Resolución de Presidencia N° 295-2017-IPD/P

Lima 14 **de** diciembre **del** 2017

VISTO: El Memorando N°4912-2017-IPD/OPP de fecha 14 de diciembre 2017 y el Informe N° 883-2017-IPD/OAJ, de fecha 14 de diciembre 2017;

CONSIDERANDO:

Que, el Instituto Peruano del Deporte, en adelante IPD, conforme a la Ley N° 28036, Ley de Promoción y Desarrollo del Deporte, es el órgano rector del Sistema Deportivo Nacional, constituye un organismo público ejecutor y cuenta con autonomía funcional, administrativa y presupuestal;

Que, mediante Resolución de Presidencia Nº 247-2017-IPD/P, se aprueba la Directiva de Conversión de Documentos del Archivo del IPD al Sistema de Microformas y Microarchivos en el marco del uso obligatorio en todas las entidades integrantes del Sistema Nacional de Informática de la "Norma Técnica Peruana "NTP- ISO/IEC 17799:2007EDI Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información -2ª. Edición";

Que, a fin de implementar la Directiva de Conversión de Documentos del Archivo del IPD al Sistema de Microformas y Microarchivos, resulta necesario contar con un Manual de Seguridad de la Información del Sistema de Producción y Almacenamiento de Microformas;

El Manual precitado, tiene como finalidad, establecer las normas y procedimientos de seguridad de la información del sistema de producción y almacenamiento de microformas, en concordancia con la normatividad legal y técnica para implementar, gestionar y mantener la integridad, confidencialidad, seguridad de la información y las comunicaciones del IPD;

Que, mediante Informe Nº 091-2017-IPD/OPP/UOM la Unidad de Organización y Métodos de la Oficina de Presupuesto y Planificación del IPD, emite opinión favorable respecto la aprobación del Manual de Seguridad de la Información del Sistema de Producción y Almacenamiento de Microformas;

Que, a través del Informe N° 883-2017-IPD/OAJ, la Oficina de Asesoría Jurídica señala que el Manual descrito precedentemente, cumple con los lineamientos contenidos en la Directiva de Conversión de Documentos del Archivo del IPD al Sistema de Microformas y Microarchivos, emitiendo opinión favorable por su aprobación;

De conformidad con lo dispuesto en la Ley Nº 28036 – Ley de Promoción y Desarrollo del Deporte y sus modificatorias, el Reglamento de la Ley de Promoción y Desarrollo del Deporte aprobado mediante Decreto Supremo N° 018-2004-PCM, el Reglamento de Organización y Funciones del Instituto Peruano del Deporte, aprobado mediante Decreto Supremo N° 017-2004-PCM y modificado por el Decreto Supremo N° 086-2004-PCM;

Con los vistos de la Secretaría General, de la Oficina de Presupuesto y Planificación y la Oficina de Asesoría Jurídica;

SE RESUELVE:

Artículo 1.- Aprobar el Manual de Seguridad de la Información del Sistema de Producción y Almacenamiento de Microformas del Instituto Peruano del Deporte.

Artículo 2.- Publicar el Manual de Seguridad de la Información del Sistema de Producción y Almacenamiento de Microformas del Instituto Peruano del Deporte, en la página web del Instituto Peruano del Deporte (www.ipd.gob.pe).

Regístrese y comuníquese.

OSCAR FERNÁNDEZ CÁCERES
Presidente
INSTITUTO PERUANO DEL DEPORTE

INSTITUTO PERUANO DEL DEPORTE

MANUAL DE SEGURIDAD DE LA INFORMACION DEL SISTEMA DE PRODUCCION Y ALMACENAMIENTO DE MICROFORMAS DEL INSTITUTO PERUANO DEL DEPORTE

Concepto		Nombre y Apellido – Cargo	Firma
Elaborado por	:	Gabriela Doig Gómez Carrillo - Jefa de la Oficina de Trámite Documentario y Archivo	
Revisado por	:	Julio César Luque Maldonado - Jefe de la Unidad de Organización y Métodos	
Revisado por	:	Anita Marlene Reyes Huamán – Jefa de la Unidad de Informática	
Revisado por		Rony Salazar Martínez – Jefe de la Oficina de Asesoría Jurídica	
Revisado por	:	Miriam Betty Fernández Rodríguez – Jefa de la Oficina de Presupuesto y Planificación	
Aprobado por	:	Pilar Espinoza Galarcep – Secretaria General del IPD	

ÍNDICE

OFICINA DE ASESORÍA JURÍDICA IPD LIMA

OFICINA DE PRESUPUESTO Y PLANIFICACIÓN IPD LIMA

OF. TRAMITE DOCUMENTARIO Y ARCHIVO IPD LIMA

OFICINA GENERAL DE ADMINISTRACIÓN IPD UNIDAD DE INFORMÁTICA

OFICINA DE PRESUPUESTO Y PLANIFICACIÓN IPD Unidad de Organización y Métodos

SECRETARIA GENERAL IPD LIMA

MANUAL DE SEGURIDAD DE LA INFORMACIÓN DEL SISTEMA DE PRODUCCIÓN Y ALMACENAMIENTO DE MICROFORMAS DEL INSTITUTO PERUANO DEL DEPORTE

I. FINALIDAD

El presente manual tiene por finalidad instruir y cautelar sobre la integridad, confidencialidad, seguridad de la información y comunicaciones del Sistema de Producción de Microformas del IPD.

