REGLAMENTO DE SEGURIDAD
PARA LAS TECNOLOGÍAS DE LA INFORMACIÓN

CAPITULO I
GENERALIDADES
Objetivos y Alcance

ARTÍCULO 1: El presente Reglamento tiene por objeto establecer los requerimientos que rigen la seguridad de las tecnologías de la información y garantizar un respaldo legal que responda a las condiciones y necesidades del proceso de informatización del país. Este Reglamento no sustituye las medidas específicas que norman el procesamiento de la información clasificada y limitada, que son objeto de normativas emitidas por el Ministerio del Interior.

ARTÍCULO 2: El término Seguridad de las Tecnologías de la Información utilizado en este Reglamento está relacionado con la confidencialidad, integridad y disponibilidad de la información tratada por los ordenadores y las redes de datos. El empleo de otros términos, tales como seguridad de la información, seguridad de los ordenadores, seguridad de datos o seguridad informática, tienen a los efectos de lo que aquí se establece, el mismo significado.

ARTÍCULO 3: Este Reglamento será de aplicación, en lo que a cada cual concierne, en todos los Órganos y Organismos de la Administración Central del Estado y sus dependencias; otras entidades estatales; empresas mixtas; sociedades y asociaciones económicas que se constituyan de acuerdo a la Ley; entidades privadas radicadas en el país; organizaciones políticas, sociales y de masas y personas naturales que posean o utilicen, en interés propio o de un tercero, tecnologías de la información. El cumplimiento de este Reglamento en áreas sensibles que son objeto de la atención directa del MININT y el MINFAR será realizado por los especialistas de estos órganos designados al efecto.

CAPITULO II

DEL SISTEMA DE SEGURIDAD INFORMATICA.

ARTÍCULO 4: Cada entidad que haga uso para el desempeño de su actividad de las tecnologías de la información está en la obligación de diseñar, implantar y mantener actualizado, un Sistema de Seguridad Informática a partir de la importancia de los bienes a proteger y de los riesgos a que están sometidos, con el fin de alcanzar los siguientes objetivos:

- Minimizar los riesgos sobre los sistemas informáticos.
- Garantizar la continuidad de los procesos informáticos.

ARTÍCULO 5: A partir del Sistema de Seguridad Informática diseñado, cada entidad elaborará su Plan de Seguridad Informática.

ARTÍCULO 6: El diseño del Sistema de Seguridad Informática y la elaboración del Plan de Seguridad Informática de cada entidad se realizarán en correspondencia con las metodologías establecidas al respecto por la Oficina de Seguridad para las Redes Informáticas, adscripta al Ministerio de la Informática y las Comunicaciones.

ARTÍCULO 7: Los jefes de entidades responden por la actualización de los Planes de Seguridad Informática, considerando para ello los siguientes factores:

a) La aparición de nuevas vulnerabilidades.
b) Los efectos de los cambios de tecnología o de personal.
c) La efectividad del sistema, demostrada por la naturaleza, número y daño ocasionado por los incidentes de seguridad registrados;

ARTÍCULO 8: En los Órganos y Organismos de la Administración Central del Estado y en aquellas organizaciones en que las tecnologías de la información son determinantes para su gestión se dispondrá de los cargos de especialistas de Seguridad Informática que se requieran para atender esta actividad, los cuales tendrán las siguientes atribuciones y funciones:

a) Organizar y controlar la actividad de Seguridad Informática.
b) Evaluar el estado de cumplimiento y aplicación de la base legal vigente en la materia.
c) Supervisar el trabajo del personal que responde por la Seguridad Informática en las entidades y organizar su preparación.
d) Proponer medidas ante violaciones de la base legal establecida en la materia.

ARTÍCULO 9: Los jefes a las diferentes instancias en los órganos, organismos y entidades responden por la protección de los bienes informáticos que le han sido asignados y tienen las siguientes obligaciones:

a) Identificar los requerimientos de seguridad de los bienes informáticos bajo su responsabilidad y de las aplicaciones en desarrollo, determinar el nivel de acceso de los usuarios a los mismos y la vigencia de estos accesos.
b) Participar en el diseño del Sistema de Seguridad y en la elaboración, evaluación y actualización del Plan de Seguridad Informática en la parte que concierne a su esfera de acción y garantizar su cumplimiento.
c) Aplicar las medidas y procedimientos establecidos en su área de responsabilidad.
d) Especificar al personal subordinado las medidas y procedimientos establecidos y controlar su cumplimiento.
e) Participar en la elaboración de los procedimientos de recuperación ante incidentes de seguridad y en sus pruebas periódicas.
f) Imponer o proponer sanciones ante violaciones del Sistema de Seguridad, en correspondencia con su naturaleza y con los daños ocasionados.

ARTÍCULO 10: El responsable de la actividad informática en cada entidad tiene las siguientes obligaciones:

a) Participar en el diseño del Sistema de Seguridad y en la elaboración, evaluación y actualización del Plan de Seguridad Informática, supervisar su aplicación y disciplina de cumplimiento.
b) Establecer y mantener los controles en correspondencia con el grado de protección requerido por el Sistema de Seguridad Informática diseñado.
c) Garantizar la disponibilidad de los bienes informáticos.
d) Asesorar a las distintas instancias sobre los aspectos técnicos vinculados con la seguridad de las tecnologías de la información.
e) Establecer los controles necesarios para impedir la instalación de cualquier tipo de hardware o software sin la autorización de la Dirección de la Entidad.
f) Participar en la elaboración de los procedimientos de recuperación ante incidentes de seguridad y en sus pruebas periódicas.
g) Informar a los usuarios de las regulaciones establecidas.

ARTÍCULO 11: Los usuarios de las tecnologías de la información asumen en primera instancia la responsabilidad de las consecuencias que se deriven de la utilización impropia de las mismas.

