ANEXO 2
ACUERDO: INE/GIMA/01/2023

RECOMENDACIONES PARA LA SEGURIDAD Y ASIGNACIÓN DE ACCESO, USO, ALMACENAMIENTO Y, EN SU CASO, CONSERVACIÓN DE LA INFORMACIÓN

Capítulo I
Del objetivo y ámbito de aplicación

Objetivo

1. Las presentes Recomendaciones tienen por objeto aumentar la seguridad en cuanto a las asignaciones de acceso y uso de la información que se genera y resguarda en el Instituto Nacional Electoral, mediante acciones que sirvan para garantizar la integridad, disponibilidad y confidencialidad de la información, en los equipos de cómputo y en los sistemas de información donde ésta se deposita y gestiona.

Ámbito de aplicación

2. Las Recomendaciones están dirigidas a las personas servidoras públicas y/o prestadoras de servicios del Instituto Nacional Electoral que, por razón de su función, cargo o comisión: accedan, manipulen, almacenen y usen archivos digitales y/o electrónicos.

Glosario

3. Para efectos de las presentes Recomendaciones se entenderá por:

A. Siglas y abreviaturas

I. **SAI:** Sistema de Archivos Institucional;
II. **UTSI:** Unidad Técnica de Servicios de Informática;
III. **UTTyPDP:** Unidad Técnica de Transparencia y Protección de Datos Personales.

B. Definiciones

I. **AES:** *Advanced Encryption Standard*, estándar de cifrado avanzado, tipo de algoritmo utilizado para realizar cifrado simétrico;
II. **Biblioteca de documentos:** Espacio destinado para almacenar, crear, editar, adicionar, eliminar y compartir archivos con otras personas usuarias.
III. **Bit:** Dígito del sistema de numeración binario, que se representa con dos valores, el 0 y el 1;
IV. **Carpeta:** Es una estructura que permite agrupar y administrar documentos o archivos relacionados.

V. **Documento de archivo electrónico:** Es el registro de información generada, recibida, almacenada y/o comunicada por medios electrónicos, en razón de las funciones, atribuciones o actividades del Instituto Nacional Electoral, que permanece almacenada electrónicamente durante todo su ciclo de vida y cuenta con al menos un valor administrativo, legal, fiscal y/o contable (valores primarios); valor informativo, evidencial y/o testimonial (valores secundarios) que debe ser tratado conforme a los principios y procesos archivísticos;

VI. **Expediente**: Es la unidad documental constituida por uno o varios documentos de archivo, ordenados y relacionados por un mismo asunto, y se abrirá cuando no exista antecedente de éste, debe contener preferentemente documentos originales, cuando éstos posean elementos probatorios de las funciones, competencias y/o atribuciones del área generadora;

VII. **Lista**: Es una colección de datos que puede compartirse con los miembros de un equipo y con las personas a las que se les ha proporcionado acceso al sitio;

VIII. **Nube**: Término que se utiliza para describir una red mundial de servidores, cada uno con una función única que se encuentran conectados. Estos servidores están diseñados para almacenar y administrar datos, ejecutar aplicaciones o entregar contenido o servicios.

IX. **Sitio:** Espacio virtual en una plataforma de colaboración, que permite el almacenamiento y gestión de la información dentro de una organización. El cual, está conformado por una colección de páginas web, listas, bibliotecas y aplicaciones que se encuentran organizadas de manera lógica y pueden ser personalizadas según las necesidades específicas de un equipo;

X. **Software**: Conjunto de programas de cómputo, procedimientos, reglas, documentación y datos asociados, que forman parte de las operaciones de un sistema informático;

Capítulo II
De las Recomendaciones de para el acceso, uso, almacenamiento y, en su caso, conservación de la información

4. No toda la información del Instituto Nacional Electoral debe estar al alcance de todas las personas servidoras públicas y/o prestadoras de servicios, por lo que se sugiere establecer grupos de trabajo o designar personal de las áreas para que estas tengan acceso únicamente a la información que deben manejar, para con ello garantizar la resolución de ciertos procedimientos y, en su caso, su confidencialidad, así como el cumplimiento de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, Ley General de Transparencia y Acceso a la Información Pública y Ley Federal de Transparencia y Acceso a la Información Pública.

