



“Políticas de Seguridad Informática”

2026



Tabla de contenido

TITULO I	4
PRINCIPIOS GENERALES	4
CAPITULO I	4
DEL OBJETO, ALCANCE Y DEFINICIONES	4
Artículo 1. Objeto. –	4
Artículo 2. Alcance. –	4
Artículo 3. Definiciones. –	4
TITULO II	7
Políticas generales de seguridad informática	7
CAPITULO I	7
Sistema de protección y respuesta de software malicioso	7
Artículo 4. Directrices de uso. –	7
CAPITULO II	8
Contraseñas	8
Artículo 5. Recomendaciones para creación de contraseñas. –	8
Artículo 6. Protección de contraseñas. –	9
CAPITULO III	9
Control de Acceso	9
Artículo 7. Bloqueo de Sesión.	9
Artículo 8. Identificación, clasificación y valoración de activos. –	10
Artículo 9. Acceso, protección y ubicación de los activos tecnológicos. -	10
Artículo 10. Acceso a los servicios tecnológicos. -	11
Artículo 11. Gestión de privilegios. -	11
Artículo 12. Software. -	11
Artículo 13. Red de datos. -	12
Artículo 14. Conexiones remotas. -	12
Artículo 15. Acceso a la Red Inalámbrica. -	12
Artículo 16. Monitoreo de los Accesos. -	12
Artículo 17. Sesiones Inactivas. –	13
Artículo 18. Accesos al Sistema Operativo. -	13
Artículo 19. Centro de Datos. -	13
CAPITULO IV	14



Medios Removibles	14
Artículo 20. Directrices de uso. –.....	14
CAPITULO V.	14
RESPALDOS	14
Artículo 21. Gestión de respaldos. –.....	14
CAPITULO VI.....	15
TELETRABAJO	15
Artículo 22. Equipo y sistema operativo.....	15
Artículo 23. Equipos no confiables.	15
Artículo 24. Tablets y smartphones.....	15
Artículo 25. Protección física de los equipos.....	16
Artículo 26. Borrado remoto. –.....	16
Artículo 27. Sistemas de almacenamiento online.	16
Artículo 28. Ingeniería social.....	16
Artículo 29. Puesto de trabajo.....	16
CAPITULO VII.....	17
Responsabilidades, consecuencias de la aplicación inadecuada de las políticas de seguridad informática	17
Artículo 30. Responsabilidades de la DTIC.	17
Artículo 31. Responsabilidades de la Dirección de Talento Humano. –.....	17
Artículo 32. Responsabilidades de los estudiantes.....	17
Artículo 33. Responsabilidad de terceros. –.....	18
Artículo 34. Inobservancia. –.....	18



CONSIDERANDO

Que, los numerales 1 y 2 del artículo 16 de la Constitución de la República del Ecuador, señala: "Todas las personas, en forma individual o colectiva, tienen derecho a: 1. Una comunicación libre, intercultural, incluyente, diversa y participativa, en todos los ámbitos de la interacción social, por cualquier medio y forma, en su propia lengua y con sus propios símbolos; 2. El acceso universal a las tecnologías de información y comunicación";

Que, el artículo 350 de la Constitución de la República del Ecuador señala: "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, la norma 410 sobre Tecnología de la Información, numeral 410-01, de las Normas de Control Interno de la Contraloría General del Estado, señala: "Las entidades y organismos del sector público deben estar acopladas en un marco de trabajo para procesos de tecnología de información que aseguren la transparencia y el control, así como el involucramiento de la alta dirección, por lo que las actividades y procesos de tecnología de información de la organización deben estar bajo la responsabilidad de una unidad que se encargue de regular y estandarizar los temas tecnológicos a nivel institucional. La Unidad de Tecnología de Información, estará posicionada dentro de la estructura organizacional de la entidad en un nivel que le permita efectuar las actividades de asesoría y apoyo a la alta dirección y unidades usuarias; así como participar en la toma de decisiones de la organización y generar cambios de mejora tecnológica. Además, debe garantizar su independencia respecto de las áreas usuarias y asegurar la cobertura de servicios a todas las unidades de la entidad u organismo. (...)";

Que, el artículo 2 de la Ley de Comercio Electrónico señala: "Los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos se someterá al cumplimiento de lo establecido en esta ley y su reglamento.".