ARTÍCULO 12: Los usuarios de las tecnologías de información en órganos, organismos y entidades tienen las siguientes obligaciones:

a) Adquirir la preparación necesaria y los conocimientos de Seguridad Informática imprescindibles para el desempeño de su trabajo.
b) Contar con la autorización expresa del jefe facultado, para obtener acceso a cualquiera de los bienes informáticos.
c) Utilizar las tecnologías de información solo en interés de la entidad.
d) No transgredir ninguna de las medidas de seguridad establecidas.
e) Proteger las tecnologías o la terminal de red que le ha sido asignada y colaborar en la protección de cualquier otra, para evitar que sea robada o dañada, usada la información que contiene o utilizado de manera impropia el sistema al que esté conectada.
f) No instalar ni utilizar en las tecnologías equipamientos o programas ni modificar la configuración de las mismas, sin la correspondiente autorización del jefe facultado.
g) Cumplir las reglas establecidas para el empleo de las contraseñas.
h) Informar al dirigente facultado de cualquier anomalía de seguridad detectada.

CAPITULO III
EMPLEO CONVENIENTE Y SEGURO DE LAS TECNOLOGÍAS DE LA INFORMACION

Sección Primera
Clasificación y control de bienes informáticos

ARTÍCULO 13: Los bienes informáticos de una entidad deben ser utilizados en las funciones propias del trabajo en correspondencia con su objeto social.

ARTÍCULO 14: Todos los bienes informáticos de una entidad deberán estar identificados y controlados, para lo cual se conformará y mantendrá actualizado un inventario de éstos incluyendo sus componentes y las especificaciones técnicas de aquellos que pudieran ser suplantados.

ARTÍCULO 15: Cada uno de los bienes informáticos de una entidad tienen que ser puestos bajo la custodia documentada legalmente de una persona, que actuando por delegación de la dirección de la entidad, es responsable de su protección.

ARTÍCULO 16: Los jefes de entidades instrumentarán los procedimientos que se requieran para garantizar la autorización y el control sobre el movimiento de los bienes informáticos, los cuales deberán ser considerados a esos efectos de igual forma que el resto de los medios de la entidad.

Sección Segunda
Del personal

ARTÍCULO 17: Las funciones y responsabilidades de seguridad, tanto general como específica, serán documentadas y se incluirán dentro de las responsabilidades laborales del personal.

ARTÍCULO 18: El personal previsto para ocupar cargos vinculados a la actividad informática en órganos, organismos, entidades, organizaciones políticas, sociales y de masas, incluyendo personal eventual, estudiantes insertados y otros casos similares con acceso a sistemas críticos, a información de valor o a la supervisión y seguridad de los sistemas, deberá ser seleccionado adecuadamente.

ARTÍCULO 19: Los términos y condiciones del contrato de empleo incluirán la obligación de la entidad contratante en cuanto a la preparación del contratado, así como la responsabilidad del trabajador hacia la Seguridad Informática, precisando que este último aspecto mantiene su vigencia una vez finalizada la relación laboral. Deberán incluirse las acciones a tomar en caso que el trabajador pase por alto los requerimientos de seguridad.

ARTÍCULO 20: La utilización de las tecnologías y sus servicios asociados en cada entidad estará aprobada previamente por la dirección de la misma y basada en cada caso en la necesidad de uso por interés de la propia entidad.

ARTÍCULO 21: El uso no autorizado de las tecnologías de información y sus servicios asociados constituye una violación de los derechos de la entidad que es sancionable. Es un deber y un derecho de la dirección de cada entidad la supervisión del empleo de las tecnologías de la información por parte de los usuarios.

ARTÍCULO 22: Los Jefes a cada nivel, garantizarán que el personal vinculado a las tecnologías de la información esté capacitado para la utilización de las mismas, así como que conozca sus deberes y derechos en relación con el Sistema de Seguridad Informática implementado, los cuales deberán firmar una declaración como constancia de su conocimiento y compromiso de cumplimiento, que se incluirá en el contrato de trabajo.

ARTÍCULO 23: El acceso a las facilidades de procesamiento y a los servicios que brindan las tecnologías por parte de personal que no forme parte de la plantilla será en todos los casos objeto de una estricta autorización y control por parte de la dirección de cada entidad y a partir de los riesgos que esto pueda introducir se establecerán los requerimientos específicos que correspondan para garantizar la seguridad.

ARTÍCULO 24: Los usuarios de las tecnologías de la información están en la obligación de informar de inmediato cualquier incidente de seguridad, debilidad o amenaza a sistemas o servicios y las direcciones correspondientes exigirán su cumplimiento.

ARTÍCULO 25: Constituye una violación grave de la seguridad la realización de acciones de comprobación de vulnerabilidades contra sistemas informáticos nacionales o extranjeros.

ARTÍCULO 26: Ninguna persona está autorizada a introducir, ejecutar, distribuir o conservar en los medios de cómputo programas que puedan ser utilizados para comprobar, monitorear o transgredir la seguridad, así como información contraria al interés social, la moral y las buenas costumbres, excepto aquellas aplicaciones destinadas a la comprobación del sistema instalado en la organización para uso por especialistas expresamente autorizados por la dirección de la misma. En ningún caso este tipo de programas o información se expondrá mediante las tecnologías para su libre acceso.

Sección Tercera
Seguridad Física y Ambiental

ARTÍCULO 27: La dirección de cada entidad determinará las tecnologías de información que por las funciones a que estén destinadas, la información que contengan y las condiciones de los locales en que se encuentren ubicadas, requieran la aplicación específica de medidas de protección física.

ARTÍCULO 28: Las tecnologías de la información se ubicarán en áreas que garanticen la aplicación de medidas alternativas que permitan la creación de una barrera de protección a estos medios e impidan su empleo para cometer acciones malintencionadas o delictivas.

ARTÍCULO 29: En los edificios e instalaciones de cada entidad se determinarán áreas o zonas controladas con requerimientos específicos, protegidas por un perímetro de seguridad definido en dependencia de la importancia de los bienes informáticos contenidos en ellas y su utilización, de acuerdo con los criterios y denominaciones siguientes:

a) **Áreas limitadas,** son aquellas donde se concentran bienes informáticos de valor medio cuya afectación puede determinar parcialmente los resultados de la gestión de la entidad o de terceros.
b) **Áreas restringidas,** son aquellas en que se concentran bienes informáticos de alto valor e importancia crítica cuya afectación pueda paralizar o afectar severamente la gestión de ramas o sectores de la economía o de la sociedad; territorios o entidades.
c) **Áreas estratégicas**, son aquellas en que se concentran bienes informáticos de alto valor e importancia crítica que inciden de forma determinante en la seguridad y la defensa nacional; la seguridad aeronáutica; biológica; industrial; la generación y distribución de energía eléctrica; las redes informáticas y de comunicaciones del país; las relaciones exteriores y de colaboración; la economía nacional; las investigaciones científicas y el desarrollo tecnológico; la alimentación de la población; la salud pública y el suministro de agua.

