



esPOCH

Secretaría
General

RESOLUCIÓN 426.CP.2026

El Consejo Politécnico en sesión ordinaria realizada el día martes 23 de junio del año 2026.

CONSIDERANDO:

Que, el artículo 26 de la Constitución de la República del Ecuador establece que la educación es un derecho de las personas a lo largo de su vida y un deber ineludible e inexcusable del Estado. Constituye un área prioritaria de la política pública y de la inversión estatal, garantía de la igualdad e inclusión social y condición indispensable para el buen vivir. Las personas, las familias y la sociedad tienen el derecho y la responsabilidad de participar en el proceso educativo;

Que, el artículo 27 de la Constitución de la República del Ecuador establece la educación se centrará en el ser humano y garantizará su desarrollo holístico, en el marco del respeto a los derechos humanos, al medio ambiente sustentable y a la democracia; será participativa, obligatoria, intercultural, democrática, incluyente y diversa, de calidad y calidez; impulsará la equidad de género, la justicia, la solidaridad y la paz; estimulará el sentido crítico, el arte y la cultura física, la iniciativa individual y comunitaria, y el desarrollo de competencias y capacidades para crear y trabajar. La educación es indispensable para el conocimiento, el ejercicio de los derechos y la construcción de un país soberano, y constituye un eje estratégico para el desarrollo nacional;

Que, el artículo 350 de la Constitución de la República dispone que el Sistema de Educación Superior tiene como finalidad la formación académica y profesional con visión científica y humanista; la investigación científica y tecnológica; la innovación, promoción, desarrollo y difusión de los saberes y las culturas; la construcción de soluciones para los problemas del país, en relación con los objetivos del régimen de desarrollo;

Que, el artículo 351 de la Constitución de la República del Ecuador establece que el Sistema de Educación Superior estará articulado al sistema nacional de educación y al Plan Nacional de Desarrollo; la ley establecerá los mecanismos de coordinación del Sistema de Educación Superior con la Función Ejecutiva. Este sistema se regirá por los principios de autonomía responsable, cogobierno, igualdad de oportunidades, calidad, pertinencia, integralidad, autodeterminación para la producción del pensamiento y conocimiento, en el marco del diálogo de saberes, pensamiento universal y producción científica tecnológica global;

Que, el artículo 355 de la Constitución de la República del Ecuador, establece: "El Estado reconocerá a las universidades y escuelas politécnicas autonomía académica, administrativa, financiera y orgánica, acorde con los objetivos del régimen de desarrollo y los principios establecidos en la Constitución. - Se reconoce a las universidades y escuelas politécnicas el derecho a la autonomía, ejercida y comprendida de manera solidaria y responsable. Dicha autonomía garantiza el ejercicio de la libertad académica y el derecho a la búsqueda de la verdad, sin restricciones; el gobierno y gestión de sí mismas, en consonancia con los principios de alternancia, transparencia y los derechos políticos; y la producción de ciencia, tecnología, cultura y arte (...)"

Que, el artículo 98 del Código Orgánico Administrativo, establece: "Acto administrativo es la declaración unilateral de voluntad, efectuada en ejercicio de la función administrativa que produce efectos jurídicos individuales o generales, siempre que se agote con su cumplimiento y de forma directa. Se expedirá por cualquier medio documental, físico o digital y quedará constancia en el expediente administrativo."

Que, el artículo 100 del Código Orgánico Administrativo, establece: Motivación del acto administrativo. En la motivación del acto administrativo se observará: 1. El señalamiento de la norma jurídica o principios jurídicos aplicables y la determinación de su alcance. 2. La calificación



Riobamba-Ecuador
Panamericana Sur km 1 1/2
Código Postal: EC060155

Teléfono: 593 (03) 2998-200
Telefax: (03) 2 317-001

esPOCH.edu.ec



esPOCH

Secretaría
General

de los hechos relevantes para la adopción de la decisión, sobre la base de la evidencia que conste en el expediente administrativo. 3. La explicación de la pertinencia del régimen jurídico invocado en relación con los hechos determinados. Se puede hacer remisión a otros documentos, siempre que la referencia se incorpore al texto del acto administrativo y conste en el expediente al que haya tenido acceso la persona interesada. Si la decisión que contiene el acto administrativo no se deriva del procedimiento o no se desprende lógicamente de los fundamentos expuestos, se entenderá que no ha sido motivado.

Que, el artículo 17 de la Ley Orgánica de Educación Superior manifiesta: "**Reconocimiento de la autonomía responsable.**- El Estado reconoce a las universidades y escuelas politécnicas autonomía académica, administrativa, financiera y orgánica, acorde con los principios establecidos en la Constitución de la República.- En el ejercicio de autonomía responsable, las universidades y escuelas politécnicas mantendrán relaciones de reciprocidad y cooperación entre ellas y de estas con el Estado y la sociedad; además observarán los principios de justicia, equidad, solidaridad, participación ciudadana, responsabilidad social y rendición de cuentas";

Que, el artículo 18 literal c) de la Ley Orgánica de Educación Superior, establece: Conocer y resolver sobre los distintos asuntos relativos a la docencia, investigación, vinculación y gestión administrativa, que rebasen las atribuciones de otras instancias institucionales;

Que, el artículo 18 letras b), e), de la Ley Orgánica de Educación Superior, establece: que la autonomía responsable que ejercen las universidades y escuelas politécnicas consiste en: "b) La libertad de expedir sus estatutos en el marco de las disposiciones de la presente Ley; e) La libertad para gestionar sus procesos internos;

Que, el artículo 2 del Estatuto de la Escuela Superior Politécnica de Chimborazo, establece: **Misión.-** Formar profesionales integrales con proyección internacional, promoviendo la investigación, innovación y la transferencia de la ciencia y la tecnología para contribuir a la sostenibilidad social, ambiental y económica de la región y el país.

Que, el artículo 3 del Estatuto de la Escuela Superior Politécnica de Chimborazo, establece: **Visión.** - Ser una institución de educación superior reconocida a nivel nacional e internacional por su liderazgo en la formación, transferencia de conocimientos y diálogo de saberes, contribuyendo al desarrollo sostenible de la sociedad

Que, el artículo 31 del Estatuto de la Escuela Superior Politécnica de Chimborazo, **Atribuciones y deberes del Consejo Politécnico.** - señala: **literal e)** Conocer y resolver sobre los distintos asuntos relativos a la docencia, investigación, vinculación y gestión administrativa, que rebasen las atribuciones de otras instancias institucionales; (...).

Que, mediante Resolución 785.CP.2024, se resolvió: **Artículo 1.** - Derogar las Resoluciones 222.CP.2018 y 040.CP.2024. **Artículo 2.-** Aprobar las Políticas de Seguridad Informática, de acuerdo al pedido remitido mediante Oficio Nro. 2106-DTIC-ESPOCH-2024, suscrito por el Ing. Diego Bernardo Palacios Campana, Director Tecnologías de la Información y Comunicación, de conformidad con el documento adjunto. **Artículo 3.-** Delegar al Secretario General de la ESPOCH, o su delegado, para que en representación de la ESPOCH actúe en calidad de abogado y proceda a participar en las políticas de la Superintendencia de Protección de Datos Personales dentro de las políticas de seguridad informática institucional, protección de Datos para instituciones públicas..."

