INSTITUTO SALVADOREÑO PARA EL DESARROLLO DE LA MUJER

UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN

LINEAMIENTO PARA LA ADMINISTRACIÓN Y SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS INSTITUCIONALES

ISDEMU
Instituto Salvadoreño para el Desarrollo de la Mujer

GOBIERNO DE EL SALVADOR

El Salvador, 2026

CONTENIDO

I. INTRODUCCIÓN

El Instituto Salvadoreño para el Desarrollo de la Mujer (ISDEMU) dispone de una estructura de gestión tecnológica orientada a garantizar la conectividad institucional, el desarrollo y administración de sistemas de información, y la implementación de las medidas necesarias para asegurar la integridad y disponibilidad de los datos a nivel nacional.

Los sistemas informáticos institucionales concentran información estratégica relacionada con el personal, los servicios de atención prestados a las usuarias y las operaciones desarrolladas en las distintas áreas de la institución. Su administración comprende la gestión de usuarios, el otorgamiento y control de accesos, el mantenimiento de la información y la implementación de mecanismos de respaldo que garanticen su disponibilidad y protección.

El presente lineamiento establece las directrices para la administración segura de los sistemas informáticos institucionales, con el propósito de regular los controles de acceso, la modificación de datos y el respaldo de la información, fortaleciendo la trazabilidad y la integridad de los registros como parte de los mecanismos de control interno institucional.

II. OBJETIVOS

- Establecer las directrices para la administración segura de los sistemas informáticos institucionales, garantizando la confidencialidad, integridad y disponibilidad de la información mediante el control de accesos y la gestión adecuada de usuarios.
- Determinar parámetros para el respaldo de la información institucional, de conformidad con el tipo y nivel de criticidad de dicha información.

III. FUNDAMENTO LEGAL

- Ley de Ciberseguridad y Seguridad de la Información
- Ley de Protección de los Datos Personales
- Ley Especial Contra los Delitos Informáticos y Conexos
- Ley de Firma Electrónica
- Ley de Telecomunicaciones

IV. ÁMBITO DE APLICACIÓN

El presente lineamiento es de aplicación obligatoria para el personal del área responsable de la gestión tecnológica institucional, así como para toda persona que, en razón de sus funciones, tenga acceso o realice gestiones relacionadas con los sistemas de información institucional.

Entre el personal responsable de aplicar y hacer cumplir estas disposiciones se encuentran:

- Personal técnico de soporte informático
- Personal técnico de desarrollo de software
- Personal técnico de redes y ciberseguridad
- Jefatura del área responsable de la gestión tecnológica institucional
- Todo el personal que, en el ejercicio de sus funciones interactúe con los diferentes sistemas de información institucional.

V. CONSIDERACIONES

La información generada y administrada en los sistemas informáticos institucionales constituye un activo estratégico que requiere controles documentados para garantizar su confidencialidad, integridad y disponibilidad, previniendo su manipulación indebida o no autorizada.

La institución cuenta con diversos sistemas de información que concentran datos del personal, de los servicios prestados y de las operaciones internas, cuya administración implica riesgos asociados al control de accesos, la modificación de datos y la disponibilidad de la información ante eventuales contingencias.

La revisión de los mecanismos de control institucional identificó brechas en la regulación de los respaldos de información documentada, el control de cambios en la gestión de usuarios y la trazabilidad de las acciones ejecutadas sobre los sistemas, aspectos que la versión anterior del instrumento no abordaba de manera integral.

En atención a lo anterior, se hace necesaria la actualización del presente lineamiento a fin de fortalecer el ciclo completo de gestión de los sistemas informáticos institucionales.