ARTÍCULO 30: Las áreas o zonas controladas estarán protegidas con medidas adecuadas para garantizar el acceso exclusivamente al personal autorizado.

ARTÍCULO 31: La selección y diseño de las áreas controladas tomará en cuenta la posibilidad de daño por fuego, inundación, explosión, perturbaciones del orden y otras formas de desastre natural o artificial.

ARTÍCULO 32: El equipamiento instalado en las áreas controladas estará protegido contra fallas de alimentación y otras anomalías eléctricas, incluyendo el uso de fuentes de alimentación alternativas para los procesos que deban continuar en caso de un fallo de electricidad prolongado y será ubicado y protegido

de manera tal que se reduzcan los riesgos de amenazas ambientales y oportunidades de cualquier tipo de acceso no autorizado.

ARTÍCULO 33: En las Áreas Limitadas se aplicarán las medidas de protección física siguientes:

a) Se ubicarán en locales cuyas puertas y ventanas estén provistas de cierres seguros;
b) A los locales que tengan ventanas que se comuniquen con el exterior de la instalación, se le aplicarán medidas que garanticen su seguridad y que eviten la visibilidad hacia el interior del mismo;
c) Se prohíbe el acceso de personal no autorizado por la dirección de la entidad.
d) Se prohíbe la permanencia del personal fuera del horario laboral sin la debida justificación y autorización por escrito de la dirección de la entidad. Las autorizaciones referidas serán conservadas para su verificación en caso de necesidad.

ARTÍCULO 34: En las Áreas Restringidas, además de las medidas requeridas en las Áreas Limitadas, se aplicarán las siguientes:

a) Tienen que permanecer cerradas, incluso cuando existan personas laborando en ellas, y el acceso a las mismas debe ser controlado mediante los documentos de registro que para ello se establezcan;
b) El personal que acceda a estas áreas deberá cumplir requisitos especiales de idoneidad.
c) Los medios informáticos no podrán estar conectados de manera física o lógica a medios que se encuentren fuera del alcance de estas áreas ni a redes públicas de transmisión de datos;
d) Se aplicarán sistemas de detección y alarma que permitan una respuesta , efectiva ante accesos no autorizados cuando no se encuentre el personal que labora en las mismas;
e) Se implementarán mecanismos y procedimientos de supervisión de la actividad que se realiza en estas áreas;
f) Se prohíbe la introducción de soportes ópticos y magnéticos personales, excepto los que hayan sido autorizados de forma expresa por la dirección de la entidad.
g) Se prohíbe la introducción de cámaras fotográficas, de grabación de imágenes o cualquier tipo de almacenamiento digital ajeno a la misma.

ARTÍCULO 35: En las Áreas Estratégicas, además de las medidas requeridas en las Áreas Restringidas y Limitadas, se aplicarán las siguientes:

a) Todo el personal que labora en ellas o que por razones de servicio sea autorizado a permanecer en las mismas, deberá contar con una identificación personal visible que distinga el área.
b) Se implementarán medios especiales de supervisión de la actividad que en ellas se realiza;

c) El acceso a estas áreas por personas ajenas a la misma solo se realizará de manera excepcional, restringida y bajo supervisión, mediante un permiso especial en cada caso emitido por la dirección de la entidad.

ARTÍCULO 36: Todas las tecnologías de información, independientemente de su importancia, se protegerán contra alteraciones o sustracciones, ya sea de éstas o sus componentes, así como de la información que contienen.

ARTÍCULO 37: En las redes de las entidades los cables de alimentación o de comunicaciones que transporten datos o apoyen los servicios de información se protegerán contra la intercepción o el daño. Los cables de alimentación deberán estar separados de los cables de comunicaciones para evitar la interferencia.

ARTÍCULO 38: Los jefes de entidades garantizarán que el equipamiento reciba el mantenimiento correcto de acuerdo con los intervalos de servicio y especificaciones recomendados por el fabricante para asegurar su disponibilidad e integridad continuas. En caso de necesidad de envío de equipamiento fuera de las instalaciones para que reciban mantenimiento, se realizará en correspondencia con los procedimientos que se establezcan previamente para ello, observando las regulaciones establecidas en el país en materia de protección a la información.

ARTÍCULO 39: El uso fuera de las instalaciones de una entidad de cualquier equipo para el procesamiento de información tiene que estar autorizado legalmente por la dirección de la misma mediante el documento correspondiente. La seguridad que se le garantice deberá ser equivalente a la que tiene en las instalaciones habituales el equipamiento usado para el mismo propósito, tomando en cuenta los riesgos de trabajar fuera de la instalación.

ARTÍCULO 40: El equipamiento que cause baja o sea destinado para otras funciones será objeto de un procedimiento adecuado para evitar que la información que contiene pueda resultar comprometida. Los dispositivos de almacenamiento que contengan información crítica para la entidad deberán destruirse físicamente o sobrescribirse mediante un proceso completo en lugar de borrarlos como usualmente se hace.

ARTÍCULO 41: Se prohíbe el movimiento sin autorización de los equipos, la información o el software y en caso de que se autorice será realizado mediante un documento oficial que demuestre su legalidad y el movimiento deberá registrarse a la salida y a la entrada al reintegrarse el medio a su origen. Se deberán realizar inspecciones sorpresivas para detectar las extracciones no autorizadas.

Sección Cuarta
Seguridad de Operaciones

ARTÍCULO 42: Al determinar las responsabilidades que se asignan al personal se tendrá en cuenta el principio de separación de funciones, considerando aquellas tareas que no deben ser realizadas por una misma persona, a fin de reducir oportunidades de modificación no autorizada o mal uso de los sistemas informáticos.
ARTÍCULO 43: La introducción en una entidad de nuevos sistemas informáticos, actualizaciones y nuevas versiones será aprobada previamente a partir de su correspondencia con el sistema de seguridad establecido y los resultados de las pruebas que se realicen para determinar si cumple los criterios de seguridad apropiados.