Que, se conoció el Oficio No. DJ-ESPOCH-MLPC-032-2026, suscrito por la Abg. Marcela Parra Carrasco, ANALISTA DE NORMATIVA Y CONSULTA 3., quien indica: "Con un cordial saludo, en atención al trámite reasignado mediante el Sistema de Gestión Documental Institucional, referente al Oficio Nro. 0792-DTIC-ESPOCH-2026, firmado electrónicamente



Riobamba-Ecuador
Panamericana Sur km 1½
Código Postal: EC060155

Teléfono: 593 (03) 2998-200
Telefax: (03) 2 317-001

esPOCH.edu.ec



esPOCH

Secretaría
General

por el Ing. Diego Bernardo Palacios Campana, DIRECTOR TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN, por medio del que manifiesta: "(...) Me permito solicitar de la manera más comedida se proceda con la elaboración del informe jurídico correspondiente, con el fin de sustentar la aprobación de la actualización de las Políticas de Seguridad Informática ante el Consejo Politécnico. Esta solicitud se fundamenta en la necesidad de garantizar que dichas políticas se encuentren alineadas con la normativa legal vigente, así como con las mejores prácticas en materia de seguridad de la información, fortaleciendo de esta manera la protección de los activos tecnológicos institucionales y la adecuada gestión de riesgos. Asimismo, el informe permitirá contar con un respaldo técnico y legal que facilite la toma de decisiones por parte del Consejo Politécnico, asegurando cumplimiento normativo y mejora continua en los procesos institucionales. (...)"; al respecto cúmpleme con informar a su autoridad lo siguiente: ANTECEDENTES: - El Consejo Politécnico en sesión extraordinaria realizada el día lunes 30 de diciembre del año 2024, mediante RESOLUCIÓN 785.CP.2024, resolvió expedir el: "(...)Artículo 2.- Aprobar las Políticas de Seguridad Informática, de acuerdo al pedido remitido mediante Oficio Nro. 2106-DTIC-ESPOCH-2024, suscrito por el Ing. Diego Bernardo Palacios Campana, Director Tecnologías de la Información y Comunicación, de conformidad con el documento adjunto.(...)" (...) ANÁLISIS JURÍDICO: Las políticas de seguridad informática son un conjunto de reglas, directrices y procedimientos establecidos en la ESPOCH, para proteger la información y los sistemas de tecnología de la información, contra amenazas y riesgos de seguridad, por lo que avocando conocimiento sobre el documento presentado por la Dirección de Tecnologías de la Información y Comunicación, en uso de sus atribuciones y competencias, en tal virtud desde esta Dirección Jurídica se procede a efectuar un análisis comparativo entre la normativa institucional vigente en contraste con la propuesta presentada expuesta a través del presente cuadro comparativo:

RESOLUCIÓN 785.CP.2024 POLITICAS DE SEGURIDAD INFORMATICA VIGENTES	REFORMA PROPUESTA A LAS POLITICAS DE SEGURIDAD INFORMATICA	OBSERVACION
Artículo 2.- Alcance. - Las presentes políticas serán aplicadas de manera obligatoria por los estudiantes, autoridades, personal académico, administrativo y trabajadores, y demás personal o terceros que intervengan en la ejecución de los procesos de la ESPOCH. La ESPOCH se reserva el derecho de cambiar los términos de esta política a futuro.	Artículo 2.-Alcance. - Las presentes políticas serán aplicadas de manera obligatoria por los estudiantes, autoridades, personal académico, administrativo y trabajadores, y demás personal o terceros que intervengan en la ejecución de los procesos de la ESPOCH. La ESPOCH se reserva el derecho de actualizar o complementar los términos establecidos en la presente política, conforme a sus necesidades institucionales y a la normativa vigente.	Se delimita la potestad institucional de modificación de las políticas internas, evitando interpretaciones discrecionales y otorgando mayor claridad a los sujetos obligados respecto de la aplicación futura de la normativa institucional.
Artículo 3.- Definiciones. - Para la aplicación de estas políticas se considerarán las siguientes definiciones: • Anti-RootKit: escanea procesos activos, módulos del sistema, memoria, objetos AutoRun y proporciona acceso al código de malware a otros componentes antivirus como un emulador, motor AV, heurística estática, heurística basada en el comportamiento potenciada por el modelo ML, etc.	Artículo 3.- Definiciones. - Para la aplicación de estas políticas se considerarán las siguientes definiciones:	En la propuesta de actualización se elimina el señalado texto.
	Inteligencia Artificial Generativa (IA): Sistemas computacionales (como ChatGPT, Gemini, Copilot, etc.) capaces de generar texto, imágenes, código u otro contenido en respuesta a comandos del	Se agrega



Riobamba-Ecuador
Panamericana Sur km 1 1/2
Código Postal: EC060155

Teléfono: 593 (03) 2998-200
Telefax: (03) 2 317-001

esPOCH.edu.ec



esPOCH

Secretaría
General

	usuario.	
	MFA (Autenticación Multifactor): Método de control de acceso que requiere que el usuario presente dos o más pruebas de identidad (algo que sabe, algo que tiene, algo que es).	Se agrega
• Políticas de uso de la plataforma de servicios de colaboración y productividad institucional basado en la nube: permite que las personas trabajen simultáneamente a través de varios servicios desde cualquier lugar que tenga conexión a internet. Abarca varios servicios en línea como: Correo electrónico, almacenamiento en la nube, Videoconferencias, Aplicaciones de ofimática (Editores de texto, hojas de cálculo, editor de presentaciones o diapositivas). Además, permite la integración con otros sistemas informáticos y servicios tecnológicos para diferentes propósitos. Ejemplo: Microsoft 365 antes denominado Office 365, Google Worksapce.	Políticas de uso de la plataforma de servicios de colaboración y productividad institucional basado en la nube: Garantizar un correcto uso de la plataforma de servicios de colaboración y productividad institucional basados en la nube (Resolución 417.CP.2024)	Únicamente se modifica la redacción
	Shadow IT / Shadow AI: Uso de software, aplicaciones, servicios en la nube o herramientas de inteligencia artificial por parte de los usuarios sin la aprobación explícita o el conocimiento de la DTIC.	Se agrega
• Sistema de mesa de ayuda: Garantizar un correcto uso del sistema de Mesa de Ayuda Institucional (soporte@esPOCH.edu.ec).	Sistema de mesa de ayuda: Garantizar un correcto uso del sistema de Mesa de Ayuda Institucional (soporte@esPOCH.edu.ec) Resolución 422.CP.2024	Se armoniza la redacción con la demás normativa institucional vigente
	Sistema de protección y respuesta de software malicioso: Solución de seguridad informática que protege los equipos contra virus, programas maliciosos y otros tipos de amenazas digitales. Funciona como un "antivirus avanzado", ya que no solo detecta y elimina malware, sino que también monitorea el comportamiento del sistema, identifica actividades sospechosas y ejecuta acciones automáticas de respuesta para evitar daños o propagación de una infección.	Se agrega
Artículo 4.- Clasificación. - Toda la información generada, procesada y almacenada en las plataformas y sistemas informáticos de uso institucional es de propiedad de la ESPOCH. Toda la información institucional en formato digital como por ejemplo documentos de carácter electrónico, bases de datos, correos electrónicos, medios de almacenamiento se clasifica en niveles según su sensibilidad y los riesgos asociados con la divulgación.	Artículo 4.- Directrices de uso. - La gestión de uso del Sistema de protección y respuesta, se regirá a través de los siguientes lineamientos: 1. La Dirección de Tecnologías de la Información y Comunicación, a través del área de Seguridad Informática, brindará un Sistema de protección y respuesta de software malicioso. 2. Todos los equipos de cómputo institucionales deben tener instalado y activo el Sistema de protección y respuesta de software	Se realiza cambios en los términos de la redacción, que guardan relación con la norma inicialmente señalada, no obstante, es de fundamental importancia informar que estos cambios responden al criterio profesional de la Dirección de Tecnologías de la Información y Comunicación