II. OBJETIVO

Establecer las normas y procedimientos de seguridad de la información del sistema de producción y almacenamiento de microformas, en concordancia con la normatividad legal y técnica para implementar, gestionar y mantener la integridad, confidencialidad, seguridad de la información y las comunicaciones, del IPD.

III. ALCANCE

Las disposiciones establecidas en el presente manual son de cumplimiento de todos los Órganos y Unidades del IPD que participan directamente o en apoyo del Sistema de Producción de Microformas.

IV. BASE LEGAL

- Decreto Supremo N° 017-2004-PCM, que aprueba el Reglamento de Organización y Funciones, de fecha 03.03.2004
- Resolución de Contraloría Nº 320-2006-CG, que aprueba las Normas de Control Interno.
- Resolución Ministerial Nº 246-2007-PCM, que aprueba el 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 Jefatural Nº 053-2003-INEI, aprueba la Directiva "Norma Técnica para la implementación del Registro de Recursos Informáticos en las instituciones de la Administración Pública".
- Resolución de Presidencia N° 440-2006-P/IPD, que aprueba el Manual de Organización y Funciones del IPD, de fecha 08.11.2006

V. DISPOSICIONES GENERALES

5.1 POLITICA DE SEGURIDAD ASOCIADA AL SISTEMA DE PRODUCCION Y ALMACENAMIENTO DE MICROFORMAS

Descripción:

Las Políticas de Seguridad descritas en el presente manual, es de aplicación al Sistema de Producción de Microformas de la Oficina de Tramite Documentario y Archivo (OTDA), del IPD.

5.1.1 Política de seguridad de la información

Son políticas de seguridad de la información del IPD para el sistema de producción y almacenamiento de microformas.

a. Referente a la gestión de seguridad de la información

i. Cumplir con las recomendaciones de seguridad de la información aplicables al personal, procedimientos, incorporación de soluciones informáticas, hardware, software aplicables al sistema de producción y almacenamiento de microformas con valor legal.

ii. Mejorar de manera continua la gestión de la seguridad de la información del sistema de producción y almacenamiento de microformas.

b. Referente al personal

Todo el personal es responsable de la seguridad de la información y de salvaguardar la confidencialidad, integridad y disponibilidad de la misma.

c. Referente a los accesos

El usuario debe mantener la confidencialidad de sus contraseñas, las cuales son de carácter personal y confidencial.

5.1.2 Documento de política de seguridad de la información

La documentación referente a la seguridad de la información es de conocimiento de todo el personal involucrado en el sistema de producción y almacenamiento de microformas.

5.1.3 Objetivos del sistema de seguridad de la información asociado al sistema de producción y almacenamiento de microformas.

a. Asegurar la integridad de la información incorporando elementos de control automáticos y supervisando la efectividad mediante evaluaciones periódicas.

b. Asegurar la integridad y confiabilidad de la seguridad de la información asociado al sistema de producción y almacenamiento de microformas.

5.1.4 Revisión y Evaluación

La seguridad de la información del sistema de producción y almacenamiento de microformas es un sistema que evoluciona de acuerdo con el avance tecnológico que se incorpora en los procesos y procedimientos del sistema de producción y almacenamiento de microformas.

La evaluación y revisión de la seguridad de la información del sistema de producción y almacenamiento de microformas, es realizada por la Unidad de Informática o, en caso requerido, por especialistas externos contratados para tal fin.

VI. DISPOSICIONES ESPECIFICAS

6.1ORGANIZACIÓN PARA LA SEGURIDAD

6.1.1 Organización Interna

Es un espacio físico adecuado para que varios usuarios cómodamente sentados, puedan trabajar en forma simultánea.

a. Sistemas e Información.

La Unidad de Informática, es responsable de brindar el soporte técnico para la seguridad de la información del sistema de producción y almacenamiento de microformas.

b. Asesoría Legal

La Oficina de Asesoría Jurídica, es responsable de informar a la Unidad de Informática sobre las variaciones de la normatividad establecida en la base legal y otras relacionadas a la materia para su adecuación permanente.

c. Archivo Central

Las funciones del personal que participa en el sistema de producción y almacenamiento de microformas, se encuentra descrito en el "Manual del Sistema de Producción y Almacenamiento de Microformas".