VI. DEFINICIONES

- **Software**: Programa que hace posible la funcionalidad de los sistemas informáticos, para el procesamiento de la información, como los sistemas operativos, aplicaciones, navegadores web, etc.
- **Datos**: La palabra datos se deriva del latín datum, que literalmente significa hecho, el cual puede ser un número, una afirmación o una imagen. Los datos son la materia prima en la producción de información.
- Información: Son los hechos o las conclusiones que tienen un significado dentro de un contexto. Para convertirse en información, los datos se manipulan mediante la formación de tablas o cualquier operación que permita comprender mejor una situación.
- **Proceso**: Es cualquier manipulación de los datos, con el propósito de producir información. Por lo tanto, mientras los datos son materia prima, la información es una salida o resultado.
- **Sistema de Información**: Está formado por todos los componentes que colaboran para procesar los datos y producir información. Casi todos los sistemas de información empresariales están integrados por muchos subsistemas con metas secundarias, todas las cuales contribuyen a la meta principal de la organización.
- **Backup**: Copias de seguridad que permiten recuperar los sistemas informáticos y sus datos ante una catástrofe informática, natural o un ataque cibernético.
- **Hardware**: Son elementos que conforman la parte física o tangible de un sistema informático, que incluye componentes eléctricos, electrónicos y electromecánicos.
- SIMEC: Sistema Integrado de Manejo de Expedientes y Citas.
- SIMUJER: Sistema de Gestión de Usuarias Ciudad Mujer.

VII. DISPOSICIONES GENERALES

1. CREACIÓN DE NUEVOS USUARIOS

Cada vez que se realice una nueva contratación, el área responsable de la gestión del talento humano deberá solicitar mediante memorando dirigido a la jefatura de la unidad responsable de la gestión tecnológica institucional remitido por correo electrónico, que se ejecuten las siguientes acciones:

- Asignación de un equipo informático, si el cargo lo requiere.
- Creación del usuario de la red institucional.
- Creación de una cuenta de correo electrónico institucional.
- Creación de usuarios para los sistemas informáticos de conformidad con el área a la que haya sido asignado el personal.

2. OTORGAMIENTO DE ACCESOS

Consiste en la asignación de permisos a un usuario, a fin de que pueda ejecutar diferentes acciones en los sistemas informáticos que anteriormente no tenía habilitadas.

La solicitud deberá remitirse mediante un correo electrónico acompañado de un memorándum en formato digital, por parte de la jefatura inmediata de la persona solicitante. La solicitud deberá especificar el nuevo perfil, el cual deberá encontrarse entre los perfiles autorizados del sistema, así como la justificación correspondiente para el cambio solicitado.

3. MODIFICACIÓN DE DATOS

Si se recibe la solicitud de modificación de los datos de un expediente de atención a usuarias, según se hace mención en el *Lineamiento para la Modificación a Expedientes en el SIMEC 2.0* y *Certificación de Expedientes Generados en los Centros de Atención del ISDEMU*; será por medio de correo electrónico dirigido a la jefatura de la unidad responsable de la gestión tecnológica institucional, adjuntando memorándum en formato digital remitido con visto bueno de la responsable del proceso misional de atención especializada.

La solicitud deberá contener evidencia gráfica del cambio solicitado para tener una mejor visualización de las modificaciones a realizar.

El técnico de soporte de sistemas hace las modificaciones correspondientes, notifica por los mismos medios en que se recibió la solicitud, que se han realizado los cambios solicitados a satisfacción, y solicita que la técnica de atención que solicitó el cambio lleve a cabo la verificación en el sistema para corroborar la actualización de los datos.

Cabe mencionar que la modificación de datos a expedientes del sistema SIMEC, solo es realizada a solicitud del proceso misional de atención especializada.

4. TRASLADO Y CAMBIO FUNCIONAL.

Cuando una persona servidora pública es trasladada de una unidad a otra con cambio funcional, se realizará una reasignación de los accesos, llevando a cabo las medidas necesarias para preparar el equipo y habilitarlo de acuerdo con las funciones de su nuevo cargo.

El área responsable de la gestión del talento humano realizará la comunicación con la solicitud del traslado mediante correo electrónico adjuntando memorándum en formato digital con las indicaciones de la asignación de los accesos, acorde a su nuevo cargo funcional. Posteriormente la jefatura inmediata se comunicará a través de correo electrónico, especialmente cuando el cambio funcional implique accesos críticos o especiales.