Riobamba-Ecuador
Panamericana Sur km 1½
Código Postal: EC060155

Teléfono: 593 (03) 2998-200
Telefax: (03) 2 317-001

esPOCH.edu.ec



El nivel de clasificación determina las protecciones de seguridad que deben utilizarse para la información. Es obligación para los docentes, administrativos y trabajadores firmar la carta compromiso de confidencialidad, no divulgación, reserva y resguardo de información digitalizada. Los niveles de clasificación son: • Confidencial: acceso restringido que requiere autorización del titular para su acceso. • Restringido: tienen acceso los directores departamentales y/o servidores politécnicos autorizados. • Público: todas las personas, dentro y fuera de la organización, tienen acceso. En función a la clasificación, la información de la institución debe estar adecuadamente protegida contra el acceso no autorizado, la pérdida y el daño. 1. Información de acceso confidencial. - Es aquella información o documentación, en cualquier formato, final o preparatoria, haya sido o no generada por el sujeto obligado, derivada de los derechos personalísimos y fundamentales, y requiere expresa autorización de su titular para su divulgación, que contiene datos que, al revelarse, pudiesen dañar los siguientes intereses privados: El uso ilegal que se haga de la información personal o su divulgación, dará lugar a las acciones legales pertinentes. La información considerada confidencial será: • Datos personales cuya difusión requiera el consentimiento de sus titulares y deberán ser tratados según lo dispuesto en la Ley Orgánica de Protección de Datos Personales; • Las patentes • Derechos de autor • Códigos de programación 2. Información de acceso restringido. - Es aquella a la que sólo ciertos miembros de la institución tienen acceso. La información considerada restringida será: • Información médica • Documentos internos relacionados con los estudiantes 3. Información de acceso público. - Todo tipo de dato en documentos de cualquier formato, final o preparatoria, haya sido o no generada por el sujeto obligado, que se encuentre en poder de los	malicioso, por lo tanto, la instalación, desinstalación y actualización de este software será responsabilidad del área de Soporte y Mantenimiento y de los técnicos afines al área informática de cada facultad y/o sede. Todo custodio o usuario responsable de un equipo de cómputo institucional deberá reportar de manera inmediata, a través del sistema de mesa de ayuda, cualquier anomalía relacionada con la ausencia, inactividad o desactualización del software antivirus institucional. 3. El área de Seguridad Informática en coordinación con los técnicos afines al área informática de las Facultades y Sedes en su rol de administradores del Sistema de protección y respuesta institucional serán los responsables de: a. Descargar y distribuir los programas de instalación. b. Instalar en todos los equipos de cómputo el Sistema de protección y respuesta de software malicioso. c. Actualizar programas, bases de datos, parches y demás aplicaciones requeridas por la herramienta antivirus para su óptimo desempeño. d. Realizar controles periódicos a los equipos, dirigidas a garantizar que los mismos se encuentran libres de códigos malignos, así como asegurar que los usuarios posean instalado el software antivirus autorizado por la Institución. e. Cuando así se estime conveniente, se debe proceder a la revisión de los equipos que se considere pueden estar comprometiendo la seguridad de la Institución. f. Uso responsable e inducción del manejo del Sistema de protección y respuesta de software malicioso. g. Protección de medios removibles. h. Respuesta y reporte de incidentes de seguridad. 4. En ninguna circunstancia los usuarios podrán desactivar o desinstalar el Sistema de protección y respuesta de software malicioso
--	--



sujetos obligados por la Ley Orgánica de Transparencia y Acceso a la Información Pública, contenidos, creados u obtenidos por ellos, que se encuentren bajo su responsabilidad y custodia o que se hayan producido con recursos del Estado. La información considerada de acceso público, será: • Resoluciones del Órgano Colegiado Superior. • Presupuesto anual que maneja la institución • Información financiera y contable • Información sobre la ejecución presupuestaria • Informes de rendición de cuentas • Normativas y Reglamentos internos • Informe anual sobre el cumplimiento del derecho de acceso a la información pública. • Distributivo de remuneraciones de administrativos, docentes y trabajadores. • Y demás información relacionada a la Ley Orgánica de Transparencia y Acceso a la Información Pública.	instalado en los equipos de la institución. De existir esta necesidad emergente se deberán realizar una solicitud a través del sistema de mesa ayuda con la justificación respectiva. 5. Todo equipo de cómputo que se conecte a la red de datos institucional deberá contar obligatoriamente con un Sistema de protección y respuesta de software malicioso, activo y con sus bases de datos de firmas y motores de detección debidamente actualizados. 6. Todo usuario responsable de un equipo de cómputo institucional deberá garantizar que los medios removibles y los archivos descargados desde Internet sean analizados mediante el Sistema de protección y respuesta de software malicioso, el cual deberá permanecer activo y actualizado en todo momento. 7. Cualquier sospecha de una posible presencia de software malicioso en equipos informáticos institucionales se deberá notificar de manera inmediata a través del sistema de mesa de ayuda institucional, a fin de que se activen los procedimientos técnicos de análisis, contención y remediación correspondientes.	
CAPITULO III Antivirus Artículo 5.- Directrices de uso. - La gestión de uso del antivirus, se regirá a través de los siguientes lineamientos: 1. La Dirección de Tecnologías de la Información y Comunicación (DTIC), a través del Área de Seguridad Informática, implementará una solución de antivirus institucional. 2. Todos los equipos de cómputo institucionales deben tener instalado y activo el antivirus, por lo tanto, la instalación, desinstalación y actualización de este software será responsabilidad del área de Soporte y Mantenimiento y de los técnicos afines al área informática de cada facultad y/o sede. Los servidores politécnicos tienen la obligación de reportar a través del sistema de mesa de ayuda si el equipo de cómputo que utilizan no dispone de un antivirus institucional. 3. El Área de Seguridad Informática en coordinación con los técnicos afines al área informática de las Facultades y Sedes en su rol de administradores del antivirus institucional serán los responsables de: a. Descargar y distribuir los programas de instalación.		Se elimina el capítulo completo, bajo el criterio técnico de la unidad requirente de la reforma de estas políticas.