6.1.2 Seguridad de acceso a terceros

a. Acceso de terceros

La seguridad de la información comprende el control de acceso físico a personas externas no pertenecientes al personal del sistema de producción y almacenamiento de microformas mediante controles que incluye:

i. Acceso sólo si se ha verificado la identidad del visitante.

ii. El acceso a las áreas administrativas se realiza sólo mediante autorización del responsable de la OTDA.

iii. El acceso a las áreas productivas no está permitido, salvo que sea autorizado por el responsable de la OTDA.

iv. El acceso lógico a los servidores, PCs, base de datos, o sistemas informáticos, no está permitido a terceros.

v. Sólo tendrán acceso a la base de datos o sistemas informáticos inspectores o auditores que en cumplimiento de labores reglamentarias o auditoría de sistemas sean autorizados por el responsable de la OTDA, en coordinación con la Unidad de Informática. Este acceso se realizará bajo la supervisión del responsable de la gestión auditada.

vi. El personal subcontratado que realiza labores de limpieza y mantenimiento de las instalaciones del sistema de producción y almacenamiento de microformas no tienen acceso a los recursos de información y los procesos de tratamiento de la información.

b. Requisitos de seguridad de terceros

En caso de contratistas, que requieran trabajar temporalmente en las instalaciones del sistema de producción y almacenamiento de microformas deben conocer las políticas, objetivos del sistema de seguridad de la información y cumplir con mantener la confidencialidad e integridad de la información.

El responsable de la OTDA debe verificar que todos los equipos pertenecientes a personal externo que sean conectados a la red del IPD, cuentan con un antivirus instalado y actualizado a la fecha.

6.2RESPONSABILIDAD DE ACTIVOS

6.2.1 Inventario de activos

a. La Unidad de Informática coordina el mantenimiento y actualización del inventario de activos del sistema de producción y almacenamiento de microformas.

b. Son objeto de inventario, el hardware y software incorporado en el sistema de producción y almacenamiento de microformas.

6.2.2 Clasificación de la información

a. Criterios de clasificación

Para establecer el tratamiento que se dará al tipo de documentación que se procesará en el Sistema de Producción de Microformas se ha tomado el siguiente criterio de clasificación:

CRITERIO DE CLASIFICACIÓN	DESCRIPCIÓN	TRATAMIENTO
Confidencial	Documentación que ingresa al IPD en sobres cerrados o en cajas con precintos de seguridad.	No Aplica, al IPD no llegan documentos que se consideren confidenciales.
General	Documentación que ingresa al IPD sin distintivos de confidencialidad.	Los documentos se digitalizan íntegramente.

6.3SEGURIDAD EN RECURSOS HUMANOS

6.3.1 Seguridad en el trabajo

Con una frecuencia anual y cuando se identifiquen incidentes de seguridad, La Unidad de Informática verifica el cumplimiento de las políticas de seguridad de la información.

a. Acuerdos de confidencialidad y condiciones de la relación laboral

La información contenida en los documentos que se procesan en el sistema de producción de microformas se protege mediante un acuerdo de confidencialidad que suscribe el personal que participa en la elaboración de microformas. (el formato se encuentra en el anexo VI del MPAM).

6.3.2 Formación de usuarios

a. Formación y capacitación en seguridad de la información

i. El personal recién ingresado es entrenado en los procedimientos específicos y materia de seguridad de la información del sistema de producción y almacenamiento de microformas antes de asumir responsabilidades.

ii. La formación en seguridad de la información se actualiza cuando sea requerido incorporar nuevas especificaciones en los procedimientos o cuando existan cambios en las normas legales o técnicas aplicables a la seguridad de la información.

6.4SEGURIDAD FÍSICA Y DEL ENTORNO

6.4.1 Áreas seguras

El objetivo de definir áreas de seguridad física y control de acceso, es prevenir el acceso sin autorización a las instalaciones, daño a la propiedad e interferencias a los procedimientos del sistema de producción y almacenamiento de microformas y la información clasificada.

a. El perímetro de seguridad física:

Comprende el cerco perimétrico de la sede central del IPD.

b. Controles físicos de entrada

i. La primera barrera de control es la establecida en la recepción del IPD, la que permite acceso a personas previa identificación y registro de equipos que se requieran ingresar a la institución.

ii. La segunda barrera de control de acceso de personas es la establecida en cada piso, donde el visitante se anuncia, y se autoriza el ingreso al área correspondiente.

c. Seguridad del área del sistema de producción de microformas

El área cuenta con una puerta de acceso que se encuentra cerrada para evitar el acceso de personas no autorizadas.

El **control de acceso** a visitantes, personal temporal, proveedores de servicios y terceros al área de producción de microformas corresponde al responsable de la OTDA, quien autoriza el acceso a dicha área, verificando en todo momento la seguridad de la información y como medida salvaguardar la confidencialidad e integridad del procesamiento de los datos, el visitante al área de Producción deberá firmar la declaración mediante la Carta de Compromiso de Confidencialidad (Ver Anexo 1).

