Director General, Directoras, y Directores de área y de plantel y Titular del Órgano Interno de Control.

P R E S E N T E

San Juan Tilcuautla, Mpio. De San Agustín Tlaxiaca, Hgo., 16 de febrero, 2026.

CRITERIOS DEL BUEN USO DE LA TECNOLOGÍA Y LA INFORMACIÓN DIGITAL DEL COLEGIO DE ESTUDIOS CIENTÍFICOS Y TECNOLÓGICOS DEL ESTADO DE HIDALGO

Sección primera
Generales

I. Objetivo

El objetivo de estos lineamientos es establecer un conjunto de directrices claras y prácticas para el manejo responsable y seguro de la información digital en el Colegio de Estudios Científicos y Tecnológicos del Estado de Hidalgo, con la finalidad de asegurar que todos los usuarios comprendan la importancia de proteger la información digital, siguiendo criterios que minimicen los riesgos asociados a su uso y aseguren su integridad, confidencialidad y disponibilidad. Buscando propiciar un aumento de la seguridad y aprovechamiento de la tecnología, la cual impacta de manera determinante y permite aumentar la eficiencia en el trabajo.

II. Justificación

El uso de tecnologías de la información ha crecido exponencialmente, aumentando los riesgos asociados a la gestión de la información digital. Las brechas y vulnerabilidades pueden comprometer la integridad y confidencialidad de los datos, afectando negativamente al Colegio, para esto es necesario gestionar la información digital a tres niveles: aseguramiento y control sobre la infraestructura (nivel físico), plataformas digitales (nivel lógico) y medidas organizacionales (factor humano).

La implementación rigurosa de estos lineamientos asegurará que el Colegio se mantenga en un estado de seguridad óptimo, protegiendo sus datos y plataformas digitales contra amenazas internas y externas.

III. Para los efectos de los presentes lineamientos, se entenderá por:

Activo Informático: Dispositivos electrónicos, hardware, software o recursos de tecnología que la institución asigna a un usuario para la realización de sus funciones laborales, como computadoras, servidores y equipos de telecomunicaciones.

Autenticación Multifactorial (MFA): Proceso de seguridad que requiere más de un método de verificación para confirmar la identidad del usuario, como una contraseña combinada con un código enviado al teléfono móvil.

CECyTEH: Colegio de Estudios Científicos y Tecnológicos del Estado de Hidalgo.

Clasificación de la Información: Proceso de organizar la información en diferentes categorías o niveles de confidencialidad, tales como pública, restringida o confidencial, para su protección y gestión adecuada.

Cifrado de Datos: Técnica de seguridad que convierte la información en un formato codificado que solo puede ser leído o descifrado por las personas autorizadas, protegiendo así la confidencialidad de los datos.

Confidencialidad: Propiedad de la información que asegura que solo las personas autorizadas pueden acceder a los datos sensibles, evitando su divulgación no autorizada.

Control de Acceso: Mecanismo de seguridad que restringe el acceso a recursos informáticos y datos a usuarios específicos en función de su rol o responsabilidades dentro de la institución.

Datos Sensibles: Información que, por su naturaleza, puede afectar la privacidad o los derechos de las personas si es divulgada, tales como información médica, financiera, o datos personales.

Disponibilidad: Propiedad de la información que asegura que los datos y recursos están accesibles para los usuarios autorizados cuando los necesitan, garantizando la continuidad de las operaciones.

DG: Dirección General del Colegio de Estudios Científicos y Tecnológicos del Estado de Hidalgo

DTI: Dirección de Tecnologías de la Información

Integridad de la Información: Garantía de que los datos no han sido alterados o manipulados de manera no autorizada, y que se mantienen completos y consistentes.

Política de Seguridad: Conjunto de reglas y procedimientos establecidos para proteger los sistemas informáticos y la información de una organización, asegurando la integridad, confidencialidad y disponibilidad de los datos.

Privilegios de Acceso: Permisos o niveles de acceso asignados a los usuarios para realizar acciones específicas dentro de un sistema de información, como consultar, modificar o eliminar datos.

Restauración de Datos: Proceso de recuperación de datos desde un respaldo en caso de pérdida, corrupción o eliminación accidental de la información original.

SIAA: Sistema de Información Académica Administrativa

SIGA: Sistema Integral de Gestión Administrativa

TI: Tecnologías de la Información

Transparencia: Obligación de la institución de permitir el acceso claro y comprensible a la información pública, garantizando el derecho de las personas a conocer cómo se manejan los datos y recursos.