esPOCH

Secretaría
General

b. Instalar en todos los equipos de cómputo el antivirus institucional c. Actualizar programas, bases de datos, parches y demás aplicaciones requeridas por la herramienta antivirus para su óptimo desempeño. d. Realizar controles periódicos a los equipos, dirigidas a garantizar que los mismos se encuentran libres de códigos malignos, así como asegurar que los usuarios posean instalado el software antivirus autorizado por la Institución. e. Cuando así se estime conveniente, se debe proceder a la revisión de los equipos que se considere pueden estar comprometiendo la seguridad de la Institución. f. Uso responsable e inducción del manejo del antivirus institucional. g. Protección de medios removibles. h. Respuesta y reporte de incidentes de seguridad. 4. En ninguna circunstancia los usuarios podrán desactivar o desinstalar el antivirus instalado en los equipos de la institución. De existir esta necesidad emergente deberán realizar una solicitud a través del sistema de mesa ayuda con la justificación respectiva. 5. Todos los equipos de cómputo ajenos a la institución que por alguna circunstancia se utilicen dentro de la ESPOCH deben tener instalado y activado un software de antivirus actualizado con licencia legal. 6. Los servidores politécnicos tienen la obligación de realizar escaneos permanentes a los medios removibles utilizados o archivos provenientes del internet. 7. Los servidores politécnicos que sospechen o detecten alguna infección por software malicioso en los equipos informáticos institucionales deben notificar a la mesa de ayuda o comunicarse directamente con el área de Soporte y Mantenimiento para recibir asistencia técnica.		
Artículo 6.- Recomendaciones para creación de contraseñas. - Las contraseñas o claves deben estar alineadas a los requisitos y recomendaciones que a continuación se indican: 1. No utilizar información personal en la contraseña: nombre del servidor o de sus familiares, ni sus apellidos, ni su fecha de nacimiento, ni cuentas bancarias, ni tarjetas de crédito, etc. 2. Utilizar al mínimo 8 caracteres. 3. Deben utilizar la combinación aleatoria de los siguientes tipos de caracteres: a. Minúsculas	Artículo 5.- Recomendaciones para creación de contraseñas. - Las contraseñas o claves de acceso deberán cumplir con los siguientes requisitos y buenas prácticas de seguridad: 1. Utilizar por lo menos 12 caracteres. 2. No utilizar información personal del usuario, tales como nombres, apellidos, fechas de nacimiento, números de identificación, datos bancarios, u otra información fácilmente asociable al titular de la cuenta. 3. Deben utilizar la combinación aleatoria de los siguientes tipos de	Se modifica la redacción y por tanto el contenido del presente artículo considerando que el mismo cuenta con un aporte técnico enfocado al tema de seguridad informática



Riobamba-Ecuador
Panamericana Sur km 1½
Código Postal: EC060155

Teléfono: 593 (03) 2998-200
Telefax: (03) 2 317-001

esPOCH.edu.ec



b. Mayúsculas c. Números d. Caracteres especiales como +*! @ # \$ & % ^ - / 4. Evitar utilizar secuencias básicas de teclado (por ejemplo: "qwerty", "asdf" o las típicas en numeración: "1234" ó "98765"). 5. No repetir los mismos caracteres en la misma contraseña. (ej.: "111222"). 6. No se debe utilizar como contraseña, ni contener, el nombre de usuario asociado a la misma. 7. No utilizar fechas. 8. No debe basarse en dos palabras separadas por un espacio (), guion (-) o guion bajo (_). 9. No se debe asignar contraseñas en blanco. No utilizar datos relacionados con el usuario que sean fácilmente deducibles, o derivados de estos. (ejemplo, no poner como apodos, el nombre del actor o de un personaje de ficción preferido, etc.). 10. No se deben utilizar palabras que se contengan en diccionarios en ningún idioma. 11. Cuando el sistema le solicite cambio de contraseña esta no debe haber sido utilizada en los históricos del sistema. 12. Elegir una contraseña que pueda recordarse fácilmente y es deseable que pueda escribirse rápidamente, preferiblemente, sin que sea necesario mirar el teclado.	caracteres: a. Letras minúsculas b. Letras mayúsculas c. Números d. Caracteres especiales como +*! @ # \$ & % ^ - / 4. Evitar patrones predecibles, no deberán emplearse secuencias comunes o patrones fácilmente deducibles tales como: a. Secuencias de teclado, por ejemplo: "qwerty", "asdf". b. Secuencias numéricas: "1234" ó "98765"). a. Repeticiones simples: (ej.: "111222") 5. La contraseña no deberá ser igual ni contener el nombre de usuario o identificador asociado a la cuenta. 6. No utilizar fechas. 7. No debe basarse en dos palabras separadas por un espacio (), guion (-) o guion bajo (_). 8. No se debe asignar contraseñas en blanco. No utilizar datos relacionados con el usuario que sean fácilmente deducibles, o derivados de estos. (ejemplo, no poner como apodos, el nombre del actor o de un personaje de ficción preferido, etc.). 9. No se deben utilizar palabras que se contengan en diccionarios en ningún idioma. 10. Cuando el sistema le solicite cambio de contraseña, la nueva clave no deberá coincidir con las utilizadas previamente. 11. Elegir una contraseña que pueda recordarse fácilmente y es deseable que pueda escribirse rápidamente, preferiblemente, sin que sea necesario mirar el teclado.	
Artículo 7.- Protección de contraseñas. - La protección de contraseñas o claves deben estar alineadas a los requisitos y recomendaciones que a continuación se indican: 1. Cuando un usuario inicie sesión por primera vez o cuando se realice una activación del usuario, el sistema exigirá cambio de contraseña. 2. Las contraseñas no deben compartirse con nadie. Las contraseñas deben tratarse como información sensible y confidencial de la institución. 3. Las contraseñas no deben incluirse en ningún tipo de comunicación electrónica. 4. No es recomendable incluir sugerencias para recordar contraseñas. No habilite tampoco la funcionalidad de 'pregunta secreta' y si es obligatorio, no incorpore	Artículo 6.- Protección de contraseñas. - La protección de contraseñas o claves deben estar alineadas a los requisitos y recomendaciones que a continuación se indican: 1. Cuando un usuario inicie sesión por primera vez o cuando se realice una activación del usuario, el sistema exigirá cambio de contraseña. 2. Es obligatorio el uso de Autenticación Multifactor (MFA) para el acceso a los sistemas institucionales y al correo institucional. El usuario es responsable de proteger el segundo factor en su dispositivo móvil. 3. Las contraseñas no deben compartirse con ninguna persona. Las contraseñas deben tratarse	Se verifica un cambio en la redacción técnica del contenido correspondiente a la protección de contraseñas conforme la propuesta emitida por la unidad proponente



