROLLO Y/O MANTENIMIENTO DE APLICACIONES):

Requerimiento: CREACIÓN ☐ MODIFICACIÓN ☐ ELIMINACIÓN ☐

De marcar "Eliminación" proceder a indicar "no" para retiro de accesos, asumiéndose que antes tenía ese acceso asignado.

Sistemas a solicitar

Sistema Peruano de Información Jurídica (SPIJ)	SI / No	Accesos al SIGA: Debe ser visado por la Oficina de Asesoría Jurídica autorizándose el uso del SPIJ.	
Sistema de Integrado de Administración Financiera (SIAF)	SI / No	Accesos al SIAF: Debe ser visado por la Oficina de Planeamiento y Presupuesto y/o Oficina Administración de ser el caso, autorizándose el uso del SIAF.	
Sistema Integrado de Tramite Documentario (SITRAD)	SI / No	Accesos al SITRAD: Debe ser visado por la Secretaría General, autorizándose el uso del SITRAD	
OTROS	SI / No	Describa:	

Acceso a Carpetas Compartidas ☐ SI ☐ No

En caso marcar "SI" para el acceso a Carpetas Compartidass, debe especificar la relación de Carpetas, según tabla adjunta.

TABLA DE RECURSOS COMPARTIDOS DE INFORMACIÓN

NOMBRE DEL RECURSO COMPARTIDO	PRIVILEGIO DE ACCESO		NOMBRE DEL RECURSO COMPARTIDO	PRIVILEGIO DE ACCESO	
	LECTURA (L)	ESCRITURA (E)		LECTURA (L)	ESCRITURA (E)

De requerir alguna carpeta adicional que no se indique en la tabla adjunta, sírvase indicarlo a continuación:

Observaciones/Comentarios

Autorizaciones del área solicitante

V° B° Director o Jefe de la Oficina del Area solicitante	V° B° Jefe de la Oficina de Administración

De requerir apoyo en el llenado de este formulario, puede comunicarse con el Coordinador de Informática o al email: informatica@otass.gob.pe

OFICINA DE ADMINISTRACIÓN

ANEXO 02

Acuerdo de Confidencialidad para Personal / Locador del OTASS

_____, ____ de _____ de _____

<Nombre de Ciudad> <Día> <Mes> <Año>

Yo, _____, con DNI _____, personal ( ) / locador ( ) del OTASS del área de _____ en la sede de _____, suscribo el presente acuse de recibo de credenciales y acuerdo de confidencialidad.

Declaro ser consciente de la importancia de las credenciales que me fueron asignadas y acepto que las mismas solo serán utilizadas para los propósitos de mis funciones, en la red y sistemas del OTASS.

Adicionalmente, entiendo que la publicación, traspaso no autorizado o mal uso de las mismas están sujetos a sanciones definidas por la Oficina de Administración y, en algunos casos, puede ser un crimen penado por ley.

Debido a ello, durante la vigencia del vínculo laboral o contrato de locación, me comprometo a no compartir mis claves de acceso a los recursos institucionales y me responsabilizo en comunicar por escrito o correo electrónico a mi superior inmediato y al Jefe de la Oficina de Administración en caso de detectar el uso no autorizado de los mismos, a fin de que se tomen los correctivos necesarios.

El compromiso indicado en el párrafo precedente incluirá un periodo de cinco (5) años posteriores a la finalización del vínculo laboral con el OTASS o término del contrato de locación.

Dejo constancia por escrito a través de este documento, de mi aceptación a los términos y condiciones, aquí expresados.

_____

Nombres y Apellidos

ANEXO 03

Acuerdo de Confidencialidad para Personal / Locador que tenga la función o preste un servicio relacionado a sistemas o informática en la Oficina de Administración

_____, ____ de _____ de _____

<Nombre de Ciudad> <Día> <Mes> <Año>

Yo, _____, con DNI _____, personal ( ) / locador ( ) del OTASS del área de _____ en la sede de _____, suscribo el presente acuse de recibo de credenciales y acuerdo de confidencialidad.

Declaro ser consciente de la importancia de las credenciales, códigos fuentes, recursos informáticos e información que me fue asignada y acepto que las mismas sólo serán utilizadas para los propósitos de mis funciones, en la red y sistemas del OTASS.

Adicionalmente, entiendo que la publicación, traspaso no autorizado o mal uso de las mismas están sujetos a sanciones definidas por la Oficina de Administración y, en algunos casos, puede ser un crimen penado por ley.

Debido a ello, durante la vigencia del vínculo laboral o contrato de locación, me comprometo a:

a. No compartir con terceros mis claves de acceso a los recursos institucionales, bajo ningún motivo, puesto que esta clave permite el acceso a datos e información confidencial y privilegiada.
b. No compartir códigos fuentes, recursos informáticos e información que me fue asignada, salvo me encuentre laborando y tenga la aprobación expresa de mi jefe inmediato y jefe de la Oficina de Administración.
c. Comunicar por escrito o correo electrónico a mi jefe inmediato y al Jefe de la Oficina de Administración, en caso de detectar el uso no autorizado de los mismos, a fin de que se tomen las medidas correctivas necesarias.

OFICINA DE ADMINISTRACIÓN

Los compromisos a y b indicados en los párrafos precedentes incluirá un periodo de cinco (5) años posteriores a la finalización del vínculo laboral con el OTASS o término del contrato de locación.

Dejo constancia por escrito a través de este documento, de mi aceptación a los términos y condiciones, aquí expresados.

_____

Nombres y Apellidos