5. No compartir contraseñas o equipos de cómputo entre personas servidoras públicas del Instituto Nacional Electoral o personas externas, sin importar que las primeras se encuentren adscritas a la misma área responsable que el titular de la contraseña o resguardante del equipo de cómputo que se trate.

6. Para ofrecer una colaboración sencilla, se sugiere se utilicen las herramientas colaborativas[1], con el objetivo de permitir que varias personas servidoras públicas y/o prestadoras de servicios trabajen al mismo tiempo en la versión inicial de un documento y evitar que circulen múltiples versiones, incluidas las que puedan distribuirse inadvertidamente y que contengan datos inexactos o incompletos.

En este sentido, a través de los repositorios documentales, particularmente en el servicio de infraestructura de procesamiento, almacenamiento y aplicaciones, como lo es la plataforma *SharePoint*, es posible asignar permisos de acceso a los documentos, para tal efecto se sugiere lo siguiente:

a) Otorgar acceso únicamente a las personas usuarias autorizadas con el nivel de permisos adecuados, entre los que se pueden encontrar los siguientes:

- **Lectura:** Las personas usuarias con permiso de lectura, solo podrán ver el contenido de las carpetas de una biblioteca de documentos, así como realizar la descarga de los mismos.
- **Colaboración y edición:** Este permiso permite agregar, editar, eliminar elementos y documentos del sitio, así como crear subcarpetas y cargar documentos.
- **Control total:** Permite a las personas usuarias tener un control completo sobre el contenido del sitio de la plataforma de colaboración.

b) Hacer uso de bibliotecas de archivos para segregar los permisos de las personas usuarias autorizadas.

c) Generar bibliotecas, una para información pública y otra para información clasificada en la que se asignen permisos de acceso específicos.

d) Se sugiere que el otorgamiento de acceso y permisos a los medios de almacenamiento sea autorizado por la persona responsable de la información.

e) Privilegiar los accesos mínimos necesarios para el desempeño de las funciones o atribuciones de las personas autorizadas.

[1] Con sistemas como Sharepoint/OneDrive o Teams de Microsoft 365, se pueden crear distintos espacios para cada área y grupos de trabajo, para que todas las personas puedan guardar y compartir contenidos, sin perder privacidad, ni seguridad.

f) Establecer periodos de validación y/o actualización de los accesos y permisos otorgados.

Una vez que se cuente con la versión definitiva del documento que se trate, este deberá incluirse en el SAI, para su gestión y, en su caso, integración en el expediente correspondiente, conforme a lo dispuesto en el Capítulo IV de los Lineamientos del Instituto Nacional Electoral en materia de archivos.

7. Para el caso de los sistemas de información utilizados en el Instituto Nacional Electoral, así como las carpetas compartidas que se generen, se sugiere contar con un rol en cada área responsable, a través del cual se solicite, exclusivamente, o, en su caso, otorgue, los accesos de las personas servidoras públicas al sistema o carpeta compartida que se trate, con la finalidad de controlar el personal que podrá visualizar, utilizar y gestionar la información.

8. Se recomienda que la persona que fungirá con el rol señalado en el numeral anterior sea designada por el titular del área responsable de la información.

9. Para el módulo e-oficio del SAI, el rol señalado en el numeral 7 se denominará facilitador. Se sugiere exista mínimo 1 y hasta 3 por órgano responsable, quienes otorgarán directamente los accesos al módulo e-oficio, a efecto de optimizar la gestión documental del Instituto Nacional Electoral.

10. Para el caso del módulo e-archivo del SAI, se recomienda que la persona que solicite los accesos al Archivo Institucional sea exclusivamente la persona designada como responsable del archivo de trámite del área responsable o, en su caso, su suplente.