información verídica relacionada con usted. 5. No escriba su contraseña y la almacene cerca de su lugar de trabajo habitual. Tampoco guarde sus contraseñas en un archivo en su equipo de cómputo del trabajo, teléfono móvil o tablet salvo que dicho archivo se almacene cifrado. 6. No escriba su contraseña si el acceso a la web del servicio no se realiza mediante protocolo web seguro ('https') 7. No emplee la opción "Recordar contraseña" que ofrecen los navegadores, especialmente cuando se trate de equipos de cómputo compartidos. 8. Ante cualquier sospecha de que su contraseña ha podido ser comprometida, informe de este particular a la DTIC a través del sistema de mesa de ayuda y cámbiela. 9. El control de las contraseñas y uso de equipos de red será responsabilidad del Área de Infraestructura de Tecnologías de la Información y Comunicación y la DTIC y dichas contraseñas son codificadas y almacenadas de forma segura. 10. Las contraseñas de super administrador de los sistemas informáticos, base de datos y demás servicios tecnológicos serán conservadas por la DTIC. Además, deben ser cambiadas en intervalos de al menos una vez al año y en todo caso cuando el personal adscrito al cargo cambie. 11. Las contraseñas de administrador de los servidores serán conservadas por la DTIC, Área de Desarrollo de Sistemas Informáticos y Área de Infraestructura de Tecnologías de la Información, son cambiadas en intervalos regulares de tiempo y en todo caso cuando el personal adscrito al cargo cambie.	como información sensible y confidencial de la institución. 4. Las contraseñas no deben incluirse, transmitirse ni solicitarse a través de correo electrónico, mensajería instantánea u otros medios electrónicos no seguros. 5. No es recomendable incluir pistas o sugerencias que faciliten la deducción de la contraseña. No habilite tampoco la funcionalidad de 'pregunta secreta' y si es obligatorio, no incorpore información verídica relacionada con el dueño de la cuenta. 6. No se debe escribir la contraseña en soporte físicos ni almacenarla cerca de su lugar de trabajo habitual. Tampoco guarde sus contraseñas en archivos digitales en su equipo de cómputo del trabajo, teléfono móvil o tablet salvo que dicho archivo se almacene cifrado. 7. No ingrese su contraseña si el acceso a la web no se realiza mediante un protocolo web seguro ('https') o si el navegador advierte sobre un certificado no confiable. 8. No se debe utilizar la opción "Recordar contraseña" que ofrecen los navegadores, especialmente cuando se trate de equipos de cómputo compartidos. 9. Ante cualquier sospecha de que su contraseña ha sido comprometida, se deberá cambiar la contraseña de inmediato.	
	Artículo 7.- Bloqueo de Sesión.- Todo usuario debe bloquear la sesión de su computador cada vez que se ausente de su puesto de trabajo, incluido por periodos breves de tiempo. Nota: Al finalizar la jornada laboral, no deberá dejarse documentación física que contenga información sensible o confidencial (por ejemplo: evaluaciones, informes financieros, datos personales, expedientes u otra información institucional) a la vista sobre el escritorio o en áreas de fácil acceso.	Se inserta esta disposición a efectos de cuidado individual de la información por parte de cada servidor institucional, al inicio del Capítulo III denominado "Control de Acceso"
Artículo 9.- Acceso, Protección y Ubicación de los activos tecnológicos. - 1. El custodio o responsable de un activo tecnológico será el único responsable de su correcto uso, así como también de la información contenida en los mismos, por lo que debe evitar compartirlos. En caso de requerir compartirlo o prestar el activo	Artículo 9.- Acceso, protección y ubicación de los activos tecnológicos. - 1. El custodio o responsable de un activo tecnológico será el único responsable de su correcto uso, así como también de la información contenida en los mismos, por lo que debe evitar compartirlos. En	Se elimina el número 4 del presente artículo, además en el numeral 6 letra i) se modifica el texto al final y se señala: "Esto incluye programas o archivos que traten de interceptar, monitorear o descubrir información de otros usuarios en la red."



tecnológico, será solamente para actividades laborales y sin liberarlo de su responsabilidad. Mientras se opera un activo tecnológico no se deberá ingerir líquidos y consumir alimentos. 2. No se puede mover o reubicar, ni retirar sellos de seguridad de un activo tecnológico sin la intervención y acompañamiento de la DTIC y/o técnicos afines al área informática de las facultades y sedes. 3. Es responsabilidad del usuario almacenar la información institucional únicamente en la carpeta "Documentos" del computador de escritorio o portátil asignado. 4. Un activo tecnológico se debe mantener en un entorno limpio y sin humedad. 5. Cuando exista la necesidad de reemplazo o reubicación de activos tecnológicos debe notificarse a través del sistema de mesa de ayuda. 6. Nadie puede ver, copiar, alterar o destruir la información sin el consentimiento explícito del responsable. 7. En ningún caso se podrá acceder a los activos tecnológicos con las finalidades siguientes: • Incurrir en actividades ilícitas o ilegales de cualquier tipo y, particularmente difundir contenidos o propaganda de carácter racista, xenófobo, pornográfico, sexista, de apología del terrorismo o atentatorio contra los derechos humanos, o actuar en perjuicio de los derechos a la intimidad, al honor, a la propia imagen o contra la dignidad de las personas. • Difundir contenidos contrarios a los principios enunciados en el estatuto institucional. • Dañar los sistemas físicos y lógicos de la ESPOCH, de sus proveedores o de terceras personas. • Introducir o difundir en la red virus informáticos o cualesquiera otros sistemas físicos o lógicos que sean susceptibles de provocar los daños anteriormente citados. • Usar cuentas de usuario sin autorización. Obtener la contraseña de acceso de una cuenta de usuario sin la autorización del propietario. Comunicar a otros la contraseña para que puedan entrar en la cuenta. • Usar la red o computadores de la ESPOCH para conseguir el acceso no autorizado a cualquier computador. • Realizar con conocimiento de causa cualquier acto que interfiera en el correcto funcionamiento de los computadores, terminales, periféricos, red de comunicaciones, etc.	caso de requerir compartirlo o prestar el activo tecnológico, será solamente para actividades laborales y sin liberarlo de su responsabilidad. Mientras se opera un activo tecnológico no se deberá ingerir líquidos y consumir alimentos. 2. No se puede mover o reubicar, ni retirar sellos de seguridad de un activo tecnológico sin la intervención y acompañamiento de la DTIC y/o técnicos afines al área informática de las facultades y sedes. 3. Es responsabilidad del usuario almacenar la información institucional únicamente en la carpeta "Documentos" del computador de escritorio o portátil asignado. 4. Cuando exista la necesidad de reemplazo o reubicación de activos tecnológicos debe notificarse a través del sistema de mesa de ayuda. 5. Nadie puede ver, copiar, alterar o destruir la información sin el consentimiento explícito del responsable. 6. En ningún caso se podrá acceder a los activos tecnológicos con las finalidades siguientes: a) Incurrir en actividades ilícitas o ilegales de cualquier tipo y, particularmente difundir contenidos o propaganda de carácter racista, xenófobo, pornográfico, sexista, de apología del terrorismo o atentatorio contra los derechos humanos, o actuar en perjuicio de los derechos a la intimidad, al honor, a la propia imagen o contra la dignidad de las personas. b) Difundir contenidos contrarios a los principios enunciados en el estatuto institucional. c) Dañar los sistemas físicos y lógicos de la ESPOCH, de sus proveedores o de terceras personas. d) Introducir o difundir en la red virus informáticos o cualesquiera otros sistemas físicos o lógicos que sean susceptibles de provocar los daños anteriormente citados. e) Usar cuentas de usuario sin autorización. Obtener la contraseña de acceso de una cuenta de usuario sin la autorización del propietario. Comunicar a otros la contraseña para que puedan entrar en la cuenta. f) Usar la red o computadores de la ESPOCH para conseguir el acceso no autorizado a cualquier computador. g) Realizar con conocimiento de causa cualquier acto que interfiera en el	
---	---	--