Que, es necesario contar con un instrumento que regule la seguridad informática institucional;



TITULO I

PRINCIPIOS GENERALES

CAPITULO I

DEL OBJETO, ALCANCE Y DEFINICIONES

Artículo 1. Objeto. –

Establecer las políticas a cumplirse por todos los usuarios de la comunidad politécnica y terceros que intervengan en la ejecución de los procesos de la institución, con la finalidad de proporcionar un marco de seguridad que garantice la protección, confiabilidad, integridad, y disponibilidad de la información digital de la Escuela Superior Politécnica de Chimborazo frente a la pérdida, daño o el acceso no autorizado.

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.

Artículo 3. Definiciones. –

Para la correcta aplicación e interpretación de la presente política, se adoptarán las siguientes definiciones:

Activo: cualquier componente (tecnológico, electrónico, software, hardware, o de infraestructura) que forme parte dentro de los bienes de la institución, se puede clasificar en:

- **Activos de información:** Corresponde a elementos en formato digital tales como bases de datos, documentación, manuales de usuarios, planes de continuidad, etc.
- **Activos de software:** Son elementos tales como: Licencias de software, Sistemas operativos, Aplicaciones y programas informáticos, herramientas de desarrollo, y utilidades adicionales suministradas por la ESPOCH.
- **Activos físicos:** Se consideran activos físicos elementos tales como: Computadores de escritorio y portátiles, Equipos activos de red, impresoras, equipos de Comunicaciones, medios removibles, UPS, Servidores, Escáner, Teléfonos IP, Cámaras IP, Controles biométricos, Dispositivos móviles, entre otros.

Autenticación: es el procedimiento de comprobación que permite verificar si un usuario de un sitio web o un servicio es quien dice ser.

Confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas



autorizadas a tener acceso a la misma.

Derechos de autor: es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley conoce a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

colaboración y productividad institucional basados en la nube (Resolución 417.CP.2024)

Confiability de la Información: integridad y precisión de los datos como una medida de qué tanto puede contarse con que son constantes y no presentan errores en los distintos tiempos y fuentes

Información digital: Cualquier tipo de información contenida en un medio digital, bien sea en forma de base de datos, en forma de archivos digitales o de intercambio.

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 usuario.

Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

Infraestructura Tecnológica: Es el conjunto de hardware y software, que se implementa conformando una plataforma tecnológica para el funcionamiento de las actividades de una organización u empresa.

Medios removibles: Se define como medio removible para todo dispositivo de almacenamiento de información que sea extraíble de su gestor de información, entiéndase entonces que medios removibles son: Unidades USB, Discos Duros portables, Tarjetas SD, CD, DVD, Blu-ray, e incluso unidad de almacenamiento de Smartphone o Tablet, o todo lo que permita transportar información.

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).

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

Servicio tecnológico: Conjunto de servicios que la institución pone a disposición de los usuarios, siendo los más conocidos el acceso a internet, acceso a páginas web, el correo electrónico, la transferencia de archivos, los chats, videoconferencia, conversaciones, entre otros.

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.

Sistema de mesa de ayuda: Garantizar un correcto uso del sistema de Mesa de Ayuda Institucional (soporte@epoch.edu.ec) Resolución 422.CP.2024

Sistema de autenticación centralizada: La institución cuenta con un sistema único de inicio de sesión. Consistiría que con un único usuario y contraseña se ingresa a los diferentes servicios institucionales.

Sistema informático: Entendemos por sistema informático el conjunto de elementos físicos y lógicos que se encargan de recibir, guardar y procesar datos para luego entregarlos en forma de resultados.

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.

Terceros: o usuarios externos, se considera a los ciudadanos, personas naturales o jurídicas, nacionales o extranjeras que intervengan en la ejecución de los procesos de la institución.

**TITULO II****Políticas generales de seguridad informática****CAPITULO I****Sistema de protección y respuesta de software malicioso****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 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 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 II

Contraseñas

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 caracteres:
 - a. Letras minúsculas
 - b. Letras mayúsculas
 - c. Números
 - d. Caracteres especiales como +*! @ # \$ & % ^ -/
4. Evitar patrones predecibles, no deberán emplearse utilizar secuencias comunes o patrones fácilmente deducibles tales como:
 - a. Secuencias de teclado, por ejemplo: "qwerty", "asdf".
 - b. Secuencias numéricas: "1234" ó "98765".
 - c. 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 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 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.

CAPITULO III

Control de Acceso

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.