6.4.2 Seguridad de los equipos

a. El objetivo es prevenir pérdida, daño, robo o poner en riesgo los activos e interrumpir las actividades del sistema de producción y almacenamiento de microformas.

b. El cuidado de los equipos es responsabilidad del personal a quien se asigna dicho equipo.

c. La Unidad de Informática verifica las condiciones de instalación y protección de todos los equipos y PCs del sistema de producción y almacenamiento de microformas.

d. La Unidad de Informática diseña la arquitectura de redes internas y provee de seguridad al sistema de cableado, de acuerdo a las especificaciones técnicas aplicables, para evitar interrupciones en las operaciones.

e. La Unidad de Informática determina la frecuencia de mantenimiento de equipos, siendo el responsable de la OTDA quien verifica su cumplimiento. El mantenimiento de los equipos se debe realizar dentro de los siguientes periodos de tiempo:

EQUIPO	MANTEMIENTO
Escáner de producción	01 veces al año
PC's	01 veces al año
Impresoras	01 veces al año
Servidores	01 veces al año

f. La seguridad en el uso de equipos que cuenten con dispositivos de memoria o almacenamiento automático de información es controlada por la Unidad de Informática.

g. El personal del sistema de producción y almacenamiento de microformas debe mantener control de la seguridad de su puesto de trabajo y aplicar las buenas prácticas de uso de las PCs asignadas a sus funciones y responsabilidades.

   i. Mantener los cajones de su escritorio y las gavetas de sus armarios debidamente cerradas y accesibles sólo bajo su responsabilidad y supervisión.

   ii. Mantener su lugar de trabajo libre de cualquier información escrita especialmente aquella de carácter confidencial, especialmente cuando se tenga que ausentar temporalmente de su puesto de trabajo.

   iii. Las PCs deben estar aptas para los controles de acceso personal y contar con los derechos de usuario de acuerdo a las funciones operativas que le corresponden.

   iv. La pantalla debe bloquearse cuando no se utiliza y debe ser reiniciada mediante su propia contraseña. Al no utilizar el equipo por un tiempo de 5 minutos los equipos se bloquean automáticamente.

   v. Su puesto de trabajo debe presentar una imagen de limpieza y orden que permita detectar cualquier alteración en caso de ausencia o por efectos de accesos no autorizados.

   vi. Ejecutar las rutinas de antivirus a todo medio de soporte de información, datos y aplicativos de origen externo al sistema de producción y almacenamiento de microformas, que por razones de sus funciones les sea entregado.

   vii. Notificar inmediatamente a la Unidad de Informática cualquier incidente de seguridad o violaciones potenciales que identifique en la PC asignada para realizar sus funciones.

h. La extracción de equipos de las instalaciones del sistema de producción y almacenamiento de microformas debe ser autorizada por el responsable de la OTDA previa coordinación con la Unidad de Informática.

i. La instalación, actualización o retiro de software de las PCs debe ser autorizada por el responsable de la OTDA en coordinación con la Unidad de Informática.

6.5GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

6.5.1 Respuestas ante incidencias y malos funcionamientos de la seguridad referente al personal

a. Comunicación de las incidencias de seguridad

i. Todo el personal asume pleno conocimiento de las políticas, objetivos de la seguridad de la información relacionados al sistema de producción y almacenamiento de microformas. Para el caso de proveedores de servicios o terceros subcontratados, éstos son informados de la política de seguridad y deberán firmar la Declaración Jurada.

ii. En caso de ocurrencia de incidencias relativas a la seguridad de la información, debilidades del sistema, situaciones anormales en el uso del software o indicios de acceso no autorizado, el personal reporta inmediatamente estos eventos al responsable de la OTDA, quien a su vez dará aviso a la Unidad de Informática.

iii. La Unidad de Informática propone las medidas correctivas hasta eliminar, reducir o corregir las incidencias que atentan contra la seguridad de la información

b. Procedimientos de gestión de incidencias

i. Para asegurar la información y minimizar las incidencias de seguridad del sistema de producción y almacenamiento de microformas, se configuran los procesos creando un grupo de estaciones de trabajo bajo políticas de seguridad, sin conexión a internet y deshabilitar todos los puertos periféricos (que no se utilicen), y con PCs accesibles solo al personal del sistema de producción y almacenamiento de microformas.

ii. El personal que cuenta con equipos con conexión a internet reporta las incidencias directamente a Soporte Técnico para eliminar o reducir los daños producidos por ataques de virus o accesos no autorizados.

iii. La Unidad de Informática, verifica las unidades portátiles en previsión de haber sido afectado por virus, y realiza la limpieza de sus directorios.