• Instalar o ejecutar en cualquier punto de la red informática programas o archivos que deterioren o incrementen en exceso la carga en cualquier punto de la misma, hasta el límite de llegar a perjudicar a otros usuarios o al rendimiento de la propia red. Esto incluye cualquier tipo de ensayo, experimento o actividad que incluso pudiendo ser considerada legítima perjudique el buen funcionamiento de la red. • Instalar o ejecutar en cualquier punto de la red informática programas o archivos que traten de descubrir información distinta de la del propio usuario, en cualquier elemento de la red. Esto incluye los Sniffer, scanner de puerto, etc. • Intentar sobrepasar protecciones de datos o sistemas de seguridad informática. • Violar la privacidad de los datos y el trabajo de los otros usuarios. 8. La DTIC gestionará la restricción de acceso a sitios web que no estén acordes a las actividades de academia, investigación, vinculación con la colectividad y gestión administrativa en función a las necesidades institucionales. Sin embargo, si por la naturaleza del cargo se requiere el acceso a páginas de acceso controlado, se debe solicitar mediante al sistema de mesa de ayuda por parte el responsable de la unidad requirente. 9. Se prohíbe descargar archivos como: imágenes, sonidos, música, videos, etc. o instalar programas de sitios web desconocidos o gratuitos.	correcto funcionamiento de los computadores, terminales, periféricos, red de comunicaciones, etc. h) Instalar o ejecutar en cualquier punto de la red informática programas o archivos que deterioren o incrementen en exceso la carga en cualquier punto de la misma, hasta el límite de llegar a perjudicar a otros usuarios o al rendimiento de la propia red. Esto incluye cualquier tipo de ensayo, experimento o actividad que incluso pudiendo ser considerada legítima perjudique el buen funcionamiento de la red. i) Instalar o ejecutar en cualquier punto de la red informática programas o archivos que traten de descubrir información distinta de la del propio usuario, en cualquier elemento de la red. Esto incluye programas o archivos que traten de interceptar, monitorear o descubrir información de otros usuarios en la red. j) Intentar sobrepasar protecciones de datos o sistemas de seguridad informática. k) Violar la privacidad de los datos y el trabajo de los otros usuarios. 7. La DTIC gestionará la restricción de acceso a sitios web que no estén acordes a las actividades de academia, investigación, vinculación con la colectividad y gestión administrativa en función a las necesidades institucionales. Sin embargo, si por la naturaleza del cargo se requiere el acceso a páginas de acceso controlado, se debe solicitar mediante al sistema de mesa de ayuda por parte el responsable de la unidad requirente. 8. Se prohíbe descargar archivos como: imágenes, sonidos, música, videos, etc. o instalar programas de sitios web desconocidos o gratuitos.	
Artículo 13.- Red de datos. - 1. Está prohibido el uso de IPs no proporcionadas por la DTIC o el intercambio de ellas, en activos que no estén configurados. 2. La ESPOCH, a través de la DTIC, gestionará los rangos de direcciones IP a nivel institucional en base a criterios técnicos, de ahorro y eficiencia. 3. No es permitida la conexión de equipos activos de red no institucionales, salvo análisis del Área de Infraestructura de Tecnologías de la Información y Comunicación y autorización de la DTIC. 4. La DTIC es la única dependencia autorizada para el uso de analizadores de	Artículo 13.- Red de datos. - 1. No se permitirá conectar equipos activos personales (routers, repetidores, switches) a la red cableada institucional sin autorización, dicha acción podría comprometer la configuración, disponibilidad, integridad y seguridad de la infraestructura tecnológica institucional. 2. La ESPOCH, a través de la DTIC, gestionará los rangos de direcciones IP a nivel institucional en base a criterios técnicos, de ahorro y eficiencia.	Se modifica el contenido técnico, en virtud de que eran 5 numerales en las políticas vigentes mientras que se cambió a únicamente 3 fuentes importantes referentes la red de datos.



red, snnifers y demás herramientas de gestión de redes de datos. En caso de detectar el uso de estas herramientas por usuarios no autorizados, se desconectará temporal o permanentemente los servicios de red al equipo donde se ejecutaron estas herramientas. La reconexión se realizará en cuanto se considere que el uso no aceptable se ha suspendido. 5. La DTIC mantendrá instalados, habilitados y controlados sólo aquellos servicios de sistema operativo y puertos que sean utilizados en la institución.	3. La DTIC mantendrá instalados, habilitados y controlados sólo aquellos servicios de sistema operativo y puertos que sean estrictamente necesarios para la operación institucional.	
Artículo 22.- Equipo y sistema operativo. - Cualquier equipo que vaya a conectarse al entorno institucional, debe cumplir con los siguientes puntos: • Instalación del sistema operativo desde una fuente fiable. • Sistema operativo y aplicaciones actualizadas. • Software antivirus. • Cuentas de usuario sin permisos para instalar software. • Control de acceso robusto. • Configuraciones seguras en aplicaciones (navegación web, correo electrónico, etc.). • Bloqueo automático por inactividad. • Software Anti-RootKit y así evitar que un hacker tenga la capacidad de introducirse en un dispositivo y hacerse con el control del mismo. • Control de software original. • Cifrado del disco.	Artículo 22.- Equipo y sistema operativo. Todo equipo que vaya a conectarse al entorno institucional, deberá cumplir con los siguientes puntos mínimos de seguridad: 1. Instalación del sistema operativo desde una fuente fiable. 2. Sistema operativo y aplicaciones actualizadas. 3. Software antivirus. 4. Cuentas de usuario sin permisos para instalar software. 5. Control de acceso robusto. 6. Configuraciones seguras en aplicaciones (navegación web, correo electrónico, etc.). 7. Bloqueo automático por inactividad. 8. Control de software original. 9. Cifrado del disco.	En la redacción propuesta se agrega que serán puntos mínimos de seguridad, y se elimina el punto: "Software Anti-RootKit y así evitar que un hacker tenga la capacidad de introducirse en un dispositivo y hacerse con el control del mismo."
Artículo 23.- Equipos no confiables. - Los servidores politécnicos que utilicen equipos informáticos propios deben contemplar utilizar diferentes cuentas de usuarios en el computador o utilizar distribuciones "live", como se detallan en los siguientes puntos: • Diferentes cuentas de usuario: los equipos de cómputo personales deben de tener diferentes cuentas de usuario. Con el objetivo de diferenciar una para entornos confiables (teletrabajo) y otra para asuntos personales. • Distribuciones "live": Si no se configura cuentas de usuario diferentes se debe de utilizar un inicio del sistema operativo independiente utilizando distribuciones live.	Artículo 23.- Equipos no confiables. El politécnico que utilice equipos informáticos propios debe contemplar utilizar diferentes cuentas de usuarios en el computador o utilizar distribuciones "live", como se detallan en los siguientes puntos: • Diferentes cuentas de usuario: los equipos de cómputo personales deben de tener diferentes cuentas de usuario. Con el objetivo de diferenciar una para entornos confiables (teletrabajo) y otra para asuntos personales.	La unidad requirente modifica en la propuesta de reforma la redacción técnica y elimina el punto: "Distribuciones "live": Si no se configura cuentas de usuario diferentes se debe de utilizar un inicio del sistema operativo independiente utilizando distribuciones live."
Artículo 25.- Protección física de los equipos. - Si el servidor politécnico tiene la autorización para trasladar el equipo informático a su domicilio, tiene que cumplir con los siguientes puntos: • No dejar al equipo en el vehículo (aunque no esté a la vista) • No dejarlo desatendido • Evitar sacarlo de casa si no es necesario	Artículo 25.- Protección física de los equipos. Cuando se cuente con autorización para trasladar el equipo informático a su domicilio, se deberá cumplir con las siguientes medidas de protección: 1. No dejar al equipo en el vehículo (aunque no esté a la vista)	En cuanto a la protección física de los equipos se determinan cambios en la redacción de los medios físicos para cuidado de los equipos