Usuario: Persona que interactúa con las plataformas digitales y accede a los recursos informáticos de la institución, ya sea directivo, personal administrativo o docente.

Vulnerabilidad: Cualquier debilidad en una plataforma digital que puede ser explotada para comprometer la seguridad de los datos o sistemas, ya sea de manera accidental o intencionada.

IV. Alcance

Las disposiciones del presente lineamiento son aplicables y de observancia obligatoria para todo personal directivo, de apoyo y de asistencia a la educación, que utilizan la infraestructura tecnológica del Colegio, incluyendo tanto equipos y sistemas propios (SIGA y SIAA), extendiéndose a cualquier dispositivo externo conectado a la red del Colegio, emitidos por la Dirección de Tecnologías de la Información.

V. Marco Jurídico

a. Constitución Política de los Estados Unidos Mexicanos.
b. Ley General de Transparencia y Acceso a la Información Pública.
c. Norma Oficial Mexicana NOM-151-SCFI-2016 (Conservación de mensajes de datos y digitalización).
d. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPSO).
e. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Hidalgo.
f. Ley de Responsabilidades Administrativas del Estado de Hidalgo.
g. Ley de Entidades Paraestatales del Estado de Hidalgo.
h. Ley Orgánica del CECyTEH.
i. Código de conducta del CECyTEH.
j. Condiciones Generales de trabajo del CECyTEH.

Segunda sección
Activos Tecnológico

1. Los usuarios que tengan un activo tecnológico asignado de manera personal para el desempeño de sus funciones, son los únicos responsables tanto de su utilización como de la integridad de la información digital contenida en dichos dispositivos, incluyendo su correcta utilización, salvaguardando la confidencialidad de los datos y accesos que puedan estar almacenados en los mismos.
2. Bajo ninguna circunstancia se deberá compartir el activo tecnológico, las credenciales de acceso con terceros y/o la divulgación o mal uso de la información contenida en dicho activo, a menos que sea estrictamente necesario para labores institucionales y únicamente con autorización previa; en caso de compartir o prestar el activo tecnológico para fines laborales, el usuario no quedará exento de su responsabilidad total sobre dicho equipo.
3. Toda movilización de activos tecnológicos, ya sea dentro o fuera de las instalaciones de Planteles y DG, es exclusiva responsabilidad del resguardante, quien deberá garantizar el traslado seguro y su adecuada protección frente a daños, extravíos o acceso no autorizado a la información, bajo la previa notificación y autorización del Director de plantel o Director de área, según corresponda.
4. No está permitido el uso de activos tecnológicos institucionales para fines personales o ajenos a las actividades laborales y cualquier violación a este lineamiento será sujeto a las sanciones correspondientes.
5. Los usuarios deberán asegurarse de que los activos tecnológicos que se movilicen cuenten con las medidas de seguridad necesarias, como cifrado de datos, contraseñas robustas, y sistemas de autenticación múltiple, a fin de prevenir accesos no autorizados a la información confidencial. Asimismo, deberán estar atentos a realizar respaldos periódicos de la información digital crítica, de conformidad con lo establecido en la sección **Respaldo y Recuperación**.

Tercera sección
Clasificación de la Información

6. El encargado de cada plataforma digital ofrecida por el Colegio, es responsable de la información que este servicio genera y procesa.

7. Los directores de cada plantel y directores de área en Dirección General, deben informar a su personal administrativo y docente de la relevancia e importancia de la información a su cargo para su adecuado tratamiento.

8. Los usuarios responsables de resguardar información digital, deben garantizar que ésta se encuentre protegida para asegurar su integridad y confidencialidad, de acuerdo a su clasificación. La información puede almacenarse en formato digital o servicios de alojamiento en la nube.

9. Todo usuario, directivo, administrativo y docente, deberá hacer uso de la información digital a la que tenga acceso únicamente para propósitos relacionados con el cumplimiento de sus funciones, debiendo resguardar principalmente la relativa a datos personales, absteniéndose de comunicarlos a terceros sin el consentimiento expreso de la persona a la que se refieren.

10. Todos los usuarios que hacen uso de información digital clasificada como restringida o confidencial, evitarán que sea accedida por personas no autorizadas.