6.6GESTIÓN DE COMUNICACIONES Y OPERACIONES

6.6.1 Procedimientos y responsabilidades de operación

El objetivo es asegurar las operaciones que involucran la transmisión de información en red local y no se afecte la seguridad de la información.

a. Documentos de procedimientos operativos

Los manuales de seguridad de la información, y de procedimientos del sistema de producción y almacenamiento de microformas constituyen la documentación que establece los procedimientos a cumplir.

b. Segregación de Tareas

El manejo de las funciones del sistema informático del sistema de producción y almacenamiento microformas está estructurado de manera que exista una asignación particular y exclusiva para cada proceso y/o actividad, de tal forma que se asegura y minimiza las incidencias de modificar la información y evitar el riesgo de acceso no autorizado a los sistemas operativos que no sean los asignados a cada proceso y cada responsable operativo.

c. Separación de los recursos para producción de microformas

i. El ambiente de producción se encuentra separado físicamente de los ambientes administrativos de tal manera que no existan interferencias funcionales, se proteja la integridad de los equipos e instalaciones y se

reduzca el riesgo de acceso o modificaciones no autorizadas a los sistemas operativos y los procesos.

ii. La Unidad de Informática se encarga de mantener los controles informáticos asociados al sistema de producción y almacenamiento de microformas.

6.6.2 Planificación y aceptación del sistema de seguridad de la información

El objetivo es minimizar el riesgo de fallas de los sistemas informáticos.

a. La Unidad de Informática constantemente monitorea y revisa el correcto funcionamiento de los sistemas informáticos del IPD, Asimismo, realiza proyecciones de los requerimientos futuros de capacidad para asegurar la disponibilidad de capacidad de procesamiento y almacenamiento adecuados.

b. Para realizar la aceptación de un sistema, la Unidad de Informática realiza un control de calidad de dicho sistema mediante pruebas de funcionalidad, con lo cual se asegura el cumplimiento de todos los criterios de aceptación.

6.6.3 Protección contra software malicioso

El objetivo es proteger la integridad del software y de la información.

a. La Unidad de Informática evalúa y propone la implementación de medidas y controles contra software malicioso.

b. Como medida de seguridad para proteger el sistema informático del sistema de producción de microformas del software malicioso se ha establecido lo siguiente:

i. Prohibir el acceso a internet en las áreas de producción.

ii. Deshabilitar los puestos periféricos que no sean necesarios para el uso y seguridad de la Línea de Producción (usb, grabadores de discos).

iii. Utilizar licencias de software y la prohibición de software no autorizado.

iv. Actualización de software de detección y eliminación de virus.

6.6.4 Gestión interna de respaldo y recuperación

El objetivo es mantener la integridad y disponibilidad de la información y de los recursos del procesamiento de la información.

a. A fin de asegurar que las operaciones se realizan de acuerdo a lo previsto el sistema de producción y almacenamiento de microformas dispondrá de la generación de los "logs" de tal forma que se puedan evaluar los accesos no autorizados, ataques u otras incidencias de seguridad que alteren los procesos o funciones en cada módulo de trabajo.

b. La Unidad de Informática verifica el registro de intentos fallidos de ingreso del sistema, para las medidas correspondientes.

6.6.5 Gestión de red

El objetivo es asegurar la protección de la información en red y la protección de la infraestructura de soporte.

Controles de red: los procesos de la línea de producción de microformas de la OTDA se realizan en red local sin conexión a internet.

6.6.6 Utilización y seguridad de los medios de información

El objetivo es prevenir la difusión no autorizada, modificación, retiro o destrucción de los activos e interrupciones en las actividades del sistema de producción y almacenamiento de microformas.

a. Gestión de medios removibles: La Unidad de Informática, verifica que el personal asignado al sistema de producción y almacenamiento de microformas no ingresen, ni extraigan discos flexibles, discos compactos o memorias portátiles.

b. En caso se requiera eliminar medios portadores de información clasificada, obsoleta o corrupta, la Unidad de Informática verifica que la información sea removida de los medios regrabables o se destruyan físicamente los medios portadores no regrabables de tal manera que no se puedan recuperar de ellos información que pueda afectar la seguridad de la información del sistema de producción y almacenamiento de microformas.

c. El manejo de la información se realiza según lo indicado en 6.3.2 inciso a).

6.6.7 Intercambio de información y software

El objetivo es mantener la seguridad de la información y el software en el intercambio dentro del sistema de producción y almacenamiento de microformas.

6.7CONTROL DE ACCESOS

6.7.1 Requisitos para el control de accesos:

El Objetivo es controlar el acceso a la información.

En concordancia con la política de seguridad de la información del sistema de producción y almacenamiento de microformas, la información es clasificada según lo descrito en 6.3.2 inciso a) por lo cual tanto el personal, los procedimientos de seguridad, los planes de contingencia y protección del sistema son priorizados tal como se describe en el presente manual y los documentos respectivos del sistema de producción y almacenamiento de microformas.