5. TRABAJO TEMPORAL EN OTRAS SEDES.

Cuando una persona servidora pública deba desarrollar labores temporales de apoyo institucional en una sede distinta a la de su adscripción y, para ello, requiera utilizar un equipo informático de dicha sede o conectar su equipo institucional a la red local, su jefatura inmediata deberá gestionar la solicitud correspondiente ante la jefatura del área responsable de la gestión tecnológica institucional, con la debida anticipación, mediante memorándum remitido por correo electrónico.

La solicitud deberá detallar, como mínimo, la sede en la que se desarrollará el apoyo, el período previsto, las actividades a realizar, el equipo a utilizar y los accesos requeridos para el cumplimiento de las funciones asignadas.

Recibida la solicitud, el área responsable de la gestión tecnológica institucional evaluará la procedencia del requerimiento y, de ser aplicable, habilitará los accesos correspondientes a los sistemas institucionales o a la red de la sede respectiva, realizando la coordinación técnica necesaria con la persona usuaria.

6. DAR DE BAJA A UN USUARIO.

Cuando se confirme un retiro de personal, el área responsable de la gestión del talento humano deberá solicitar la baja de los usuarios creados en los diferentes sistemas, mediante correo electrónico adjuntando memorándum en formato digital con las indicaciones correspondientes.

Por parte del área de gestión de tecnología institucional, el último día que se presente a laborar la persona, realizará el respaldo de la información generada en el equipo asignado en acompañamiento del representante del área de gestión documental institucional y de la persona representante del área de auditoría interna para que den fe de la información que se recibe. También se verificará el estado en que entregan los equipos y, en ese momento, se deshabilitarán las cuentas de los sistemas, la cuenta de correo institucional y el usuario de red, quedando denegado a partir de ese momento cualquier acceso.

7. SOLICITUD DE INFORMACION.

Cuando se requiera información proveniente de alguno de los sistemas institucionales, ya sea para su visualización en un reporte de Excel, en un cuadro de mando en Power BI o en otro formato, la jefatura deberá remitir un memorándum por correo electrónico y, adicionalmente, enviarlo en formato físico, detallando de manera precisa la información solicitada.

Se considerarán criterios de confidencialidad, protección de datos personales y niveles de autorización para poder brindar la información.

El técnico de sistemas realizará las consultas necesarias en las bases de datos de los sistemas respectivos para extraer dicha información y presentarla de la manera solicitada.

A través de un correo, el técnico responsable de obtener la información enviará un memorándum con los detalles de la información solicitada, y adjuntará el reporte solicitado o hará del conocimiento de los cambios realizados en el cuadro de mandos.

8. RESPALDO DE LA INFORMACION.

Cualquier tipo de información que sea generada dentro de la institución deberá ser respaldada a través de mecanismos que garantizan la seguridad y la disponibilidad de la información en los diferentes servidores de respaldo.

Entre la información a ser respaldada, se encuentra:

- Información generada por los usuarios en los equipos asignados. Esta información deberá ser respaldada cada día a una hora determinada. El usuario deberá tener encendido su equipo y conectado a la red, para que el respaldo sea realizado en un servidor especialmente designado para ese fin.

- Expedientes ingresados en el sistema SIMEC. La información deberá ser respaldada de forma semanal a un servidor de respaldos, mediante un proceso programado en SQL Server, que es el gestor de base de datos del sistema.

- Registros ingresados en los diferentes sistemas de información institucionales, tales como Activo Fijo, Inventario, Recursos Humanos, etc. El respaldo de las bases de datos de estos sistemas de información deberá ser programado para realizarse de manera semanal. Los respaldos se almacenarán en un servidor designado especialmente para ese fin.

- Información documentada generada en cada unidad organizativa, almacenada en carpetas compartidas. Se cuenta con un repositorio de documentos, que es otro servidor donde se podrá almacenar de forma segura toda la información documentada, y al mismo tiempo cuenta como servidor de respaldo para tener la información disponible en caso de pérdida.

