
# MANUAL DE POLITICAS Y LINEAMIENTOS DE SEGURIDAD INFORMÁTICA DEL INSTITUTO PARA LA COMPETITIVIDAD Y EL COMERCIO EXTERIOR (ICCE) DE NUEVO LAREDO

## INTRODUCCIÓN

El presente documento tiene como finalidad dar a conocer las políticas y estándares de Seguridad Informática que deberán observar los usuarios de servicios de tecnologías de información, para proteger adecuadamente los activos tecnológicos y la información del ICCE.

La base para que cualquier organización pueda operar de una forma confiable en materia de Seguridad Informática comienza con la definición de políticas y estándares adecuados.

La Seguridad Informática es una función en la que se deben evaluar y administrar los riesgos, basándose en políticas y estándares que cubran las necesidades del ICCE en materia de seguridad.

**Objetivo:** Establecer y difundir las políticas y lineamientos de Seguridad Informática a todo el personal del ICCE, para que sea de su conocimiento y cumplimiento en los recursos informáticos asignados.

**Alcance:** El documento define las políticas y lineamientos de Seguridad que deberán observar todos los usuarios para el buen uso del equipo de cómputo, aplicaciones y servicios informáticos del ICCE.

**Beneficios:** Las políticas y lineamientos de Seguridad Informática establecidos dentro de este documento son la base para la protección de los activos tecnológicos e información del ICCE.

# 1. Políticas y lineamientos de seguridad del personal

Todo usuario de bienes y servicios informáticos se compromete a conducirse bajo los principios de confidencialidad de la información y de uso adecuado de los recursos informáticos del ICCE, así como el estricto apego al Manual de Políticas y Lineamientos de Seguridad Informática para usuarios.

**Obligaciones de los usuarios:**

Es responsabilidad de los usuarios de bienes y servicios informáticos leer el presente manual y cumplir las políticas y lineamientos de Seguridad Informática para usuarios explicados en el presente documento.

**Acuerdos de uso y confidencialidad:**

Todos los usuarios de bienes y servicios informáticos del ICCE deberán conducirse conforme a los principios de confidencialidad y uso adecuado de los recursos informáticos y de información del ICCE, así como comprometerse a cumplir con lo establecido en el presente manual.

## 2. Políticas y lineamientos de seguridad física y ambiental

Los mecanismos de control y acceso físico para el personal y terceros deben permitir el acceso a las instalaciones y áreas restringidas del ICCE sólo a personas autorizadas para la salvaguarda de los equipos de cómputo y de comunicaciones.

**Resguardo y protección de la información:**

- El usuario deberá reportar de forma inmediata a la Coordinación de Información cuando detecte que existan riesgos reales o potenciales para equipos de cómputo o comunicaciones.
- El usuario tiene la obligación de proteger los CD-ROM, DVDs, memorias USB, tarjetas de memoria, discos externos, computadoras y dispositivos portátiles que se encuentren bajo su administración, aun cuando no se utilicen y contengan información reservada o confidencial.
- Es responsabilidad del usuario evitar en todo momento la fuga de la información del ICCE que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

**Protección y ubicación de los equipos:**

- Los usuarios no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización de la Coordinación de Información, debiéndose solicitar a la misma en caso de requerir este servicio.
- El área de Jefatura Administrativa será la encargada de generar el resguardo y recabar la firma del usuario informático como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada.
- Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.
- Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del gabinete.
- Se debe mantener el equipo informático en un entorno limpio y sin humedad.
- El usuario debe asegurarse que los cables de conexión no sean pisados o aplastados al colocar otros objetos encima o contra ellos.
- Cuando se requiera realizar cambios múltiples del equipo de cómputo derivado de reubicación de lugares físicos de trabajo, éstos deberán ser notificados a la Coordinación de Información los movimientos debidamente autorizados por el titular del área que corresponda.
- Queda prohibido que el usuario abra o desarme los equipos de cómputo, porque con ello perdería la garantía que proporciona el proveedor de dicho equipo.

**Mantenimiento de equipos:**

- Únicamente el personal autorizado de la Coordinación de Información podrá llevar a cabo los servicios y reparaciones al equipo informático.