• Adquirir candados de seguridad para portátiles. • Adquirir un armario de seguridad donde almacenar el equipo y otros artículos de relativo valor.	2. No dejar el equipo desatendido en lugares públicos o de fácil acceso a terceros. 3. Evitar trasladarlo fuera del domicilio autorizado, salvo que sea estrictamente necesario y por motivos laborales debidamente justificados. 4. Implementar mecanismos físicos de seguridad para equipos portátiles, tales como candados de seguridad u otros dispositivos antirrobo. 5. Disponer de un espacio seguro para su almacenamiento en el domicilio, preferentemente en un armario o gabinete con cerradura u otro mecanismo de resguardo que limite el acceso no autorizado.	
Artículo 28.- Ingeniería social. - Se debe tener en cuenta las indicaciones realizadas en las diferentes charlas de concienciación que la Dirección de Tecnologías de la Información y Comunicación a través del área de Seguridad Informática imparte para no ser víctima de correos electrónicos o llamadas telefónicas suplantando a algún servidor politécnico, proveedor o externo solicitando cualquier tipo de información.	Artículo 28.- Ingeniería social. Se debe tener en cuenta las indicaciones realizadas en las diferentes charlas de concienciación que la Dirección de Tecnología de la Información y Comunicación a través su área de Seguridad Informática imparte para no ser víctima de correos electrónicos, mensajes de WhatsApp o llamadas (incluso aquellas que parezcan provenir de autoridades usando voz generada por IA) que soliciten transferencias de dinero, cambios de contraseña urgentes o instalación de software desconocido. La DTIC nunca solicitará su contraseña por estos medios.	Se incorpora nuevas modalidades de riesgo asociadas a la ingeniería social y a las tecnologías emergentes utilizadas para cometer fraudes informáticos, además mejora la precisión del contenido preventivo, al establecer ejemplos concretos de conductas fraudulentas
Artículo 29.- Puesto de trabajo. - El servidor politécnico debe tener en cuenta que, al utilizar el equipo de casa para trabajar, equipo que tienen acceso otros miembros de la familia, o donde se utiliza un equipo que no es del propio usuario, se debe realizar lo siguiente: • Cerrar todas las conexiones con servidores y páginas web utilizando cuando sea posible la opción "desconectar" o "cerrar sesión". • Eliminar información temporal prestando especial atención a la carpeta de descargas, papelera de reciclaje, o posibles carpetas perdidas que se dejen en "Documentos". • Utilizar herramientas de borrado seguro para eliminar los ficheros en caso de información sensible o especialmente confidencial. • Si se han utilizado certificados digitales (firmas electrónicas), estos deben ser borrados de forma segura. • Asegurarse de retirar cualquier medio removible que se haya utilizado en el equipo.	Artículo 29.- Puesto de trabajo. Se deberá considerar que, al utilizar equipos domiciliarios para el desarrollo de actividades laborales (especialmente cuando dichos equipos puedan ser utilizados por otros miembros del hogar o cuando no sean de uso exclusivo del usuario autorizado) se incrementa el riesgo de exposición de la información institucional. En estos casos, el servidor politécnico deberá observar las siguientes medidas de seguridad: 1. Cerrar correctamente todas las conexiones activas con servidores, sistemas y páginas web institucionales, utilizando las opciones formales de "desconectar" o "cerrar sesión". 2. Eliminar la información temporal generada durante la sesión de trabajo, prestando especial atención a la carpeta de descargas, la papelera de reciclaje y cualquier archivo almacenado en directorios locales del equipo. 3. Aplicar mecanismos de borrado	La revisión de la redacción, en su estructura normativa como en el alcance de las medidas de seguridad informática que se incorporan. en la redacción se organiza las medidas de seguridad mediante numerales claramente definidos, facilitando su comprensión, aplicación y control institucional.



esPOCH

**Secretaría
General**

• Borrar el histórico de navegación, así como las cookies, y otros datos del navegador web, prestando especial atención a las contraseñas recordadas.	seguro cuando se trate de información sensible o confidencial, a fin de evitar su recuperación posterior. 4. Eliminar de manera segura los certificados digitales o firmas electrónicas que hayan sido utilizados en el equipo. 5. Retirar cualquier medio removible empleado durante la jornada laboral, tales como memorias USB u otros dispositivos de almacenamiento externo. 6. Suprimir el historial de navegación, las cookies y otros datos almacenados por el navegador web, verificando especialmente que no queden credenciales o contraseñas guardadas en el equipo. En ninguna circunstancia se permitirá el acceso a sistemas o información institucional desde equipos públicos o compartidos, tales como los ubicados en cibercafés, hoteles, aeropuertos u otros espacios similares.	
CAPITULO IX Consecuencias de la aplicación inadecuada de las políticas de seguridad informática CAPITULO X Responsabilidades de aplicación de las políticas	CAPITULO VII Responsabilidades, consecuencias de la aplicación inadecuada de las políticas de seguridad informática	Se realiza una actualización de secuencia en el documento, para armonizar el mismo
Artículo 30.- Inobservancia. – La omisión e inobservancia de las políticas establecidas en este documento podrá conducir a la aplicación de las sanciones que correspondan al infractor según su vínculo con la Institución, observando su régimen laboral y deben ponerse en conocimiento del jefe inmediato y de la DTIC a través del sistema de mesa de ayuda de manera inmediata. Cualquier sospecha de violaciones de la seguridad debe ser reportado también a través del sistema de mesa de ayuda.	Artículo 34.- Inobservancia. – La omisión e inobservancia de las políticas establecidas en este documento podrá conducir a la aplicación de las sanciones que correspondan al infractor según su vínculo con la Institución, observando su régimen laboral y deben ponerse en conocimiento del jefe inmediato y de la DTIC a través del sistema de mesa de ayuda de manera inmediata. Cualquier sospecha de violaciones de la seguridad debe ser reportado también a través del sistema de mesa de ayuda.	Se ha movido la ubicación de orden de este artículo en el documento.