6.7.2 Gestión de acceso de usuarios

a. El responsable de la OTDA es personal autorizado en lo referente a la asignación, mantenimiento, renovación y cancelación del acceso a los módulos del sistema de producción y almacenamiento de microformas.

b. Registro de usuario: La Unidad de Informática, establece la frecuencia, y cuando sea requerido en casos de emergencias actualiza el registro de usuarios autorizados. Asimismo, coordinará el cambio de las contraseñas en caso el usuario intente 3 accesos errados, en este caso el usuario solicitará a la Unidad de Informática la asignación de un nueva contraseña, que por medidas de seguridad es cambiado obligatoriamente al primer intento por el usuario.

c. Gestión de privilegios: Para un manejo seguro, íntegro y confiable de la información y datos del sistema de producción y almacenamiento de microformas, cada responsable tiene derechos asignados para sus funciones específicas.

d. Gestión de contraseñas de usuario:

   i. Deben ser actualizadas a una frecuencia de 90 días, definida por la Unidad de Informática.

ii. Deben permanecer encriptados.

iii. Deben ser almacenadas de manera que no puedan ser accedidas por personas ajenas a su control.

iv. Al generar una nueva contraseña a un usuario, esta debe ser rechazado cuanto sea igual a una de las últimas 5 contraseñas.

e. Revisión de los derechos de acceso de los usuarios: La Unidad de Informática verifica la asignación de derechos usuarios y contraseñas, revisa los derechos asignados en concordancia con las políticas de seguridad del sistema de producción y almacenamiento de microformas y de acuerdo a lo solicitado por los responsables de los procesos específicos.

6.7.3 Control de acceso al sistema operativo

El objetivo es prevenir el acceso no autorizado a los sistemas operativos.

a. Identificación automática de terminales: La Unidad de Informática establece el procedimiento y los controles requeridos para entrada segura al sistema operativo.

b. Identificación y autenticación del usuario: Cada usuario tiene asignado un único identificador, contraseña y aplicativos asignados a sus funciones y responsabilidades.

c. Utilización de las facilidades del sistema:

i. De acuerdo a las funciones y responsabilidades del personal en el manejo de los módulos, el personal tiene derecho a utilizar las aplicaciones del sistema en forma exclusiva para dichas funciones.

ii. El responsable de la OTDA es responsable de verificar que se cumplan estas especificaciones, debiendo informar a la Unidad de Informática sobre las incidencias de seguridad.

d. Restricción acceso a terminales: La Unidad de Informática ejecuta los mecanismos de control que permita que las PCs solo sean utilizadas durante el tiempo definido con anticipación.

e. Limitación del tiempo de conexión: De ser necesario, previa evaluación de la OTDA, se incorporarán límites de tiempo (horario de trabajo establecido en el Reglamento Interno de Trabajo), para el uso de las aplicaciones de alto riesgo, las cuales podrán extenderse previa autorización de la OTDA o por disposición de la Unidad de Personal.

6.7.4 Control de acceso a las aplicaciones

El objetivo es asegurar la información cuando se utilizan computadoras portátiles y equipos remotos.

a. Restricción de acceso a la información: el sistema de producción y almacenamiento de microformas permite el uso de computadoras portátiles, bajo previa autorización de la OTDA.

b. Aislamiento de sistemas sensibles: el sistema de producción y almacenamiento de microformas no tiene conexión a redes externas.

6.7.5 Seguimiento de accesos y usos del sistema

a. Para asegurar el seguimiento de accesos y usos del sistema, se dispone el registro automático.

b. Sincronización de relojes: Los relojes de todas las unidades asignadas al sistema de producción y almacenamiento de microformas son sincronizados con el controlador principal de dominio.

6.8 MANTENIMIENTO DEL SISTEMA

6.8.1 Seguimiento de accesos y usos del sistema

a. Análisis y especificación de los requisitos de seguridad.

i. Los procedimientos de seguridad son definidos por el responsable de la OTDA en coordinación con la Unidad de Informática.

ii. Los procedimientos de seguridad son documentados, implementados por el responsable de la OTDA y divulgados a todos los usuarios definidos.

6.8.2 Seguridad en los procesos de desarrollo y soporte

El objetivo es mantener la seguridad del software y la información.

a. Procedimientos de control de cambios

En caso que se establezcan cambios en el software o el sistema operativo, estas especificaciones se incluyen en el inventario de software y equipos.

b. Revisión técnica de los cambios en el sistema operativo

La Unidad de Informática evalúa los cambios en el software del sistema de producción y almacenamiento de microformas en función a los documentos a procesar o como resultado de las evaluaciones del rendimiento de los mismos.

c. Restricciones en los cambios a los paquetes de software

Para el caso de software adquirido, no están permitidos los cambios o modificaciones. En caso de identificar anomalías en su operación, se coordina con el proveedor a fin de que restablezca las condiciones de compra o la devolución de la inversión efectuada.

d. Pérdida de información (canales encubiertos y código troyano)

La Unidad de Informática efectúa una evaluación del software adquirido a efectos de asegurar y prevenir que no existan riesgos de virus o códigos troyanos que produzcan pérdida de la información.