- Los usuarios deberán asegurarse de respaldar la información que considere relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo previendo así la pérdida involuntaria de información, derivada de proceso de reparación, solicitando la asesoría del personal de la Coordinación de Información.

**Pérdida o transferencia de equipos:**

- El usuario que tenga bajo su resguardo algún equipo de cómputo será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.
- El usuario deberá dar aviso de inmediato a la Jefatura de Administración de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su resguardo.

**Daño del equipo:**

El equipo de cómputo o cualquier recurso de tecnología de información que sufra alguna descompostura por maltrato, descuido o negligencia por parte del usuario, deberá cubrir el valor de la reparación o reposición del equipo o accesorio afectado. Para tal caso la determinará la causa de dicha descompostura.

## 3. Políticas y lineamientos de seguridad y administración de operaciones de cómputo.

Los usuarios deberán utilizar los mecanismos institucionales para proteger la información que reside y utiliza la infraestructura del ICCE. De igual forma, deberán proteger la información reservada o confidencial que por necesidades institucionales deba ser almacenada o transmitida, ya sea dentro de la red interna del ICCE o hacia redes externas como internet.

Los usuarios del ICCE que hagan uso de equipo de cómputo, deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser virus, malware o spyware. El usuario puede acudir a la Coordinación de Información para solicitar asesoría.

**Uso de medios de almacenamiento:**

Los usuarios deberán respaldar de manera periódica la información sensible y crítica que se encuentre en sus computadoras personales o estaciones de trabajo, solicitando asesoría de la Coordinación de Información para determinar el medio en el que se realizará el respaldo.

**Instalación de software:**

- Los usuarios que requieran la instalación de software que no sea propiedad del ICCE deberán justificar su uso y solicitar su autorización a la Coordinación de Información, indicando el equipo de cómputo donde se instalará el software y el período que permanecerá dicha instalación.

- Se considera una falta grave el que los usuarios instalen cualquier tipo de programa (software) en sus computadoras, estaciones de trabajo, servidores, o cualquier equipo conectado a la red del ICCE, que no esté autorizado por la Coordinación de Información.

**Administración de la configuración:**

Los usuarios de las áreas del ICCE no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red del ICCE sin la autorización por escrito de la Coordinación de Información.

**Seguridad de la Red:**

Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por la Coordinación de Información en la cual los usuarios realicen la exploración de los recursos informáticos en la red del ICCE, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y mostrar una posible vulnerabilidad.

**Uso del correo electrónico:**

- Los usuarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien más (mientras esta persona se encuentra fuera o ausente), el usuario ausente debe redireccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa al del ICCE a menos que cuente con la autorización del titular del área de adscripción.
- Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información que es propiedad del ICCE. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor
- Los usuarios podrán enviar información reservada y/o confidencial exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones, a través del correo institucional que le proporcionó la Coordinación de Información.
- El ICCE, se reserva el derecho de acceder y revelar todos los mensajes enviados por este medio para cualquier propósito y revisar las comunicaciones vía correo electrónico de personal que ha comprometido la seguridad violando políticas de Seguridad Informática del ICCE o realizado acciones no autorizadas.
  Como la información del correo electrónico institucional del ICCE es privada, la única forma en la que puede ser revelada es mediante una orden judicial.
- El usuario debe de utilizar el correo electrónico del ICCE, única y exclusivamente para los recursos que tenga asignados y las facultades que les hayan sido atribuidas para el desempeño de su empleo, cargo o comisión, quedando prohibido cualquier otro uso distinto.
- Queda prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.