ARTÍCULO 44: Las acciones para cubrir las brechas de seguridad y la corrección de los errores del sistema deberán estar minuciosamente controladas en cada entidad. Los procedimientos deberán asegurar que:

a) solo el personal claramente identificado y autorizado tenga acceso a sistemas en funcionamiento y a los datos;
b) todas las acciones de emergencia tomadas sean documentadas detalladamente;
c) la acción de emergencia sea reportada a la dirección y realizada de manera ordenada;

Sección Quinta
Identificación, autenticación y control de accesos

ARTÍCULO 45: En los sistemas en que es posible el acceso por múltiples usuarios se dispondrá para cada uno de ellos de un identificador de usuario personal y único. Las personas a las que se asignen identificadores de usuarios responden por las acciones que con ellos se realicen.

ARTÍCULO 46: La asignación de nuevos identificadores de usuarios en los sistemas se realizará a partir de un procedimiento que incluya la notificación del jefe inmediato del usuario. En caso de terminación de la necesidad del uso de los sistemas por el cese de la relación laboral u otras causas, se procederá de forma análoga para la eliminación del identificador de usuario.

ARTÍCULO 47: Para la utilización de contraseñas como método de autenticación de usuarios, se cumplirán los siguientes requisitos:

a) Serán privadas e intransferibles.
b) Su estructura, fortaleza y frecuencia de cambio estarán en correspondencia con el riesgo estimado para el acceso que protegen.

c) Combinarán en todos los casos letras y números sin un significado evidente, con una longitud mínima de 6 caracteres.
d) No pueden ser visualizadas en pantalla mientras se teclean.
e) No pueden ser almacenadas en texto claro (sin cifrar) en ningún tipo de tecnologías de información.

ARTÍCULO 48: En cada entidad se definirán de manera estricta los derechos y privilegios de acceso a sistemas y datos que tiene cada usuario y se implementará un procedimiento escrito en cada caso para otorgar o suspender dichos accesos.

Sección Sexta
Seguridad ante programas malignos

ARTÍCULO 49: Se prohíbe el diseño, la distribución o intercambio de códigos de virus informáticos u otros programas malignos entre personas naturales o jurídicas; se exceptúa la información enviada por usuarios a la autoridad competente para el análisis e investigación de programas malignos.

ARTÍCULO 50: En cada entidad se implementarán los controles y procedimientos para protegerse contra virus y otros programas dañinos que puedan afectar los sistemas en explotación, así como para impedir su generalización. Para la protección contra virus se utilizarán los programas antivirus de producción nacional u otros autorizados oficialmente para su uso en el país, debidamente actualizados.

ARTÍCULO 51: Ante indicios de contaminación por programas malignos, tanto en redes como en equipos no conectados a redes, se procederá al cese de la operación de los medios implicados y a su desconexión de las redes cuando corresponda, preservándolos para su posterior análisis y descontaminación por personal especializado y se revisarán los soportes con los cuales haya interactuado el medio contaminado.

ARTÍCULO 52: La contaminación por virus informáticos u otros programas malignos se considera un incidente de seguridad y se cumplirá en este caso lo establecido en el Artículo 89 del presente Reglamento. En todos los casos se determinará el origen y la responsabilidad de las personas involucradas.

Sección Séptima
Respaldo de la información

ARTÍCULO 53: Todas las entidades están en la obligación de implementar un sistema fiable de respaldo de la información esencial para su funcionamiento que permita la recuperación después de un ataque informático, desastre o fallo de los medios, para lo cual ejecutarán los procedimientos que aseguren la obtención sistemática de las copias que se requieran.

ARTÍCULO 54: La información de respaldo, conjuntamente con informes precisos y completos de las copias de respaldo y los procedimientos de recuperación documentados deberán almacenarse en otra ubicación que le permita no afectarse en caso de desastre en la ubicación principal.

ARTÍCULO 55: La información de respaldo deberá tener una protección física y ambiental consecuente con las normas aplicadas en la ubicación principal. Los controles aplicados a los medios en la ubicación principal deberán extenderse a la ubicación de los medios de respaldo.

ARTÍCULO 56: Los medios de respaldo deberán probarse regularmente y verificar su estado de actualización con el fin de asegurar que pueda confiarse en ellos para un uso de emergencia cuando sea necesario.

Sección Octava
Seguridad en Redes

ARTÍCULO 57: Los órganos, organismos y entidades están en la obligación de implementar los mecanismos de seguridad de los cuales están provistas las redes, así como de aquellos que permitan filtrar o depurar la información que se intercambie.

ARTÍCULO 58: En todas las redes se habilitarán las opciones de seguridad con que cuentan los sistemas operativos de forma tal que se garantice la protección de los servidores y las terminales, el acceso a la información solamente por personal autorizado y los elementos que permitan el monitoreo y auditoria de los principales eventos por un tiempo no menor de un año.

ARTÍCULO 59: Para la fiscalización y el monitoreo del empleo que se le da a las redes de datos y de los servicios en ellas implementadas las entidades instalarán los productos autorizados en el país para esos propósitos.

ARTÍCULO 60: La arquitectura y la configuración de los diferentes componentes de seguridad de una red y la implementación de sus servicios estarán en correspondencia con las políticas definidas y aprobadas para su empleo y en ningún caso deben ser el resultado de la iniciativa de una persona con independencia de la preparación que ésta posea.

ARTÍCULO 61: Toda red de computadoras deberá contar para su operación con la existencia de al menos una persona encargada de su administración.

ARTÍCULO 62: El Administrador de una red tiene, en relación con la Seguridad Informática, las siguientes obligaciones:

a) Garantizar la aplicación de mecanismos que implementen las políticas de seguridad definidas en la red.
b) Realizar el análisis sistemático de los registros de auditoria que proporciona el sistema operativo de la red.
c) Garantizar que los servicios implementados sean utilizados para los fines que fueron creados.
d) Comunicar a la dirección de la entidad los nuevos controles técnicos que estén disponibles y cualquier violación o anomalía detectada en los existentes.
h) Activar los mecanismos técnicos y organizativos de respuesta ante los distintos tipos de incidentes y acciones nocivas que se identifiquen, preservando toda la información requerida para su esclarecimiento.
i) Participar en la elaboración de los procedimientos de recuperación ante incidentes y en sus pruebas periódicas.
e) Informar a los usuarios de las regulaciones de seguridad establecidas y controlar su cumplimiento.
f) Participar en la confección y actualización del Plan de Seguridad Informática.