Cuarta sección
Acceso a la Información

11. El personal a cargo de las plataformas digitales, es responsable de autorizar el nivel de acceso con privilegios mínimos necesarios para que el personal directivo, administrativo y docente realicen sus funciones.

12. Ninguna persona debe ver, copiar, alterar o destruir la información digital que reside en los equipos de cómputo y servidores sin el consentimiento por escrito institucional del responsable del equipo o creador de la información digital.

13. Los usuarios deben acceder solo a los recursos necesarios para su trabajo o consulta.

14. A toda persona que deje tener relación laboral con el Colegio, le será cancelado su acceso de manera definitiva a los sistemas y recursos tecnológicos institucionales. El Departamento de Personal comunicará vía correo electrónico, escrito institucional o SIAA, a la DTI de toda alta, baja o cambio del personal, para que se tomen las medidas correspondientes de privilegios de acceso a los servicios de manera inmediata o lo más pronto posible.

Quinta sección
Intercambio de la información

15. Todo convenio que tenga CECyTEH con terceras personas para compartir información digital reservada y/o confidencial, deberá apegarse a las disposiciones de las leyes, reglamentos y demás instrumentos normativos relacionados con acceso a la información pública y protección de datos personales.

16. Los usuarios deben asegurarse que la información digital que utilice proviene de fuentes confiables y verificadas, revisando autores o sitios web, los cuales deben de ser citados para dar crédito a la fuente.

Sexta sección
Cuentas de Usuario y Contraseña

17. Todas las cuentas de usuario y su respectiva contraseña de acceso a las plataformas digitales del Colegio, así como a los de telefonía, son personales, permitiéndose el uso bajo la responsabilidad del usuario única y exclusivamente durante la vigencia de su relación laboral.

18. La vigencia de las cuentas de usuarios es facultad de la DTI, éstas son habilitadas, suspendidas o canceladas por el área en consideración a las solicitudes, necesidades y conductas de los usuarios.

19. Todo usuario debe actualizar la contraseña de su cuenta de acceso a las plataformas digitales de manera periódica (al menos cada 6 meses) o cuando sospeche de su divulgación. La contraseña debe ser de al menos 8 caracteres alfanuméricos.

20. Las contraseñas no deben ser compartidas con otros usuarios.

21. Las contraseñas no deben ser almacenadas en archivos de texto o lugares accesibles a otros.

22. Se debe utilizar autenticación multifactorial para cuentas de alto riesgo.

23. Los usuarios recibirán información y recomendaciones de la DTI sobre la importancia y mejores prácticas de seguridad de contraseñas por medio de correo electrónico institucional.

24. Cuando se requiera acceder a información digital de un equipo de cómputo o cuenta de correo institucional de una persona ausente, ya sea por cuestiones de salud, por estar comisionado a actividades fuera de su área de trabajo u otro motivo no especificado, el responsable de la dirección, ya sea plantel o de área, deberá solicitar por medio de correspondencia en SIAA a la DTI o enlace de TI que brinde el acceso al equipo y/o servicio de correo para poder dar continuidad al proceso institucional.

25. Únicamente personal de la DTI proporcionará acceso al responsable de la Dirección de área o plantel correspondiente que lo haya solicitado a efecto de que sustraiga la información necesaria, dejando constancia de ello bajo solicitud vía SIAA o correo electrónico institucional.

26. En caso de que un Director de área o plantel solicite el acceso a un equipo institucional bajo su mando, la DTI o enlace de TI proporcionará el acceso para sustraer la información necesaria, dejando constancia de ello bajo la previa solicitud vía correo electrónico, escrito institucional o SIAA. El tiempo máximo de respuesta será de 48 horas, considerando días hábiles, según los establecido en la sección **"Políticas de Seguridad"**.

Séptima sección
Respaldo y Recuperación

27. Es responsabilidad de cada usuario identificar, clasificar y respaldar de forma regular los datos críticos y sensibles generados o almacenados en los activos tecnológicos bajo su control. Estos

datos incluyen, información digital confidencial del Colegio, documentos administrativos esenciales, datos financieros y cualquier archivo necesario para la continuidad operativa.

28. El respaldo debe realizarse en servicios de alojamiento digital autorizadas, así como en dispositivos de almacenamiento físico seguro, tales como discos duros externos cifrados o unidades flash certificadas.

29. Bajo ninguna circunstancia deben utilizarse servicios o dispositivos no aprobados por la DTI, a fin de evitar riesgos de seguridad.

30. La restauración de información digital debe ser probada al menos una vez al año para validar la integridad del proceso.