La Dirección de Tecnologías de la Información y Comunicación, como unidad administrativa competente para brindar el apoyo y asesoramiento continuo a las autoridades ejecutivas y comunidad politécnica, a través de soluciones de tecnologías de la información y comunicación, facilitando, potencializando y maximizando las actividades relacionadas a los ejes sustantivos institucionales, ha elaborado una propuesta de actualización a las "POLÍTICAS DE SEGURIDAD INFORMÁTICA", en tal virtud bajo sus atribuciones establecidas en la legislación interna de la ESPOCH, así como bajo su competencia profesional que incluye el conocimiento y habilidades necesarias para ayudar a asegurar una actuación ordenada, ética, eficaz y eficiente, al igual que un buen entendimiento de las responsabilidades individuales relacionadas con el control interno para el manejo y la protección de la información y los sistemas de tecnología de la información que maneja la ESPOCH. Bajo el análisis expuesto, es importante informar a su autoridad que estas políticas observan a nivel institucional el cumplimiento obligatorio de lo estipulado en la Ley Orgánica de Protección de Datos Personales, ajustada a lo dispuesto por el Art. 92 de la Constitución de la República del Ecuador, por lo que la actualización constituye una mejora en términos de técnica normativa y seguridad jurídica respecto de la redacción original, guardando el alcance subjetivo de aplicación obligatoria de las políticas institucionales para estudiantes, autoridades, personal académico, administrativo, trabajadores y terceros vinculados



Riobamba-Ecuador
Panamericana Sur km 1½
Código Postal: EC060155

Teléfono: 593 (03) 2998-200
Telefax: (03) 2 317-001

esPOCH.edu.ec



esPOCH

Secretaría
General

a los procesos de la ESPOCH, por lo que toda modificación se centra principalmente en una actualización normativa. En lo referente al contenido de la Resolución 785.CP.2024, por medio de la cual el Consejo Politécnico, aprobó las "Políticas de Seguridad informática" de la Escuela Superior Politécnica de Chimborazo", se verifica que la actualización implica una importante modificación técnica al contenido inicialmente aprobado, por lo que al ser una actualización en un porcentaje mayor al 50% de su contenido, desde esta Dirección Jurídica se sugiere derogar la referida resolución, para lo cual se ha incluido una disposición derogatoria en el documento adjunto al presente trámite. Es importante informar que la propuesta de actualización observa el contenido de la Constitución de la República del Ecuador, la Ley Orgánica de Protección de Datos Personales, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, la Ley del Sistema Nacional de Registro de Datos Públicos, el Código Orgánico Integral Penal, el Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, la Guía para Tratamiento de Datos Personales en Administración Pública y demás decretos reglamentarios referentes al tema, por lo que las mismas acogen el criterio y la competencia profesional de la Dirección de Tecnologías de la Información y Comunicación como dependencia proponente de la modificación a la normativa institucional técnica interna. Para concluir señor Director Jurídico y por todas las consideraciones expuestas, me permito informar que la propuesta adjunta es procedente, en tal virtud, sugiero que la Dirección de Tecnologías de la Información y Comunicación siguiendo el respectivo órgano regular realice la gestión para la aprobación ante Consejo Politécnico, por lo que el presente criterio jurídico es favorable y habilita su trámite de aprobación conforme lo dispuesto por el inciso segundo del Artículo 23 del Reglamento de Funcionamiento de Consejo Politécnico."

Que, se conoció el Oficio Nro. ESPOCH-DJ-2026-0625-O, suscrito por el Abg. Daniel Antonio Núñez Bucay, Mg., DIRECTOR JURÍDICO, quien indica: "En atención a su Oficio No. 0792-DTIC-ESPOCH-2026, donde solicita (...) la elaboración del informe legal, con el fin de sustentar la aprobación de la actualización de las Políticas de Seguridad Informática ante el Consejo Politécnico (...). Al respecto anexo criterio jurídico inserto en el Oficio No. DJ-ESPOCH-MLPC-032-2026, elaborado por Marcela Parra, Abogada de la institución, informe que lo he revisado, analizado y tiene mi Aval en calidad de Director Jurídico Institucional."

Que, se conoció el Oficio Nro. 1149-DTIC-ESPOCH-2026, suscrito por el Ing. Diego Bernardo Palacios Campana, DIRECTOR TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN, quien indica: "En atención al documento Nro. ESPOCH-DJ-2026-0625-O, suscrito electrónicamente por el abogado Daniel Núñez, Director Jurídico Institucional, mediante el cual manifiesta lo siguiente: "...En atención a su Oficio No. 0792-DTIC-ESPOCH-2026, donde solicita la elaboración del informe legal con el fin de sustentar la aprobación de la actualización de las Políticas de Seguridad Informática ante el Consejo Politécnico. Al respecto, adjunto el criterio jurídico contenido en el Oficio No. DJ-ESPOCH-MLPC-032-2026, elaborado por la abogada Marcela Parra, informe que ha sido revisado, analizado y cuenta con mi aval en calidad de Director Jurídico Institucional...". En virtud de lo expuesto y considerando que se cuenta con un informe jurídico favorable para la actualización de las Políticas de Seguridad Informática, me permito solicitar comedidamente a usted se sirva gestionar ante el Consejo Politécnico la aprobación de dichas políticas, a fin de viabilizar su aplicación e implementación a nivel institucional. Agradezco de antemano la atención brindada a la presente solicitud y quedo atento a cualquier información adicional que se requiera."

Que, se conoció el Oficio Nro. 3706.R.ESPOCH.SGD.2026, suscrito por el Ing. Byron Ernesto Vaca Barahona, PhD., RECTOR, quien indica: "Me permito remitir el Oficio Nro. 1149-DTIC-ESPOCH-2026, firmado electrónicamente por el Ing. Diego Palacios Campana; Director Tecnologías de la Información y Comunicación, quien solicita se ponga a consideración de los señores miembros de Consejo Politécnico, para análisis y aprobación la actualización de las Políticas de Seguridad Informática."

Con base en las disposiciones jurídicas invocadas y a las consideraciones expuestas, este Organismo, por unanimidad,



Riobamba-Ecuador
Panamericana Sur km 1½
Código Postal: EC060155

Teléfono: 593 (03) 2998-200
Telefax: (03) 2 317-001

esPOCH.edu.ec



espoch

Secretaría
General

RESUELVE:

Artículo 1.- Derogar la Resolución 785.CP.2024.

Artículo 2.- Aprobar las Políticas de Seguridad Informática, de acuerdo al pedido remitido mediante oficio Nro. 1149-DTIC-ESPOCH-2026, suscrito por el Ing. Diego Bernardo Palacios Campana, Director Tecnologías de la Información y Comunicación, de conformidad con el documento adjunto.

Artículo 3.- Disponer a las unidades académicas y administrativas, la realización de las acciones dentro de ámbito de competencia que se deriven de la aprobación de la presente resolución

.....
Abg. Carlos Iván de la Cadena Reinoso Mgs.,

SECRETARIO GENERAL DE LA ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO.

CERTIFICA:

Que, la Resolución que antecede fue adoptada por el Consejo Politécnico en sesión ordinaria realizada el día martes 23 de junio del año 2026.



Validar únicamente en FirmaEC.
Firmado electrónicamente por:
**CARLOS IVAN DE LA
CADENA REINOSO**

Abg. Carlos Iván de la Cadena Reinoso Mgs.

SECRETARIO GENERAL

Copia: Rectorado, Vicerrectorado Académico, Vicerrectorado de Investigación y Posgrado, Vicerrectorado Administrativo, Dirección de Planificación, Dirección Financiera, Dirección Administrativa, Dirección Tecnologías de la Información y Comunicación, Dirección de Talento Humano, Archivo.



Riobamba-Ecuador
Panamericana Sur km 1½
Código Postal: EC060155

Teléfono: 593 (03) 2998-200
Telefax: (03) 2 317-001

espoch.edu.ec