ARTÍCULO 63: La gestión de administración de las redes implica la concesión de máximos privilegios, debiéndose realizar directamente desde los puestos de trabajo habilitados al efecto. Se prohíbe la administración remota de estas redes mediante conexiones conmutadas a través de las redes públicas de transmisión de datos.

ARTÍCULO 64: Se prohíbe la adición de algún equipo o la introducción de cualquier tipo de software en una red, ya sea a través de soportes removibles o mediante acceso a redes externas, sin la autorización de la dirección de la entidad, garantizando su compatibilización con las medidas de seguridad establecidas para la protección de dicha red.

ARTÍCULO 65: Los usuarios que han recibido la autorización para el empleo de los servicios que brindan las redes son responsables por su propia conducta. Los usuarios deben conocer las políticas de seguridad para las computadoras y redes a que ellos acceden y están en la obligación de cumplir estas políticas.

ARTÍCULO 66: En las redes que prevean conexiones desde o hacia el exterior de una entidad es obligatorio instalar los medios técnicos que aseguren una barrera de protección entre las tecnologías de información de la entidad y la red externa, mediante los mecanismos de seguridad que sea necesario implementar.

ARTÍCULO 67: Las entidades instrumentarán la ejecución de procedimientos periódicos de verificación de la seguridad de las redes con el fin de detectar posibles vulnerabilidades, incluyendo para ello cuando sea procedente la comprobación de forma remota por entidades autorizadas oficialmente a esos efectos, debido a la sensibilidad de estas acciones.

ARTÍCULO 68: Las entidades autorizadas oficialmente para la comprobación de la seguridad de las redes de otras entidades están en la obligación de:

a) Garantizar la profesionalidad que requiere esta actividad.
b) Obtener la aprobación previa de las entidades que requieren estos servicios para su realización.
c) Mantener el máximo de discreción con relación a las posibles vulnerabilidades detectadas.
d) Abstenerse de la utilización del conocimiento obtenido sobre la red comprobada en beneficio propio.
e) Informar a la Oficina de Seguridad para las Redes Informáticas de los resultados de las comprobaciones realizadas.

ARTÍCULO 69: En las redes donde se establezcan servicios de intercambio de datos o mensajes con otras redes o usuarios externos se implementarán mecanismos de seguridad que garanticen la confidencialidad, la integridad, el control de accesos, la autenticación y el no repudio, según corresponda.

ARTÍCULO 70: Las entidades que coloquen información en servidores para su acceso público, establecerán las medidas y procedimientos que garanticen su integridad y disponibilidad, así como la correspondencia de su contenido con los intereses de la propia entidad y del país.

ARTÍCULO 71: Si por necesidades de conectividad u otros intereses se requiere hospedar un sitio en servidores ubicados en un país extranjero, siempre se hará como espejo o réplica del sitio principal en servidores ubicados en Cuba, estableciendo las medidas requeridas para garantizar su seguridad, particularmente durante el proceso de actualización de la información.

ARTÍCULO 72: Se prohíbe la colocación de páginas o sitios Web desde entidades estatales en servidores extranjeros que ofrecen estos servicios de forma gratuita.

ARTÍCULO 73: Los servidores de redes de una entidad destinados a facilitar accesos hacia o desde el exterior de las mismas no serán instalados en las máquinas en que se instalen los servidores destinados para el uso interno de dicha red.

ARTÍCULO 74: En los casos de redes corporativas que prevean la extrapolación de servicios internos, esto se realizará por puertos bien identificados y mediante la protección con dispositivos que garanticen el acceso a esos servicios por el personal autorizado.

ARTÍCULO 75: Los servicios que ofrecen las redes de datos de una entidad mediante conexiones externas solo se utilizarán en interés de la misma. La asignación de cuentas para el empleo de estos servicios será aprobada en todos los casos por la dirección de la entidad sobre la base de las necesidades requeridas para su funcionamiento.

ARTÍCULO 76: Se prohíbe el establecimiento de cuentas de correo electrónico desde entidades estatales en servidores que se encuentran en el exterior del país, considerando la inseguridad que el empleo de los mismos implica para la entidad por hallarse fuera del control del Estado Cubano. Si de manera excepcional por no haber otra alternativa, surgiera esta necesidad de forma puntual, tiene que ser aprobada previamente y por escrito por la dirección de la entidad, a partir de la valoración de las razones existentes, especificando claramente el tipo de información que se va a transmitir y el plazo de vigencia de esta modalidad.

ARTÍCULO 77: Se prohíbe vincular cuentas de correo electrónico de un servidor de una entidad a un servidor en el exterior del país con el fin de redireccionar y acceder a los mensajes a través del mismo.

ARTÍCULO 78: La suscripción a listas de correo electrónico y el empleo de servicios de conversación en tiempo real (chat) por parte del personal de una entidad será autorizado en todos los casos por la dirección de la misma en correspondencia con sus intereses y de las normas particulares establecidas para estos servicios, debiendo documentarse esta autorización de manera que pueda ser objeto de comprobación.

ARTÍCULO 79: Se prohíbe la difusión a través de las redes públicas de transmisión de datos de información contraria al interés social, la moral, las buenas costumbres y la integridad de las personas; o que lesione la Seguridad Nacional, por cualquier persona natural o jurídica. Las entidades instalarán los controles y mecanismos que permitan detectar y obstaculizar este tipo de actividades. Las violaciones detectadas serán informadas oportunamente a las instancias pertinentes.

ARTÍCULO 80: Ninguna persona natural o jurídica está autorizada para enviar mensajes de correo electrónico no solicitados a múltiples usuarios de forma indiscriminada (spam), ya sean de carácter informativo, comercial, cultural, social, con intenciones de engaño (hoax) u otros.

ARTÍCULO 81: Las redes proveedoras de servicios tomarán las medidas que se requieran para impedir la sobrecarga de los canales de comunicaciones, restringiendo el envío o recepción de grandes volúmenes de información y la generación de mensajes a múltiples destinatarios.