**Controles contra código malicioso:**

- Para prevenir infecciones por virus informáticos, los usuarios del ICCE, deben evitar hacer uso de cualquier clase de software que no haya sido proporcionado y validado por la Coordinación de Información.
- Los usuarios del ICCE, deben verificar que la información y los medios de almacenamiento, considerando al menos memorias USB, discos flexibles, CD´s, archivos de computadora, bases de datos, documentos u hojas de cálculo, etc. que sean proporcionados por personal externo o interno, y a su vez tengan que ser descomprimidos, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado por la Coordinación de Información.
- Ningún usuario del ICCE debe intencionalmente escribir, generar, compilar, copiar, propagar, ejecutar o tratar de introducir código de computadora diseñado para autoreplicarse, dañar o en otros casos impedir el funcionamiento de cualquier memoria de computadora, archivos de sistema o software. Tampoco debe probarlos en cualquiera de los ambientes o plataformas del ICCE. El incumplimiento de este estándar será considerado una falta grave.
- Ningún usuario ni empleado del ICCE o personal externo podrá bajar o descargar software de sistemas, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización de la Coordinación de Información.
- Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo y llamar a la Coordinación de Información para la detección y erradicación del virus.
- Los usuarios no deberán alterar o eliminar las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por la Dirección de Informática en programas tales como:
    - Antivirus;
    - Correoelectrónico;
    - Paquetería Office;
    - Navegadores; u
    - Otros programas
- Debido a que algunos virus son extremadamente complejos, ningún usuario del ICCE debe intentar erradicarlos de modo manual, lo indicado es llamar al personal de la Dirección de Informática o representante de Tecnología Educativa en su zona para que sean ellos quienes lo solucionen

**Permisos de uso de internet:**

- El acceso a internet provisto a los usuarios del ICCE es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña.
- Los usuarios con acceso a Internet del ICCE tienen que reportar todos los incidentes de seguridad informática a la Coordinación de Información, inmediatamente después de su identificación, indicando claramente que se trata de un incidente de seguridad informática.
- Los usuarios con servicio de navegación en internet al utilizar el servicio aceptan que:
    - Serán sujetos de monitoreo de las actividades que realizan en internet.
    - Saben que existe la prohibición al acceso de páginas no autorizadas.

- Saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.
- Saben que existe la prohibición de descarga de software sin la autorización de la Coordinación de Información.
- La utilización de internet es para el desempeño de su función y puesto en el ICCE y no para propósitos personales.

## 4. Políticas y lineamientos de controles de acceso lógico.

Cada usuario es responsable del mecanismo de control de acceso; esto es, de su identificador de usuario (Usuario Id) y contraseña (password) necesarios para acceder a la información y a la infraestructura tecnológica del ICCE por lo cual deberá mantenerlo de forma confidencial.

El titular del área es el único que puede solicitar y otorgar la autorización para que se tenga acceso a la información que se encuentra en la infraestructura tecnológica del ICCE, otorgándose los permisos mínimos necesarios para el desempeño de sus funciones.

**Controles de Acceso Lógico:**

- Está prohibido que los usuarios utilicen la infraestructura tecnológica del ICCE para obtener acceso no autorizado a la información u otros sistemas de información de la misma.
- Todos los usuarios de servicios de información son responsables por su identificador de usuario y contraseña que recibe para el uso y acceso de los recursos.
- Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica del ICCE, a menos que se tenga autorización de la Jefatura Administrativa, y la Coordinación de Información.
- Los usuarios tienen prohibido compartir su identificador de usuario y contraseña, ya que todo lo que ocurra con ese identificador y contraseña será responsabilidad exclusiva del usuario al que pertenezcan, salvo prueba de que le fueron usurpados esos controles.
- Los usuarios tienen prohibido usar el identificador de usuario y contraseña de otros, aunque ellos les insistan en usarlo.

**Equipo desatendido:**

Los usuarios deberán mantener sus equipos de cómputo con controles de acceso como contraseñas y protectores de pantalla como una medida de seguridad cuando el usuario necesita ausentarse de su escritorio por un tiempo.

**Administración y uso de contraseñas:**

- La asignación de la contraseña para acceso a la red y la contraseña para acceso a sistemas, debe ser realizada de forma individual, por lo que queda prohibido el uso de contraseñas compartidas.