Artículo 8. Identificación, clasificación y valoración de activos. –

La DTIC en coordinación con la Unidad de Control de Bienes y Bodega tiene la responsabilidad de mantener el inventario completo y actualizado de los recursos de hardware y software de la institución en función a las normas de control interno.

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 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 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 10. Acceso a los servicios tecnológicos. -

- 1. Los sistemas informáticos institucionales y demás servicios de tecnología que provee la institución a la comunidad politécnica son de uso exclusivo para el ámbito académico, de investigación, vinculación con la sociedad y gestión administrativa; y el acceso a estos será a través de una cuenta de correo institucional asignada utilizando un sistema de autenticación centralizada (CAS).
- 2. El propietario de una cuenta es el único responsable de su uso, cuando se detecte una actividad prohibida, la ESPOCH responsabilizará al propietario de la misma.

Artículo 11. Gestión de privilegios. -

- 1. La asignación, modificación o revocación de privilegios en los sistemas informáticos y demás servicios institucionales será responsabilidad del administrador. De igual manera el usuario se hace responsable de sus privilegios asignados. Los privilegios de un usuario serán cancelados en el momento de la finalización de su relación con la ESPOCH.
- 2. Al menos, cada año, se realizará una revisión de los privilegios de acceso de todos los usuarios.

Artículo 12. Software. -

- 1. Queda estrictamente prohibido gestionar software y demás fuentes que violen la ley de derechos de autor.
- 2. Solo el personal autorizado (personal de la DTIC y técnicos afines al área informática de las facultades y sedes) se encargará de la instalación de software en la institución.
- 3. Se prohíbe descargar software sin la autorización de la DTIC. De ser necesario la unidad requirente debe solicitar por medio del sistema de mesa de ayuda la validación para su descarga.
- 4. Se prohíbe que los miembros de la comunidad politécnica realicen copias no autorizadas de código fuentes, sistemas informáticos institucionales, base de datos, y demás información de propiedad de la ESPOCH.
- 5. Se prohíbe ceder o comercializar las licencias de software adquiridas por la ESPOCH.
- 6. La DTIC a través de sus áreas correspondientes contará con un repositorio donde se almacenará todo el software autorizado para su uso.



7. A menos que expresamente se estipule lo contrario, está absolutamente prohibida la instalación y/o utilización de cualquier tipo de software no licenciado y/o no autorizado, en los equipos conectados a la red de la institución, incluyendo "freeware" o "shareware".
8. No se ejecutarán archivos o software que provengan de fuentes desconocidas en los equipos informáticos conectados a la red institucional para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos. Al ser necesario y fundamentado para creer que un archivo o software de fuente desconocida pueda contener información de importancia, debe reportarse a través del sistema de mesa de ayuda para recibir asistencia.

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.
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 14. Conexiones remotas. -

1. Los usuarios únicamente deben establecer conexiones remotas a través de VPN y software de escritorio remoto seguros.
2. Se utilizará la conexión de acceso remoto únicamente para acceder a servicios exclusivos de la ESPOCH los cuales sean inalcanzables desde redes externas, el acceso será solo para el personal autorizado, de acuerdo con las labores desempeñadas y condiciones de uso. La DTIC monitoreará las conexiones remotas a los recursos de la plataforma tecnológica de la institución de manera permanente.

Artículo 15. Acceso a la Red Inalámbrica. -

1. La DTIC es la única dependencia autorizada para configurar redes inalámbricas y administrar sus usuarios. Cuando se identifique redes inalámbricas no autorizadas serán deshabilitadas inmediatamente.
2. La institución garantizará el servicio de red inalámbrica para usuarios invitados, misma que permitirá acceder a los servicios tecnológicos autorizados en las zonas de cobertura institucional.

Artículo 16. Monitoreo de los Accesos. -

1. El área de Seguridad Informática realizará el monitoreo de los servicios tecnológicos con el fin de localizar accesos no autorizados, registrando eventos que suministren evidencias en caso de producirse incidentes relativos a la seguridad. A tal efecto, se tendrán en cuenta los registros de eventos y de uso de los sistemas descritos a continuación:
 - a) Intentos de acceso fallidos.
 - b) Bloqueos de cuenta.
 - c) Cuentas inactivas y deshabilitadas.



- d) Últimos accesos a cuentas.
- e) Accesos no autorizados.
- f) Uso de Privilegios.
- g) Alertas de sistema, entre otros.