ARTÍCULO 82: Las entidades implementarán controles dirigidos a impedir e interrumpir la generación de cartas en cadena y el envío de mensajes de correo de forma masiva a través de las redes.

ARTÍCULO 83: Las entidades con redes destinadas a proveer servicios a otras personas naturales o jurídicas mediante conexiones remotas están en la obligación de cumplir los aspectos siguientes:

a) Establecer las medidas y procedimientos de Seguridad Informática que garanticen la protección de los servicios a brindar y los intereses de seguridad de los que los reciben.
b) Implementar los mecanismos y procedimientos que aseguren la identificación del origen de las conexiones, incluidas las conmutadas, así como su registro y conservación por un tiempo no menor de un año.
c) Dar a conocer a los clientes de estos servicios los requerimientos de Seguridad Informática que deben cumplir en correspondencia con las políticas de seguridad establecidas en la red que los brinda.
d) Facilitar el acceso de las autoridades competentes a los registros de las conexiones y cooperar con las mismas en la investigación de violaciones de las normas establecidas y de incidentes de seguridad.

ARTÍCULO 84: Ninguna persona, natural o jurídica está autorizada para explorar o monitorear las redes públicas de transmisión de datos en busca de vulnerabilidades o información sobre los usuarios legales de las mismas.

ARTÍCULO 85: El acceso no autorizado o la agresión a cualquier sistema de cómputo conectado a las redes públicas de transmisión de datos y la usurpación de los derechos de acceso de usuarios debidamente autorizados se consideran violaciones del presente Reglamento, independientemente de otras implicaciones legales que puedan derivarse de estas acciones.

CAPITULO IV
GESTIÓN DE INCIDENTES DE SEGURIDAD

ARTÍCULO 86: Las entidades están obligadas a formular la estrategia a seguir ante cualquier incidente o violación de la seguridad que pueda producirse en correspondencia con la importancia de los bienes informáticos que posea y las posibles alternativas a emplear para garantizar los servicios. Dicha estrategia deberá ser consecuente con los objetivos básicos de la entidad y tomará en consideración:

a) Los riesgos que la entidad enfrenta en términos de su probabilidad y su impacto, incluyendo una identificación y asignación de prioridades a los procesos críticos.
b) El impacto probable de las interrupciones sobre la gestión de la entidad.
c) Comprobar y actualizar regularmente los planes y procesos establecidos.

ARTÍCULO 87: Una vez establecida la estrategia a seguir, las entidades dispondrán las medidas y procedimientos que correspondan con el fin de garantizar la continuidad, el restablecimiento y la recuperación de los procesos informáticos.

ARTÍCULO 88: Las medidas y procedimientos de recuperación serán definidas a partir de la identificación de los posibles eventos que puedan causar la

interrupción o afectación de los procesos informáticos e incluirán las acciones de respuesta a realizar, la determinación de los responsables de su cumplimiento y los recursos necesarios en cada caso.

ARTÍCULO 89: Los procedimientos para la gestión de incidentes y violaciones de Seguridad Informática, especificarán los pasos a seguir para garantizar una correcta evaluación de lo que ha ocurrido, a quién, cómo y cuándo debe ser reportado, la respuesta adecuada, así como los aspectos relacionados con su documentación, la preservación de las evidencias y las acciones a seguir una vez restablecida la situación inicial. Para ello considerarán lo siguiente:

a) el reporte inmediato de la acción a la autoridad correspondiente;
b) la comunicación con los afectados o los involucrados en la recuperación del incidente;
c) el análisis y la identificación de las causas de los incidentes;
d) el registro de todos los eventos vinculados con el incidente;
e) la recolección y preservación de las trazas de auditoría y otras evidencias;
f) la planificación y la implementación de medidas para prevenir la recurrencia, si fuera necesario;

ARTÍCULO 90: Ante cualquier incidente que afecte la Seguridad Informática de una entidad, se designará por la dirección de la misma una comisión presidida por un miembro del Consejo de Dirección e integrada por especialistas no comprometidos directamente con el incidente, que realizará las investigaciones necesarias con el fin de esclarecer lo ocurrido, determinar el impacto, precisar los responsables y proponer la conducta a seguir.

ARTÍCULO 91: La dirección de cada entidad garantizará que al producirse un incidente o violación de la seguridad informática la información sobre este acontecimiento se reporte inmediatamente a la Oficina de Seguridad para las Redes Informáticas y a la instancia superior de la entidad. Este reporte incluirá como mínimo:

a) En que consistió el incidente o violación.
b) Fecha y hora de comienzo del incidente y de su detección.
c) Implicaciones y daños para la entidad y para terceros.
d) Acciones iniciales tomadas.
e) Evaluación preliminar

CAPITULO V

PRESTACIÓN DE SERVICIOS DE SEGURIDAD INFORMÁTICA A TERCEROS.

ARTÍCULO 92: Solo estarán autorizadas a brindar servicios de Seguridad Informática a terceros aquellas entidades que cuenten con la correspondiente autorización emitida por la Oficina de Seguridad para las Redes Informáticas, adscripta al Ministerio de la Informática y las Comunicaciones.

ARTÍCULO 93: Los requerimientos que debe cumplir una entidad para solicitar la autorización para prestar servicios de Seguridad Informática a terceros son los siguientes:

a) que el objeto social de dicha entidad coincida con estos fines;
b) que dicha entidad cuente con mecanismos que garanticen la calidad de los servicios y la idoneidad del personal;
c) preparación técnico - profesional de los especialistas que laboren en la entidad;
d) que la entidad esté en condiciones de cumplir los reglamentos y disposiciones establecidos en esta materia;
e) que cuente con medios de protección de la información a la que tenga acceso durante su trabajo;
f) que los productos de Seguridad Informática, que utilicen estén debidamente certificados por los órganos correspondientes del Ministerio de la Informática y las Comunicaciones; y
g) que el capital sea enteramente nacional y el personal designado para brindar los servicios sea ciudadano cubano y resida de forma permanente en el país.

CAPITULO VI

DE LA INSPECCION A LA SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACION

ARTÍCULO 94: El Ministerio de la Informática y las Comunicaciones tiene como atribución estatal la ejecución de inspecciones en materia de Seguridad a las Tecnologías de la Información.