6.9 GESTIÓN DE CONTINUIDAD

6.9.1 Aspectos de la gestión de continuidad del sistema de producción y almacenamiento de microformas.

El objetivo es contrarrestar las interrupciones de las actividades del Sistema de producción y almacenamiento de microformas y proteger los procesos críticos de los efectos de fallas del sistema de la información o de los desastres y asegurar una oportuna recuperación.

a. Proceso de gestión de la continuidad del sistema de producción y almacenamiento de microformas.

El responsable de la OTDA realiza las coordinaciones necesarias a fin de garantizar la continuidad del sistema de producción y almacenamiento de microformas.

b. Continuidad del sistema de producción y almacenamiento de microformas y análisis de impactos.

El responsable de la OTDA, propone la realización de auditorías en seguridad de la información del sistema de producción y almacenamiento de microformas con una frecuencia anual o en caso se detecten desviaciones que afecten la continuidad del sistema.

c. Redacción e implantación de planes de continuidad.

d. La Unidad de Informática, recomienda las medidas correctivas necesarias para mantener y restablecer las operaciones y asegurar la disponibilidad de la información al nivel requerido y el momento oportuno después de ocurridas las interrupciones o las fallas en los procesos críticos del sistema de producción y almacenamiento de microformas.

e. Prueba, mantenimiento y reevaluación de los planes de continuidad.

f. A frecuencia no mayor a un año, los planes de continuidad son revisados por la Unidad de Informática de tal forma que se asegure una permanente actualización y efectividad.

6.9.2 PROCEDIMIENTO PARA LA ACTIVACIÓN DEL EQUIPO UPS

a. El equipo UPS alimenta los servidores de Dominio, Base de Datos, Aplicaciones, Archivos de usuarios, Archivos de Digitalización, incluyendo todos los servidores de red.

b. El equipo UPS tiene una autonomía de sesenta minutos, los cuales permitirá el apagado en forma automática de todos los servidores de la red que se encuentran conectados al UPS.

c. Cuando exista una caída intempestiva de la energía eléctrica, el equipo UPS entrará en funcionamiento y activará mensajes de alerta con sonidos en el equipo.

d. El Administrador de la red será el encargado de la supervisión y comprobación de este proceso, y será quien registrará los sucesos en el libro de bitácoras de sucesos de red.

6.9.3 PROCEDIMIENTO PARA EL RESPALDO DE LA INFORMACIÓN DIGITALIZADA (ARCHIVO).

a. OBJETIVO:

Establecer el procedimiento para la ejecución del Backup (Copias de Respaldo) de la información digitalizada proveniente de la línea de producción, registrada en los servidores de la Sede Central, a fin de asegurar su oportuna disponibilidad como medida de contingencia cuando sea necesario.

b. PROCEDIMIENTO:

i. Con el fin de resguardar la información digitalizada de la OTDA, La Unidad de Informática les ha facilitado y compartido una carpeta de red en el servidor dedicado para este fin, con los permisos para grabar lo obtenido en la línea de producción de digitalización.

ii. El usuario debe mantener la estructura de carpetas facilitada por la Unidad de Informática y grabará únicamente la información obtenida en la línea de producción digitalizado.

iii. La Unidad de Informática se hará responsable de los archivos digitales almacenados en el Servidor que está asignado para la Línea de Producción y Almacenamiento de Microformas. Las copias de

seguridad de este directorio se realizan en forma diaria y semanal, almacenándose históricos mensuales.

iv. El administrador de la red tendrá la facultad de eliminar sin previo aviso archivos (tipo videos, música, fotos, etc.) ajenos a las labores de la entidad que se encuentren en el servidor de archivos

v. El administrador de la red realizará backups diarias y backup completa (los fines de semana)

vi. Las copias de respaldo semanales serán copiados luego a unidades de cinta y resguardados en un mueble ubicado en el DataCenter del Estadio Nacional

vii. El administrador de red registrará los sucesos en el libro de bitácoras y asignará la etiqueta según la nomenclatura estandarizada usada en nuestra entidad.