Artículo 17. Sesiones Inactivas. –

La DTIC a través del área de Soporte y Mantenimiento en coordinación con los técnicos afines al área informática de las facultades y sedes activará en todos los equipos de cómputo institucionales protectores de pantalla con contraseñas, con el fin de evitar que terceros puedan acceder fácilmente a la información.

Además, si en los sistemas informáticos, sistemas operativos, entre otros, se detecta inactividad por un periodo igual o superior a 15 minutos finalizarán la sesión de usuario.

Artículo 18. Accesos al Sistema Operativo. -

Los medios de seguridad para restringir el acceso de usuarios no autorizados a los sistemas operativos deberán contener como mínimo las siguientes características:

1. Autenticar usuarios únicamente autorizados.
2. Registrar intentos exitosos y fallidos de autenticación;
3. Emitir alarmas cuando se violan las políticas de seguridad del sistema;
4. Restringir el tiempo de conexión de los usuarios.
5. Cuando se trate de privilegios especiales (administrador, root, etc.), tal revisión de privilegios se deberá realizar, al menos cada año, y, en cualquier caso, siempre que existan:
 - a) Alta o baja de nuevos usuarios.
 - b) Además, los privilegios de acceso de usuarios, deben ser revisados siempre que existan cambios en las funciones o responsabilidades. Se tendrán en cuenta, al menos, las siguientes cuestiones:
 - Necesidad de nuevos permisos.
 - Cancelación de antiguos permisos.
 - Segregación de funciones.
 - Devolución de activos y modificación o cancelación de permisos de accesos físicos.
 - Modificación de contraseñas de acceso.
 - Notificación al personal implicado de su baja o cambio.
 - Necesidad de retención de registros.

Artículo 19. Centro de Datos. -

1. El acceso al centro de datos, centros de cableado, gabinetes (racks) donde se encuentre alojada la infraestructura de procesamiento, almacenamiento, networking y seguridad es restringido y solo el personal autorizado puede tener acceso a estos. Además, no está permitida la captura de imágenes de cualquier índole, a menos de existir autorización para ello.
2. El personal de la DTIC, facultad o sede, según corresponda garantizará el monitoreo y registro de la bitácora para los accesos otorgados a estos espacios físicos.



CAPITULO IV

Medios Removibles

Artículo 20. Directrices de uso. –

El uso de medios removibles, se regirá a través de los siguientes lineamientos:

1. El manejo seguro de medios removibles en donde se puede almacenar información será responsabilidad de los servidores politécnicos y deben contemplar lo descrito en la carta compromiso de confidencialidad, no divulgación, reserva y resguardo de información digitalizada.
2. El servidor politécnico tendrá la responsabilidad de garantizar la protección de la información contenida en el medio removable que le fue asignado. Evitando accesos no autorizados, daños, manipulación, extravío de la información o del medio, e informando en forma oportuna cualquier deterioro.
3. Los medios removibles que registren información clasificada como restringida o confidencial no podrán salir de la institución salvo autorización superior expresa por escrito.
4. Los medios removibles que contengan información clasificada como restringida o confidencial y que cuya información deba ser eliminada deberá someterse a técnicas de borrado seguro de datos, dejando registro de las acciones realizadas durante el proceso de eliminación, para facilitar la trazabilidad de eventos.

CAPITULO V.

RESPALDOS

Artículo 21. Gestión de respaldos. –

La gestión de respaldos se regirá a través de los siguientes lineamientos:

1. El custodio de un computador de escritorio y portátil será el responsable de mantener respaldada la información que resida en el equipo para lo cual puede utilizar el almacenamiento asignado a su cuenta de correo institucional u otros medios de almacenamiento institucionales, de ser necesaria se realizará la inducción o acompañamiento para tal efecto, se puede realizar una solicitud a través del sistema de mesa de ayuda.
2. Toda vez que el servidor politécnico haya concluido su relación laboral con la institución debe entregar los respaldos de información a su jefe inmediato para proceder a firmar la Hoja de Paz y Salvo. Esta información se conservará por un lapso de 7 años.
3. La DTIC a través del área de Infraestructura de Tecnologías de la Información y Comunicación será la responsable de respaldar la información resguardada en el data center institucional e infraestructura como servicio en la nube.
4. Sobre la conservación de la información en el centro de datos - DTIC:
 - a. **Servicio crítico nivel 1:** impacto potencial alto y una alta probabilidad de concurrencia. La información se respaldará al menos 1 vez al día. Y el tiempo que se debe mantener el respaldo deberá ser no menos a seis (6) meses.
 - b. **Servicio crítico nivel 2:** impacto potencial moderado - alto y una probabilidad de concurrencia moderada - alta. La información debe ser respaldada al menos dos (2) veces al mes. Y el tiempo que se debe mantener el respaldo deberá ser no menos a seis (6) meses.