ARTÍCULO 95:La inspección estatal en esta materia será ejecutada exclusivamente por los inspectores del Ministerio de la Informática y las Comunicaciones.

ARTÍCULO 96: Los Jefes de Órganos, Organismos y Entidades facultarán a especialistas debidamente preparados para realizar controles en materia de Seguridad Informática en las entidades subordinadas.

Sección Primera
Objetivos

ARTÍCULO 97: La inspección estatal a la Seguridad a las Tecnologías de la Información tiene los objetivos siguientes:

a) Evaluar los conocimientos y la aplicación de la base legal vigente.
b) Realizar diagnósticos sobre la efectividad de los Sistemas de Seguridad Informática aplicados en las entidades.
c) Verificar el grado de control y supervisión que se ejerce sobre los bienes informáticos, así como los resultados de la gestión de la Seguridad Informática.
d) Valorar la efectividad de los Planes de Seguridad Informática elaborados y su actualización y correspondencia con las necesidades de cada entidad.
e) Valorar la gestión e influencia que ejercen las instancias superiores sobre esta actividad.

Sección Segunda
Facultades de los inspectores

ARTÍCULO 98: Los inspectores de Seguridad Informática tienen las facultades siguientes:

a) Realizar la inspección con aviso previo o sin él.
b) Evaluar el estado del cumplimiento y aplicación de la base legal de Seguridad Informática vigente.
c) Identificar las violaciones y vulnerabilidades detectadas en el Sistema de Seguridad Informática.
d) Hacer evaluaciones, recomendaciones y disponer acciones correctivas ante violaciones de la base legal establecida.
e) Proponer sanciones administrativas u otra de las previstas en el Artículo 99.
f) Recomendar la realización de auditorias.
g) Proponer la suspensión de los servicios cuando se viole lo establecido en el presente Reglamento.
h) Verificar el cumplimiento de las acciones correctivas que hayan sido aplicadas como resultado de inspecciones anteriores si las hubiere.
i) Exigir la entrega de las trazas o registros de auditoria de las tecnologías de la información u otras posibles evidencias que se consideren necesarias.
j) Ocupar para su revisión los medios informáticos involucrados en cualquier tipo de incidente de seguridad y proponer su decomiso definitivo a las instancias correspondientes.

CAPITULO VII

DE LOS INCUMPLIMIENTOS

ARTÍCULO 99: Toda persona natural o jurídica que incumpla lo dispuesto en la presente Resolución y en las disposiciones legales vigentes en la materia, estará sujeta a la aplicación de las siguientes medidas:

a) Invalidación temporal o definitiva de las autorizaciones administrativamente concedidas por el Ministerio de la Informática y las Comunicaciones al infractor, entre ellas, cancelación de licencias, permisos, autorizaciones, desconexión parcial o total de las redes privadas de datos y otras;
b) Suspensión y/o cancelación, temporal o definitiva, de los servicios de informática y comunicaciones que hayan suscrito con empresas debidamente reconocidas y autorizadas por el Estado cubano;
d) Ocupación cautelar de los medios, instrumentos, equipamientos y otros utilizados para cometer la infracción, con la finalidad de disponer posteriormente el decomiso de los mismos, según proceda.
e) La aplicación de las medidas que correspondan, de conformidad con lo legalmente establecido.

ARTÍCULO 100: Toda persona natural o jurídica sujeta a la aplicación de las medidas descritas anteriormente puede apelar ante el Ministro del Ministerio de la Informática y las Comunicaciones en el plazo de 30 días hábiles contados a partir de la fecha de aplicada la medida. A su vez el Ministro dispondrá de 90 días hábiles para dar respuesta a dicha reclamación. La decisión de esta última instancia será inapelable.

Anexo

Principales Términos y Definiciones

Acceso no autorizado: Acceso a un sistema o a la información que este contiene, por parte de alguien no autorizado explícitamente para ello. Se puede tener acceso autorizado a un sistema y no tener derecho a acceder a determinadas áreas del mismo.

Amenaza: Situación o acontecimiento que pueda causar daños a los bienes informáticos. Puede ser una persona, un programa maligno o un suceso natural o de otra índole. Representan los posibles atacantes o factores que inciden negativamente sobre las debilidades del sistema.

Análisis de riesgos: Proceso dirigido a determinar la probabilidad de que las amenazas se materialicen sobre los bienes informáticos. Implica la identificación de los bienes a proteger, la determinación de las amenazas que actúan sobre ellos, así como la estimación de su probabilidad de ocurrencia y el impacto que puedan causar.

***Ataque*:** Intento de acceso o acceso a un sistema mediante la explotación de vulnerabilidades existentes en su seguridad.

Ataque de desfiguración: Agresión deliberada a una página o sitio Web modificando su estado parcial o totalmente, con lo que se afecta su integridad y su disponibilidad.

Autenticación: Método para comprobar la identificación de un usuario o proceso. Una vez identificado al usuario, es necesario que este demuestre de algún modo la veracidad de su identidad.

Autorización de usuarios: Proceso de determinación y aprobación de los niveles de acceso de un usuario a los sistemas informáticos o a parte de los mismos.

Barrera de Protección: Dispositivo físico o lógico utilizado para proteger un sistema, obstaculizando el acceso al mismo o entre sus componentes, ya sea de forma directa o remota.

Bienes Informáticos: Elementos componentes del sistema informático que deben ser protegidos en evitación de que como resultado de la materialización de una amenaza sufran algún tipo de daño.

Bomba lógica: Programa maligno preparado para actuar contra un sistema informático cuando se cumplan ciertas condiciones implementadas por su autor.

Caballos de Troya: Programas malignos que se introducen de manera subrepticia en los medios de cómputo para adquirir privilegios de acceso al sistema atacado y manipularlo a su conveniencia.

Confidencialidad: Condición que asegura que la información no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados.

Conexión Externa: Conexión en la que está presente, al menos, una de las condiciones siguientes:

- Acceso remoto a sistemas informáticos internos, por empleados o por terceros, desde medios técnicos que no están controlados por la Entidad.
- Acceso remoto a sistemas informáticos externos desde medios técnicos controlados por la Entidad.