31. Los respaldos deben almacenarse en lugares seguros, preferiblemente en ubicaciones fuera del sitio principal de operación, para proteger la información digital contra riesgos físicos como incendios, inundaciones o robos. Según lo establecido en la sección "**Plan de Contingencia Digital**".

32. Los usuarios no deben almacenar los respaldos en ubicaciones personales o dispositivos sin cifrado y el acceso a los mismos deberá estar estrictamente controlado y documentado por él mismo.

33. En caso de un incidente de pérdida de datos, el usuario deberá informar inmediatamente a la DTI o enlace TI, vía SIAA o correo electrónico institucional, para iniciar los procedimientos de recuperación.

Octava Sección
Políticas de Seguridad

34. Todo personal directivo, administrativo y docente es responsable del buen uso de los servicios tecnológicos institucionales alojados en cada uno de los planteles y DG, asignados para realizar sus funciones administrativas, académicas y de consulta.

35. Personal de la DTI y enlaces TI quedan facultados para acceder a los equipos de cómputo institucionales, aun en aquellos que no están a su resguardo, para:

    a) Revisiones con base en el cumplimiento de medidas de seguridad digital como antivirus y actualizaciones.
    b) Revisión de software y hardware.
    c) Por ausencia de la persona resguardante de la información digital o activo tecnológico, con previa solicitud del director de plantel o área correspondiente, cuando requiera acceder a información y/o servicios con base a sus funciones; a petición del Órgano interno de control, para realizar una revisión de seguridad digital y descartar uso no debido (posibles daños intencionales a información digital, equipo y/o personas) del equipo de cómputo, bajo previa notificación al usuario, vía SIAA o correo electrónico institucional, como se especifica en el presente documento.
    d) En caso de ausencia e imposibilidad de localizar al usuario, la notificación se realizará a el director de plantel o área correspondiente vía SIAA o correo electrónico institucional.

36. La Dirección de Tecnologías de la Información desactivará aquellas plataformas, servicios y puertos de red que no sean necesarios para el desempeño de sus funciones. Lo anterior, con la finalidad de prevenir vulnerabilidades y garantizar la integridad de la información.

37. Personal de DTI, así como enlaces de TI, implementarán medidas físicas para proteger plataformas digitales e información digital, como cerraduras y acceso controlado.

38. Uso de internet.

    a) Respecto al servicio, las redes institucionales se consideran como herramienta de trabajo, por lo que todo usuario deberá utilizarlo exclusivamente para apoyo a sus actividades académicas y/o administrativas en el Colegio y/o DG.
    b) Todo usuario que descargue información digital y archivos de Internet mediante el navegador web u otro medio como FTP y mensajería instantánea, deberá omitirlo cuando sea de sitios web no confiables, correos electrónicos no solicitados, archivos con extensiones inusuales o no se tenga certeza de la fuente.

Novena sección
Transparencia y Rendición de Cuentas

39. Todo usuario que interactúe con las plataformas digitales del Colegio debe tener pleno conocimiento de cómo se recopilan, utilizan, procesan y publican los datos que maneja. Esto incluye comprender claramente los propósitos para los cuales se obtienen los datos, las bases legales que sustentan su tratamiento y los derechos que asisten a los propietarios de la información, en cumplimiento con las normativas de protección de datos personales vigentes, como la Ley Federal de Protección de Datos Personales.

40. Aquellos usuarios que tengan acceso a información sensible, como datos personales, información financiera, o cualquier otro tipo de contenido confidencial, asumen la responsabilidad plena de su protección y gestión ética. Esto implica implementar medidas adecuadas de seguridad para evitar accesos no autorizados, en cumplimiento a lo establecido en la sección "**Políticas de Seguridad**".

41. Los usuarios deberán actuar con integridad en todas las etapas del tratamiento de la información digital, garantizando que solo el personal autorizado y acreditado tenga acceso a dicha información, cualquier acto negligente o malintencionado en la gestión de datos podrá derivar en sanciones disciplinarias o legales, según las normativas aplicables.

	Elaboró:	Revisó:	Autorizó:
Puesto:	**Director de Tecnologías de la Información**	**Director Jurídico**	**Director General**
Fecha:			
Nombre y Firma:	**Ing. Aldo Serafín Pedraza Montiel**	**Lic. Daniel Pérez Becerra**	**Lic. José Edmundo Ramírez Martínez**