- c. **Servicio crítico nivel 3:** impacto potencial moderado - bajo y una probabilidad de concurrencia moderada - baja. La información se respaldará al menos dos (2) veces cada seis (6) meses. Y el tiempo que se debe mantener el respaldo deberá ser no menos a seis (6) meses.
- d. **Servicio crítico nivel 4:** impacto potencial bajo y una probabilidad de concurrencia baja. La información se respaldará al menos una (1) vez al año o según requerimiento del administrador del servicio o sistema. Y el tiempo que se debe mantener el último respaldo deberá ser no menos a un (1) año.

CAPITULO VI TELETRABAJO

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.

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.

Artículo 24. Tablets y smartphones.

Al utilizar dispositivos móviles como tablets o smartphone, el servidor politécnico debe activar lo siguiente en el dispositivo:

1. Se debe limitar el acceso al dispositivo mediante un bloque o con contraseña, patrón o similar.
2. Se debe cifrar la memoria del dispositivo en caso de contener información sensible.





3. Se debe disponer de medidas para poder localizar el dispositivo o hacer un borrado remoto del dispositivo en caso de pérdida o robo.
4. Se deben tomar medidas para prevenir y detectar malware en los dispositivos móviles.
5. Se deben instalar siempre las últimas actualizaciones de seguridad de los programas y sistemas operativos.
6. No conectarse a Wi-Fi abiertas, redes públicas de hoteles, bibliotecas, locutorios, etc.
7. Se deben desactivar las conexiones inalámbricas que no se utilicen como el Bluetooth, Wi-Fi o NFC.

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)
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 26. Borrado remoto. –

Todo equipo informático, sea de escritorio, portátil, tablets o smartphone deben instalarse aplicaciones para que contemple lo siguiente:

1. Administrar remotamente los dispositivos extraviados o robados.
2. Activar el GPS del dispositivo (si lo tiene)
3. Aplicación para hacer un borrado completo del equipo

Artículo 27. Sistemas de almacenamiento online.

El almacenamiento online o en la nube, debe ser utilizada para la información institucional.

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.

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 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 VII

Responsabilidades, consecuencias de la aplicación inadecuada de las políticas de seguridad informática

Artículo 30. Responsabilidades de la DTIC.

Ejecutará las siguientes acciones:

1. Elaboración y actualización de las presentes políticas.
2. Evaluación del cumplimiento de las presentes políticas.
3. Establecer mecanismos de control, auditoría y mejora continua.
4. La DTIC es la única dependencia que gestionará las herramientas tecnológicas para garantizar la seguridad informática de la institución.

Artículo 31. Responsabilidades de la Dirección de Talento Humano. –

Asegurar que tanto los docentes, administrativos y trabajadores hayan firmado la carta compromiso de confidencialidad, no divulgación, reserva y resguardo de información digitalizada.

Artículo 32. Responsabilidades de los politécnicos.

Los estudiantes que por cualquier motivo ya sea académico, de investigación o vinculación con





la sociedad accedan a cualquier tipo de información de propiedad de la ESPOCH deben firmar la carta compromiso de confidencialidad, no divulgación, reserva y resguardo de información digitalizada anexa a este documento.

Artículo 33. Responsabilidad de terceros. –

Todo proveedor o tercero que intervenga en la ejecución de los procesos de la ESPOCH, que tenga acceso a información restringida 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; y contar con acuerdos de no divulgación ni uso que perjudique a la institución. Para ello deberá firmar la carta compromiso de confidencialidad, no divulgación, reserva y resguardo de información digitalizada anexa a este documento.

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.

Información del documento	
Documento	Políticas de Seguridad Informática
Versión	2.0
Elaborado por	Área de Seguridad Informática – DTIC
Revisado por	Dirección de Tecnologías de la Información y Comunicación
Aprobado por	Consejo Politécnico
Resolución	426.CP.2026
Fecha de aprobación	23 de junio de 2026
Vigencia	Desde su aprobación
Próxima revisión	Cuando existan cambios normativos, tecnológicos o de riesgos, o como máximo cada dos años.