- Conexión entre un servicio interno y un servicio ajeno a la Entidad.

Control de acceso: Método que garantiza que solo tengan acceso a un sistema o a la información que éste contiene, aquellos debidamente autorizados para ello. Los mecanismos de control de acceso se implementan utilizando técnicas de software y de hardware y por lo general incluyen: identificación y autenticación de usuarios; limitación de acceso a ficheros, monitorización de las acciones de los usuarios y un sistema de auditoria.

Cracker:: Intruso; individuo que intenta penetrar en un ordenador o sistema informático ilegalmente con intenciones nocivas.

Chat: Conversación interactiva utilizando diferentes métodos en tiempo real, a través de Internet, entre dos o más usuarios.

Denegación de Servicio: Significa que los usuarios no pueden obtener del sistema los recursos deseados. Es lo opuesto a disponibilidad y constituye uno de los posibles métodos de ataque realizado mediante la saturación de los sistemas provocando la generación de una cantidad tal de procesos que éstos no pueden ejecutar.

Disponibilidad: Propiedad que garantiza que los usuarios autorizados tengan acceso a la información y activos asociados cuando se requiera. Significa que el sistema, tanto hardware como software, se mantienen funcionando y que está en capacidad de recuperarse rápidamente en caso de fallo.

Gusanos: Programas que pueden provocar efectos tan dañinos como los causados por los virus, pero se diferencian de éstos en su forma de transmitirse, pues no infectan otros programas con una copia de sí mismos, ni son insertados en otros programas por sus autores. Suelen funcionar en grandes sistemas informáticos conectados en red, difundiéndose rápidamente a través de ésta.

Hacker: Intruso. Persona que con diferentes propósitos se dedica a incursionar en las redes informáticas sin reparar en las limitaciones existentes para su acceso ni en las barreras de protección establecidas en las mismas. En el contexto de nuestro país cualquier acción realizada contra las redes se considera ilegal.

Herramienta de Seguridad: Un dispositivo de hardware o software diseñado para proporcionar o comprobar la seguridad en un sistema informático.

Hoax (en español: rumor, falsedad, engaño): Mensajes de correo electrónico engañosos que se difunden por las redes con la ayuda de usuarios irresponsables que los reenvían formando largas cadenas, lo que consume un gran ancho de banda y congestiona los servidores. Su contenido generalmente se basa en temáticas religiosas o de solidaridad, alertas sobre virus muy dañinos, etc.

Identificación de usuarios: En todos los sistemas multiusuario, cada usuario posee un identificador (ID) que define quién es y qué lo identifica unívocamente en el sistema, diferenciándolo del resto.

***Impacto*:** Daños producidos por la materialización de una amenaza.

Incidente de Seguridad: Cualquier evento que se produzca, de forma accidental o intencional, que afecte o ponga en peligro las tecnologías de información o los procesos que con ellas se realizan.

Integridad: Condición que garantiza que la información sólo puede ser modificada, incluyendo su creación y borrado, por el personal autorizado. El concepto de integridad significa que el sistema no debe modificar o corromper la información que almacene, o permitir que alguien no autorizado lo haga.

Mecanismo de Seguridad: Implementación de hardware o software diseñada o construida para prevenir, detectar o responder a incidentes de seguridad.
Medidas de Seguridad Informática: Conjunto de acciones orientadas al fortalecimiento del Sistema de Seguridad Informática
No Repudio: Método para asegurar que las partes que intervienen en una transacción no nieguen su participación.
Plan de Seguridad Informática: Documento básico que establece los principios organizativos y funcionales de la actividad de seguridad informática en una entidad.
Procedimiento de Seguridad Informática: Secuencia predeterminada de acciones dirigida a garantizar un objetivo de seguridad.
Protocolo: Conjunto de normas, especificaciones y convenciones por el que se rigen los medios informáticos para comunicarse entre si e intercambiar información.
Puertas falsas (puertas traseras): Mecanismo establecido en el sistema por su diseñador o por alguien que ha modificado el funcionamiento del mismo. Su objetivo es ofrecer un modo de acceder al sistema evadiendo las medidas de seguridad establecidas cuando se usa el procedimiento normal, para proporcionar una ruta directa y oculta de acceso al sistema.
Responsable de Informática: Persona que dentro de la estructura de un Órgano, Organismo o Entidad ha sido designada para dirigir funcionalmente la actividad informática
Riesgo: Probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático, causando un impacto negativo en la organización.
Servicio de Seguridad: Función suministrada por un sistema para mejorar su seguridad. Se implementa mediante uno o varios mecanismos de seguridad.
Sistema de Seguridad Informática: Conjunto de medios humanos, técnicos y administrativos, que de manera interrelacionada garantizan diferentes grados de seguridad informática en correspondencia con la importancia de los bienes a proteger y los riesgos estimados.
Sistema Informático: Conjunto de bienes informáticos de que dispone una entidad para su correcto funcionamiento y la consecución de los objetivos propuestos
Soportes Removibles: Cualquier tipo de dispositivo intercambiable que permita la transferencia o almacenamiento de información.
Spam: Práctica de envío indiscriminado de mensajes de correo electrónico no solicitados.
Spyware: Un tipo de software que envía datos del sistema donde está instalado sin que el usuario dé su consentimiento o ni siquiera lo sepa. Este tipo de información puede ir desde los sitios Web que se visitan hasta algo más delicado como por ejemplo el nombre de usuario y la contraseña.
Trazas (logs) de auditoría: Registro cronológico de las acciones que se realizan en un sistema, los accesos al mismo y los procesos y ficheros que han intervenido.
Usuario: Quien hace uso de las tecnologías de información. Cualquier persona, con independencia de la responsabilidad asignada o del cargo que ocupe, cuando emplea estas tecnologías se denomina usuario.

Virus Informáticos: Programas capaces de reproducirse a sí mismos sin que el usuario esté consciente de ello. Se adicionan a programas de aplicación así como a componentes ejecutables del sistema de forma tal que puedan tomar el control del mismo durante la ejecución del programa infectado.
Vulnerabilidad: Punto o aspecto del sistema que es susceptible de ser atacado o de dañar la seguridad del mismo. Representan las debilidades o aspectos falibles o atacables en el sistema informático. Califica el nivel de riesgo de un sistema.