- Repositorio de información creado en el servidor de la Unidad de Formación Especializada, cumpliendo como requisito solicitado por la auditoria del SGAS. Este repositorio fue creado para almacenar información del SGAS, información interna de la institución (manuales, lineamientos, procedimientos, etc.) e información externa de la institución (Leyes, reglamentos, etc.)

- Adicionalmente se cuenta con el almacenamiento en línea de Google Drive, donde las unidades deben resguardar información generada localmente, de forma organizada a través de Unidades Compartidas.

VIII. MECANISMOS DE VIGILANCIA Y EVALUACION

La jefatura del área responsable de la gestión tecnológica institucional será la instancia encargada de velar por el cumplimiento de las disposiciones establecidas en el presente lineamiento, asegurando que las acciones relacionadas con la administración de usuarios, el control de accesos, la modificación de datos y el respaldo de información se ejecuten conforme a lo establecido.

Como parte del seguimiento continuo, dicha jefatura deberá mantener registro de las solicitudes atendidas, los respaldos realizados y los incidentes relacionados con la gestión de los sistemas informáticos, como evidencia del cumplimiento de las disposiciones del instrumento.

Será la Dirección de Administración y Finanzas, en coordinación con el área responsable de la gestión tecnológica, la responsable de realizar una revisión anual del presente lineamiento a fin de valorar su pertinencia, actualización y alineación con los requerimientos institucionales vigentes, pudiendo recomendar su actualización cuando las condiciones operativas o normativas así lo requieran.

IX. VIGENCIA Y AUTORIZACION

El presente Lineamiento ha sido autorizado por la Presidencia del Instituto Salvadoreño para el Desarrollo de la Mujer (ISDEMU), en cumplimiento de las atribuciones conferidas por la Junta Directiva en la Sexta Sesión Ordinaria, celebrada el veintiséis de julio de dos mil veinticuatro, según consta en el punto número DOCE del Acta Número NUEVE. Este lineamiento entrará en vigencia a partir de la fecha de su autorización.

Yanci Salmerón de Artiga
Presidencia del ISDEMU / Alta Dirección
Autorizó

Carlos Alberto C[illegible]
Gerencia de Asuntos Jurídicos / Asesoría Jurídica de Despacho
Revisión Jurídica

Ligia Mercedes Zetino
Gerencia de Planificación Institucional
Revisión Técnica

Héctor A. Melara
Oficialía de Cumplimiento
Revisión de Cumplimiento

Lilian Sandoval
Unidad de Tecnologías de la Información
Presentó

Fecha de autorización	Fecha de entrada en vigencia	Vigencia programada
24/06/26	24/06/26	Indefinida

X. BITACORA DE ACTUALIZACION Y CONTROL DE CAMBIOS

N°	Fecha del cambio	Tipo de cambio	Situación anterior	Razón del cambio	Unidad responsable del cambio
1	22/01/2026	Creación del documento "Lineamiento para la Administración de los Sistemas Informáticos"	Inexistencia de un lineamiento que guie al personal en cada situación referente a los sistemas informáticos, dejando una brecha para la fuga de información.	Necesidad de crear un lineamiento para normar el accionar del personal sobre los pasos a seguir en cuanto a la administración de los sistemas informáticos con el fin de proteger la información en todo momento.	Unidad de Tecnologías de la Información
2	19/06/2026	Versión 2. Actualización de los lineamientos iniciales del documento.	Se cuenta con la versión 1 del lineamiento para la administración de los sistemas informáticos, en el cual se identificó que carecía de controles para mitigar los riesgos relacionados al área de seguridad de la información.	El lineamiento existente necesita ser actualizado pues se hace de vital importancia agregar aspectos como el resguardo de los datos y cómo manejar la solicitud de información.	Unidad de Tecnologías de la Información

INSTITUTO SALVADOREÑO
PARA EL DESARROLLO DE LA MUJER