Resolución Directoral

Nº 001-2020-VIVIENDA/OGEI

Lima, 23 de Enero del 2020

VISTOS:

El Informe Nº 001-2020-VIVIENDA/OGEI-OTI-EMP de la Administradora de Base de Datos y el INFORME N° 003-2020-VIVIENDA/OGEI-GFN del Oficial de Seguridad de la Información; y,

CONSIDERANDO:

Que, mediante Decreto Supremo N° 004-2013-PCM, se aprueba la Política Nacional de Modernización de la Gestión Pública, siendo el principal instrumento orientador de la modernización de la gestión pública en el Perú, que establecerá la visión, los principios y lineamientos para una actuación coherente y eficaz del sector público, al servicio de los ciudadanos y el desarrollo del país; agregando en el numeral 3.2 los ejes transversales de la Política de Modernización en el Gobierno Electrónico;

Que, el artículo 55 del Reglamento de Organización y funciones – ROF del Ministerio de Vivienda, Construcción y Saneamiento – MVCS, establece que la Oficina General de Estadística e Informática – OGEI, es el órgano encargado responsable de la gestión de la infraestructura de tecnologías de la información y comunicaciones, así como de planificar, desarrollar, implantar y gestionar proyectos de desarrollo de soluciones basadas en tecnologías de la información y comunicación para la administración y gestión de la informática estadística sectorial;

Que, mediante Resolución Ministerial N° 004-2016-PCM, se aprueba 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, con la finalidad de coadyuvar con la Infraestructura del Gobierno Electrónico, por considerar a la seguridad de la información, como un componente crucial para dicho objetivo.

Que, mediante Resolución Ministerial N° 348-2017-VIVIENDA se aprueba el Plan Estratégico de Tecnologías de la Información y Comunicaciones (PETIC) 2017-2021 del Ministerio de Vivienda, Construcción y Saneamiento, que entre sus objetivos estratégicos: Mejorar el entorno de Tecnologías de la Información a través de la maduración de la gobernanza de Tecnologías de la Información y la rendición de cuentas, mejorar la toma de decisiones a través de sistemas interoperables con información correlacionada, establecer una infraestructura tecnológica ecoeficiente, accesible, convergente y segura que permita aumentar la productividad del personal del Ministerio haciendo uso intensivo

Resolución Directoral

de las Tecnologías de la Información y Comunicaciones, garantizar la seguridad y privacidad de la información del Sector, entre otros;

Que, con Resolución Ministerial N° 374-2017-VIVIENDA, del 02 de octubre del 2017, se aprobó el documento de gestión interno denominado "Política de Seguridad de la Información del Ministerio de Vivienda, Construcción y Saneamiento", que tiene como objetivo establecer el marco general de gestión para proteger la información del Ministerio, defendiendo directrices generales de actuación que aseguren el tratamiento adecuado de los riesgos y que conduzcan al fortalecimiento de una cultura institucional en seguridad de la Información;

Que, con Resolución Ministerial Nº 356-2018-VIVIENDA, del 23 de octubre de 2018 se constituyó el Comité de Gobierno Digital en el marco de la Resolución Ministerial N° 119-2018-PCM, entre cuyas funciones destaca la de liderar y dirigir el proceso de transformación digital en la entidad;

Que, mediante Informe N° 001-2020-VIVIENDA/OGEI-EMP la administradora de base de datos comunica que respecto a las materias de su competencia se ha emitido opinión favorable respecto a la aprobación de los citados Procedimiento;

De conformidad con lo dispuesto en la Ley N° 29158, Ley Orgánica del Poder Ejecutivo, Ley Nº 30156, Ley de Organización y Funciones del Ministerio de Vivienda, Construcción y Saneamiento; y su Reglamento de Organización y Funciones, aprobado por Decreto Supremo Nº 010-2014-VIVIENDA, modificado por Decreto Supremo Nº 006-2016-VIVIENDA, la Resolución Ministerial N° 004-2016-PCM que aprueba la Norma Técnica Peruana NTP ISO/IEC 27001:2014;

SE RESUELVE:

Artículo 1.- Aprobar el "Procedimiento de control de accesos a las bases de datos del MVCS", el mismo que forma parte integrante de la presente Resolución.

Artículo 2.- Disponer la publicación de la presente Resolución en el Portal Institucional del Ministerio de Vivienda, Construcción y Saneamiento (www.vivienda.gob.pe).

Regístrese y comuníquese

Ing. Daniel Alfonso Camacho Zárate
Director General
Oficina General de Estadística e Informática
Ministerio de Vivienda, Construcción y Saneamiento

PROCEDIMIENTO DE CONTROL DE ACCESOS A LAS BASES DE DATOS DE LA OTI-OGEI

1. OBJETIVO

Definir un claro procedimiento de control de accesos a las bases de datos de desarrollo y de producción de la OTI-OGEI.