11. Para las carpetas compartidas se recomienda, cuando se considere necesario por la información resguardada en ellas, restringir selectivamente el acceso a determinado contenido, categorizando los archivos por niveles, teniendo en cada nivel diferentes permisos de acceso.

12. Previo a la entrada en vigor de sistemas informáticos, como el SAI, cada persona servidora pública puede que posea información considerada documentos de archivo electrónicos en unidades de almacenamiento (equipos de cómputo, unidades USB, etc.), por lo que en estos casos se recomienda, recopilar todos los documentos de archivo electrónicos dispersos en diferentes ubicaciones en un lugar común, aplicando la normatividad en materia de archivos para su identificación y expedientación. De esta manera, se protegerá la información y se pondrá disposición de manera expedita cuando sea necesario. Existen distintas opciones para almacenar información y datos, tanto de forma física (unidad de almacenamiento externa) o en la nube.

13. Los documentos digitalizados y/o electrónicos que se cargue en los módulos e-oficio y e-archivo del SAI se limitan a 300 MB por cada uno, por lo cual, si los

documentos digitalizados y/o electrónicos sobrepasan dicha capacidad, se sugiere se generen tantos archivos como sean necesarios para poder cargarlos en el SAI.

Capítulo III
De las medidas de seguridad

14. Para los casos en donde se utilicen medios de almacenamiento extraíbles para resguardar información se recomienda considerar:

a) Medidas de seguridad físicas

i. Evitar derramar líquidos sobre el medio de almacenamiento.

ii. Evitar que sufra caídas o golpes.

iii. Evitar ponerlo en contacto de gases inflamables o corrosivos.

iv. Mantenerlos en lugares que no permitan la humedad, exceso de polvo.

v. Mantenerlos en lugares de acceso controlado y accesible sólo por las personas autorizadas.

vi. Mantenerlo en lugares que dificulten la posibilidad de que pueda ser sustraído, robado o dañado.

vii. Etiquetar el medio de almacenamiento en función de la clasificación o sensibilidad de la información que contiene.

viii. Hacer uso de medios de autenticación física para el acceso a los medios de almacenamiento, por ejemplo:

a. Identificación

b. Listas de acceso

c. Lectores biométricos

d. Tarjetas de proximidad

b) Medidas de seguridad lógicas

i. Usar contraseñas de acceso o cifrado, utilizando algoritmo de cifrado simétrico, como por ejemplo AES, con llaves de cifrado de al menos 256 bits, en caso de que los documentos de archivo electrónico sean clasificados como información reservada y/o confidencial.

ii. Utilizar elementos que garanticen la integridad y autenticidad de los documentos de archivo electrónico, tales como: la Firma Electrónica Avanzada Institucional y códigos de integridad (Hash) utilizando

algoritmos robustos, como lo es el algoritmo SHA con una longitud de al menos 256 bits.

iii. En caso de daño, término de vida útil, fin de arrendamiento o cambio de uso de un medio de almacenamiento masivo que contenga documentos de archivo electrónico, realizar la destrucción del medio o el borrado de la información de tal forma que esta no pueda ser recuperada.

15. Para los casos donde se utilice infraestructura tecnológica de almacenamiento, como parte de un sistema, se recomienda considerar:

a) Medidas de seguridad físicas:

i. Contar con un proceso de autorizaciones para el acceso físico al medio de almacenamiento.

ii. Autenticación física como lo son identificaciones oficiales y/o institucionales, así como listas de control de acceso.

iii. Mecanismos de lectores biométricos.

iv. Tener puertas de seguridad.

v. Contar con controles de seguridad física que permitan detectar y minimizar afectaciones como polvo, fuego, humedad, entre otros elementos.

vi. Con la finalidad de mejorar la confiabilidad, el rendimiento y/o la capacidad de recuperación de datos, se estima relevante hacer uso de la Matriz redundante de discos independientes (Redundant Array of Independent Disks en sus siglas en ingles "*RAID"*), dicho software permite configurar arreglos de disco 1 o 5, para que en caso de dañarse alguno de los medios de almacenamiento principales, a través de mecanismos *Hot Swap*, puedan ser sustituidos y regenerados, sin la necesidad de realizar el apagado del dispositivo.