6.10 CUMPLIMIENTO DE NORMATIVIDAD LEGAL Y TÉCNICA

6.10.1 Cumplimiento con los requisitos legales

El objetivo es evitar incumplimiento de cualquier ley, reglamento, contratos, y obligaciones, así como los requisitos de seguridad.

a. Identificación de la legislación aplicable

La Oficina de Asesoría Jurídica, debe informar sobre las variaciones de la normatividad establecida en la base legal y otra relacionada a la Unidad de Informática, para su adecuación permanente.

b. Derechos de propiedad intelectual (DPI)

La Oficina de Asesoría Jurídica, debe de informar a la Unidad de Informática, sobre la obligación de la aplicación de las disposiciones legales y reglamentarias establecidas por la autoridad competente en el país.

c. Control de los registros de la organización

i. La aplicación de los procedimientos del sistema de producción y almacenamiento de microformas generan información de soporte de sus actividades que en forma de registros son evidencias del control de las operaciones y procesos.

ii. El responsable de la OTDA mantiene y actualiza los registros generados y establece su estructura de tal forma que refleje y se anoten en ellos los datos necesarios para verificar el cumplimiento de los controles establecidos en el sistema.

d. Protección de los datos de la privacidad de la Información de IPD.

La documentación e información del IPD son objeto de aplicación de los controles y procedimientos de seguridad para velar por su integridad en todas las etapas de su procesamiento.

e. Evitar el mal uso de los recursos de tratamiento de la información.

El personal del sistema de producción y almacenamiento de microformas asume el compromiso de aplicar la política interna de seguridad de la información del sistema de producción y almacenamiento de microformas. Los activos y bienes asignados para el desempeño de sus funciones solo se usan para fines del sistema.

6.10.2 Revisiones de la política de seguridad y de la conformidad técnica

El objetivo es asegurar que los sistemas cumplan las políticas y las normas aplicables del IPD.

a. Conformidad con la política de seguridad

Anualmente, la Unidad de Informática revisa las políticas de seguridad a fin de verificar el cumplimiento de los controles establecidos.

b. Comprobación de la conformidad técnica

A una frecuencia anual o cuando existan desviaciones o incidentes de seguridad que pongan en riesgo la continuidad del sistema de producción y almacenamiento de microformas, la Unidad de Informática propone la realización de auditorías del sistema de seguridad de la información para asegurar la protección de la infraestructura del sistema de producción y almacenamiento de microformas desde el punto de vista físico y lógico, y verificar los procedimientos del manual de seguridad de la información del sistema de producción y almacenamiento de microformas.

6.10.3 El objetivo es maximizar el cumplimiento del control interno informático y el sistema de auditoría informática para minimizar la interferencia en los procesos.

Se aplican a la estructura de la Unidad de Informática, sistemas de aplicación, recursos informáticos, seguridad, infraestructura de redes y comunicaciones del sistema y a las especificaciones que deben cumplir los usuarios del sistema informático asociado al sistema de producción y almacenamiento de microformas,.

El personal responsable de las actividades del control interno informático y de auditoria informática debe poseer conocimiento especializado en tecnología informática, materias de auditoría, normas técnicas y la legislación aplicable.

a. Control Informático

i. El personal del sistema de producción y almacenamiento de microformas, reporta las ocurrencias a la Unidad de Informática y al responsable de la OTDA.

ii. La Unidad de Informática propone las medidas correctivas para el caso de control correctivo, a fin de lograr la vuelta a la normalidad en el más breve plazo.

b. Auditoria Informática

Está descrito en el Manual Procedimientos del Sistema de Producción y Almacenamiento de Microformas.

c. Protección de las herramientas de auditoria de informática

i. El personal involucrado en el sistema de producción y almacenamiento de microformas debe mantener con carácter de confidencialidad los informes y resultados de la auditoria informática a fin de proteger y prevenir cualquier posible mal uso de la información.

ii. Los registros generados del sistema de seguridad de la información y los generados en los procesos de control y evaluación generan información y datos que sirven para evaluar el cumplimiento del sistema y para servir de referencia en casos que se requiera optar por mejorar el sistema de producción y almacenamiento de microformas en general o cada uno de los procesos en forma específica.

iii. Los registros del servidor del sistema bajo responsabilidad de la Unidad de Informática debe ser protegido con medidas de seguridad pertinentes, para consulta, inspección o auditoria del sistema.

iv. El período de conservación de los archivos es de 2 años, bajo responsabilidad del responsable de la OTDA. Al término del período de conservación procede su eliminación por ser documentos administrativos sin valor tributario, ni valor histórico ni generan derechos.

v. De igual forma los archivos (logs) de los módulos generados automáticamente para controlar la seguridad del sistema de seguridad de la información y las comunicaciones generan información que se mantiene en permanente observancia de los elementos de control de la seguridad del sistema de producción y almacenamiento de microformas y la efectividad del mismo.

vi. Los archivos automáticos son conservados como parte de la seguridad de la información implementado para el sistema de producción y almacenamiento de microformas y su periodo de conservación es de 3 años como mínimo en la memoria de los servidores del sistema o en medios de archivo electrónico (CD-R o DVD), bajo responsabilidad de la Unidad de Informática.