2. BASE LEGAL

NTP-ISO/IEC 17799: Norma Técnica Peruana ofrece todas las recomendaciones necesarias para poder gestionar un Sistema de Seguridad de la Información (SSI)

ISO 27002: "Buenas prácticas para gestión de la seguridad de la información"

Resolución Ministerial Nº 246-2007-PCM, donde aprueban uso obligatorio de la Norma Técnica Peruana "NTP-ISO/ IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2a. Edición" en todas las entidades integrantes del Sistema Nacional de Informática.

Resolución Ministerial N° 004-2016-PCM, que aprueba el 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.

3. ALCANCE

El alcance del presente documento incluye los ambientes de base de datos de desarrollo y de producción de la OTI-OGEI.

4. CONTENIDO

El procedimiento administración de la base de datos tiene como objetivo, gestionar, administrar y garantizar la disponibilidad de las bases de datos, para brindar información en forma oportuna, segura y efectiva al ciudadano y en general a los usuarios que lo requieran.

Con la finalidad de implementar una correcta gestión de accesos a las bases de datos se deberá restringir el acceso de los desarrolladores a las bases de datos de producción y una definición de privilegios para el acceso a las bases de datos de desarrollo, dichas accesos se definirán en conjunto con el coordinador de desarrollo, a continuación, se muestran las siguientes plantillas para realizar solicitudes de accesos requeridos:

Solicitud de acceso a un ambiente de base de datos de desarrollo o producción.

- ✓ Indicar el nombre de base de datos.
- ✓ Indicar el motivo de acceso a la base de datos.

SOLICITUD DE ACCESO A UNA BASE DE DATOS	
Indicar motivo de acceso:	
Nombre de la BD:	
Indicar si la base es desarrollo/ producción:	

Solicitud de creación de la base de datos

- ✓ Indicar motivo de creación de base de datos, que tipo de información contendrá.
- ✓ Indicar nombre de la base de datos a crear.
- ✓ Indicar el ambiente en el que se creará, desarrollo o producción.
- ✓ Si el ambiente en el que se creará la base de datos es desarrollo, indicar cuánto tiempo estará habilitada y cuando se le podrá dar de baja.

SOLICITUD DE CREACIÓN DE LA BASE DE DATOS	
Motivo de creación de BD:	
Nombre de la BD:	
Se creará en desarrollo/ producción:	
Si es desarrollo, indicar la fecha tentativa de baja:	

Solicitud de dar de alta a un usuario de acceso a la base de datos

- ✓ Indicar el motivo de acceso a la base de datos
- ✓ Indicar el nombre del usuario
- ✓ Indicar a que base de datos tendrá acceso

SOLICITUD DE DAR DE ALTA A UN USUARIO DE ACCESO A LA BASE DE DATOS	
Motivo de alta de usuario:	
Nombre de la BD:	
Indicar ambiente desarrollo/ producción:	

Dar de baja a un usuario de acceso de base de datos

- ✓ Indicar el motivo de baja.
- ✓ Indicar el nombre del usuario

SOLICITUD DE DAR DE BAJA A UN USUARIO.	
Motivo de baja de usuario:	
Nombre de la BD:	
Indicar ambiente desarrollo/ producción:	

5. JUSTIFICACIÓN

✓ En la **ISO 27002: "Buenas prácticas para gestión de la seguridad de la información"**, cuyo principal objetivo es establecer directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización.

Dentro de los controles de seguridad de la información de la **ISO/IEC 27002** se encuentra la siguiente sección:

Es importante recordar que la organización puede utilizar esas directrices como base para el desarrollo del SGSI. Como sigue:

Sección 9 Control de acceso; El acceso a la información, así como a los recursos de procesamiento de la información y los procesos de negocios, debe ser controlado con base en los requisitos de negocio y en la seguridad de la información. **Debe garantizarse el acceso de usuario autorizado y prevenido el acceso no autorizado a los sistemas de información,** a fin de evitar daños a documentos y recursos de procesamiento de la información que estén al alcance de cualquiera.

9. CONTROL DE ACCESOS
9.1 Requisitos de negocio para el control de accesos
9.2 Gestión de acceso de usuario
9.3 Responsabilidades del usuario
9.4 Control de acceso a sistemas y aplicaciones

✓ Al realizar una auditoría a la administración de base de datos se solicita obligatoriamente dos controles:

a) Gestión de control de accesos a las bases de datos.
b) Gestión de copias de seguridad.