vii. Redundancia (Red, *hardware, software*, entre otros): Implementar configuraciones de alta disponibilidad en hardware y red, de copias de seguridad para los datos, así como sitios en caliente o en frío para edificios o *Sites.*

b) Medidas de seguridad lógica:

i. Contar con un proceso de autorizaciones para el acceso lógico al medio de almacenamiento masivo.

ii. Contar con un inventario de dispositivos permitidos para conexión y uso en la infraestructura tecnológica de almacenamiento masivo.

iii. Utilizar contraseñas de acceso o realizar el cifrado de la información.

iv. Considerar el uso de elementos que garanticen la integridad y autenticidad de los documentos de archivo electrónico.

v. En caso de daño, término de vida útil, fin de arrendamiento o cambio de uso de la infraestructura tecnológica de almacenamiento masivo que contenga documentos de archivo electrónico, realizar la destrucción del medio o borrado de la información de tal forma que esta no pueda ser recuperada.

16. Se recomienda hacer uso de infraestructura de almacenamiento proporcionada por el Instituto Nacional Electoral y/o servicios de nube bajo su contratación, lo anterior para la información que por su clasificación sea considerada reservada o confidencial.

17. Cuando se determine que la información contenida en un documento electrónico ha cumplido con su vida útil, se estima relevante realizar el borrado seguro de éste. En ese sentido, como medida de seguridad, o bien como última instancia se puede recurrir a la destrucción del medio de almacenamiento, de tal manera que dicha información no pueda ser recuperada.

Por cuanto hace al borrado seguro, se recomienda la utilización de los métodos de borrado lógicos; estos son aquellos que implican la sobre-escritura o modificación del contenido del medio de almacenamiento electrónico, de tal forma que la información no pueda ser recuperada.

En la siguiente tabla se muestran diversos métodos de borrado a nivel lógico. Estos métodos, realizan el borrado de la información de tal forma que sea muy difícil recuperar la información borrada, en ese sentido, mientras el nivel de seguridad sea mayor, el nivel de esfuerzo y recursos de cómputo necesarios para recuperar la información se incrementa de manera considerable. Por lo que, los métodos de borrado que a continuación se señalan son considerados seguros:

Método de borrado	Características de la sobreescritura aplicada el medio de almacenamiento	Nivel de seguridad
Grado 1. Super Fast Zero Write	Este método sobrescribe el área de datos con un valor fijo (0x00) una vez cada tres sectores.	Bajo
Grado 2. Fast Zero Write	Este método sobrescribe el área de datos con un valor fijo (0x00) una vez en todos los sectores.	Bajo
Grado 3. Zero Write	Este método sobrescribe el área de datos con un valor fijo (0x00) en toda el área.	Bajo
Grado 4. Random Write	Este método sobrescribe el área de datos con valores aleatorios. La fiabilidad aumenta con la cantidad de pasadas.	Medio
Grado 5. Random &	Este método sobrescribe el área en cuatro	Medio