- Está prohibido que los identificadores de usuarios y contraseñas se encuentren de forma visible en cualquier medio impreso o escrito en el área de trabajo del usuario, de manera de que se permita a personas no autorizadas su conocimiento.
- Todos los usuarios deberán observar los siguientes lineamientos para la construcción de sus contraseñas:
    - No deben contener números consecutivos;
    - Deben estar compuestos de al menos seis (6) caracteres y máximo diez (10). Estos caracteres deben ser alfanuméricos, o sea, números y letras;
    - Deben ser difíciles de adivinar, esto implica que las contraseñas no deben relacionarse con el trabajo o la vida personal del usuario; y
    - Deben ser diferentes a las contraseñas que se hayan usado previamente.
- La contraseña podrá ser cambiada por requerimiento del dueño de la cuenta.
- Todo usuario que tenga la sospecha de que su contraseña es conocido por otra persona, tendrá la obligación de cambiarlo inmediatamente.
- Los usuarios no deben almacenar las contraseñas en ningún programa o sistema que proporcione esta facilidad.

**Administración y uso de contraseñas:**

- Está prohibido el acceso a redes externas por vía de cualquier dispositivo, cualquier excepción deberá ser documentada y contar con el visto bueno de la Coordinación de Información.
- La administración remota de equipos conectados a internet no está permitida, salvo que se cuente con la autorización y con un mecanismo de control de acceso seguro autorizado por la Coordinación de Información.

## 5. Políticas y lineamientos de seguridad informática.

De acuerdo a las funciones y atribuciones de la Coordinación de Información "...es la encargada de fijar las bases de la política informática que permitan conocer y planear el desarrollo tecnológico al interior del ICCE".

**Revisiones del cumplimiento:**

- La Coordinación de Información realizará acciones de verificación del cumplimiento del Manual de Políticas y Estándares de Seguridad Informática para usuarios.
- La Coordinación de Información podrá implementar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, para revisar la actividad de procesos que ejecuta y la estructura de los archivos que se procesan. El mal uso de los recursos informáticos que sea detectado será reportado conforme a lo indicado por la jefatura administrativa.

**Violaciones de seguridad informática:**

- Está prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática. A menos que se autorice por la Coordinación de información.
- Está prohibido realizar pruebas de controles de los diferentes elementos de Tecnología de la Información.
- Ningún usuario del ICCE debe probar o intentar probar fallas de la Seguridad Informática identificadas o conocidas, a menos que estas pruebas sean controladas y aprobadas por la Coordinación de Información.
- No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar, introducir cualquier tipo de código (programa) conocidos como virus, malware, spyware, o similares diseñado para autoreplicarse, dañar, afectar el desempeño, acceso a las computadoras, redes e información del ICCE.

Glosario de Términos:

## A

**Acceso**: Es el privilegio de una persona para utilizar un objeto o infraestructura

**Acceso Físico**: Es la actividad de ingresar a un área.

**Acceso Lógico**: Es la habilidad de comunicarse y conectarse a un activo tecnológico para utilizarlo.

**Antivirus**: Programa que busca y eventualmente elimina los virus informáticos que pueden haber infectado un disco rígido, o cualquier sistema de almacenamiento electrónico de información

**Ataque**: Actividades encaminadas a quebrantar las protecciones establecidas de un activo específico, con la finalidad de obtener acceso a ese archivo y lograr afectarlo.

## B

**Base de Datos**: Colección almacenada de datos relacionados, requeridos por las dependencias e individuos para que cumplan con los requerimientos de proceso de información y recuperación de datos.

## C

**Confidencialidad**: Se refiere a la obligación de los servidores públicos a no divulgar información a personal no autorizado para su conocimiento.

**Contraseña**: Secuencia de caracteres utilizados para determinar que un usuario específico requiere acceso a una computadora personal, sistema, aplicación o red en particular

**Control de Acceso:** Es un mecanismo de seguridad diseñado para prevenir, salvaguardar y detectar acceso no autorizado y permitir acceso autorizado a un activo.

ICCE
INSTITUTO PARA LA COMPETITIVIDAD Y EL COMERCIO EXTERIOR

## D

**Disponibilidad:** Se refiere a que la información esté disponible en el momento que se necesite.

## E

**Estándar:** Los estándares son actividades, acciones, reglas o regulaciones obligatorias diseñadas para proveer a las políticas de la estructura y dirección que requieren para ser efectivas y significativas.

## F

**Falta Administrativa:** Acción u omisión contemplada por la normatividad aplicable a la actividad de un servidor público, mediante la cual se finca responsabilidad y se sanciona esa acción u omisión.