Método de borrado	Características de la sobreescritura aplicada el medio de almacenamiento	Nivel de seguridad
Zero Write	pasos consecutivos: 1. Con valores aleatorios, 2. Con un valor fijo (0x00), 3. Nuevamente con valores aleatorios y, 4. Con valor cero	
Grado 6. US Navy, NAVSO P5239-26 – MFM. Para discos codificados con MFM (Modified Frequency Modulation)	Método utilizado por los EE.UU. Navy que sobrescribe el área de datos en cuatro pasos consecutivos: 1. Valor fijo (0xffffffff), 2. Valor fijo (0xbfffffff), 3. Valores aleatorios y 4. Se verifica la sobre-escritura.	Medio
Grado 7. US Navy, NAVSO P5239-26 – RLL. Para discos duros y soportes ópticos (CD, DVD, Blue Ray)	Método utilizado por los EE.UU. Navy que sobrescribe el área de datos en cuatro pasos consecutivos: 1. Valor fijo (0xffffffff), 2. Valor fijo (0x27ffffff), 3. Valores aleatorios y 4. Se verifica la sobre-escritura.	Medio
Grado 8. Bit Toggle	Este método sobrescribe el área en cuatro pasos consecutivos: 1. Con un valor (0x00) 2. Con un valor (0xff) 3. Con un valor (0x00) 4. Con un valor (0xff)	Medio
Grado 9. Random Random Zero	Este método sobrescribe el área en cuatro pasos consecutivos: 1. Dos veces con valores aleatorios, 2. Con valor fijo (0x00), 3. Dos veces con valores aleatorios y 4. Con ceros	Medio
Grado 10. US Department of	Método de borrado presentado por el Departamento de Defensa de EE.UU.	Medio

Método de borrado	Características de la sobreescritura aplicada el medio de almacenamiento	Nivel de seguridad
Defense (DoD 5220.22-M)	(Pentágono). Este método sobrescribe el área en cuatro pasos consecutivos: 1. Con un valor fijo determinado, 2. Con un valor complementario (0xff), 3. Con valores aleatorios y 4. Se verifica la sobre-escritura.	
Grado 11. US Air Force, AFSSI5020	Método de borrado presentado por la Fuerza Aérea estándar de los EE.UU**.** Este método sobrescribe el área en cuatro pasos consecutivos: 1. Con un valor fijo (0x00), 2. Con un valor fijo (0xff), 3. Con un valor aleatorio constante y 4. Se verifica la sobre-escritura en al menos 10% del área de datos.	Alto
Grado 12. North Atlantic Treaty Organization (OTAN) NATO standard	Método de borrado presentado por el Tratado del Atlántico Norte Organización (OTAN). Este método sobrescribe el área de datos de destino 7 veces de la siguiente manera: 1. Las primeras seis veces sobrescribe con los valores fijos (0x00) y (0xff) de forma alternada y 2. El séptimo con un valor aleatorio.	Alto
Grado 13. Peter Gutmann Secure Deletion	Método introducido por Peter Gutmann. Este es quizás el método de eliminación más seguro disponible. Este método sobrescribe 35 veces en total de la siguiente manera: 1. Sobrescribe el área de datos con valores aleatorios cuatro 4 en cada sector, 2. Después con valores pseudo aleatorios sobre cada sector por 27 pasadas y	Alto

Método de borrado	Características de la sobreescritura aplicada el medio de almacenamiento	Nivel de seguridad
	3. Con valores aleatorios durante 4 pasadas sobre cada sector.	
Grado 14. US Department of Defense (DoD 5220.22-M) + Gutmann Method	Combina la metodología de grado 13 y 10 con un total de 35 pasadas.	Muy Alto

Capítulo IV
Consideraciones generales para la interoperabilidad y disponibilidad de los documentos electrónicos

18. La interoperabilidad y la disponibilidad de los documentos electrónicos son dos aspectos clave para garantizar la accesibilidad y seguridad de los documentos electrónicos.

En virtud de lo anterior, se mencionan algunas consideraciones generales para que los documentos electrónicos puedan ser compatibles y consultados en diferentes equipos y/o sistemas:

a) Incluir metadatos en los documentos electrónicos.

b) Generar los documentos electrónicos de manera que puedan ser exportados a diferentes formatos, según sea necesario. esto garantizará que los documentos puedan ser leídos y utilizados en diferentes sistemas y/o aplicaciones a medida que evoluciona la tecnología.

c) Evitar generar copias de los documentos electrónicos en distintos repositorios para sistemas distintos, en su lugar se recomienda copiar la referencia a la ubicación del documento.

19. La UTTyPDP, a través del Archivo Institucional, así como la UTSI, apoyará en asesorar sobre aspectos relativos la seguridad, asignación de acceso, uso, almacenamiento y conservación de la información.