**FTP:** Protocolo de transferencia de archivos. Es un protocolo estándar de comunicación que proporciona un camino simple para extraer y colocar archivos compartidos entre computadoras sobre un ambiente de red.

## G

**Gusano:** Programa de computadora que puede replicarse a sí mismo y enviar copias de una computadora a otra a través de conexiones de la red, antes de su llegada al nuevo sistema, el gusano debe estar activado para replicarse y propagarse nuevamente, además de la propagación, el gusano desarrolla en los sistemas de cómputo funciones no deseadas.

## H

**Hardware:** Elementos físicos de un equipo informático.

**Herramientas de seguridad:** Son mecanismos de seguridad automatizados que sirven para proteger o salvaguardar a la infraestructura tecnológica del ICCE.

## I

**Identificador de usuario:** Nombre de usuario (también referido como Usuario id único asignado a un servidor público para el acceso a equipos y sistemas desarrollados, permitiendo su identificación en los registros.

**Incidentes de seguridad:** Cualquier evento que represente un riesgo para la adecuada conservación de confidencialidad, integridad o disponibilidad de la información utilizada en el desempeño de nuestra función.

**Integridad:** Se refiere a la pérdida o deficiencia en la autorización, totalidad o exactitud de la información del ICCE. Es un principio de seguridad que asegura que la información y los sistemas de información no sean modificados de forma intencional.

**Intrusión:** Cualquier acceso no autorizado a los sistemas informáticos o activos.

## M

**Malware:** Código malicioso desarrollado para causar daños en equipos informáticos, sin el consentimiento del propietario. Dentro de estos códigos se encuentran: virus, spyware, troyanos, rootkits, backdoors, adware y gusanos.

**Mecanismos de Seguridad o de control:** Es un control manual o automático para proteger la información, activos tecnológicos, instalaciones, etc. que se utiliza para disminuir la probabilidad de que una vulnerabilidad exista, sea explotada, o bien ayude a reducir el impacto en caso de que sea explotada.

**Medios de Almacenamiento:** Son todos aquellos medios en donde se pueden almacenar cualquier tipo de información.

**"Necesidad de saber" principio:** Es un principio o base de seguridad que declara que los usuarios deben tener exclusivamente acceso a la información, instalaciones o recursos tecnológicos de información entre otros que necesitan para realizar o completar su trabajo cumpliendo con sus roles y responsabilidades dentro del ICCE.

## P

**Password:** Véase contraseña.

## R

**Respaldo:** Archivos, equipo, datos y procedimientos disponibles para el uso en caso de una falla o pérdida, si los originales se destruyen o quedan fuera de servicio.

**Riesgo:** Es el potencial de que una amenaza tome ventaja de una debilidad de seguridad (vulnerabilidad) asociadas con un activo, comprometiendo la seguridad de éste. Usualmente el riesgo se mide por el impacto que tiene.

## S

**Servidor**: Computadora que responde peticiones o comandos de una computadora cliente. El cliente y el servidor trabajan conjuntamente para llevar a cabo funciones de aplicaciones distribuidas

**Software:** Programas y documentación de respaldo que permite y facilita el uso de la computadora. El software controla la operación del hardware.

**Spyware:** Código malicioso desarrollado para infiltrar a la información de un equipo o sistema con la finalidad de extraerla sin la autorización del propietario.

## U

**Usuario:** Este término es utilizado para distinguir a cualquier persona que utiliza algún sistema, computadora personal o dispositivo (hardware).

## V

ICCE
INSTITUTO PARA LA COMPETITIVIDAD Y EL COMERCIO EXTERIOR

**Virus:** Programas o códigos maliciosos diseñados para esparcirse y copiarse de una computadora a otra por medio de los enlaces de telecomunicaciones o al compartir archivos o medios de almacenamiento magnético de computadoras.

**Vulnerabilidad:** Es una debilidad de seguridad o brecha de seguridad, la cual indica que el activo es susceptible a recibir un daño a través de un ataque, ya sea intencional o accidental.

ICCE
INSTITUTO PARA LA
COMPETITIVIDAD
Y EL COMERCIO EXTERIOR
DE NUEVO LAREDO