INSTITUTO DE PSIQUIATRÍA DEL ESTADO DE BAJA CALIFORNIA

(IPEBC)

Manual de aplicación de Tecnologías, Comunicación y Seguridad de la Información.

MAATIC-SI

Unidad responsable de su elaboración:
Departamento de Informática
Ejemplares impresos: 1

Página de su Publicación:
http://www.ipebc.gob.mx/transparencia/manuales.html

Mexicali, Baja California, Octubre de 2019

ÍNDICE

I. INTRODUCCIÓN

Con fundamento en el Artículo 46 del Reglamento Interno del IPEBC y en apego a las recomendaciones emitidas por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), el Departamento de Informática elaboró la presente "Manual Administrativo de aplicación en materia de Tecnologías de Información, Comunicaciones y Seguridad de la Información (MAAGTIC-SI)", con la finalidad de proteger la infraestructura computacional y todo lo relacionado con ésta, la cual incluye la información contenida.

II. OBJETIVO

Emitir las recomendaciones para los servidores públicos del ***"IPEBC"*** en el manejo y utilización de equipo de cómputo, aplicaciones y sistemas de información durante la ejecución de sus funciones a fin de cumplir con los requerimientos de seguridad y de control establecidos por la Entidad.

III. ABREVIATURAS Y DEFINICIONES

El presente es de aplicación obligatoria y tiene por objeto regular y sistematizar las actividades relativas a las recomendaciones en materia de seguridad de los sistemas y tecnologías de información que utilizan los servidores públicos del "***IPEBC"*** a través del Departamento de Informática.

Para sus efectos se entenderá por:

ACTIVOS DE INFORMACIÓN: Toda aquella información y medio que la contiene, que por su importancia y el valor que representa para la Entidad, deben ser protegidos para mantener su confidencialidad, disponibilidad e integridad, acorde al valor que se le otorgue.

ALERTA DE SEGURIDAD: Hecho o evento que se detecta y/o registra en los sistemas de tratamiento físico o electrónico, el cual advierte de un posible incidente de seguridad.

AMENAZAS: Circunstancia o condición externa, con la capacidad de causar daño a los activos explotando una o más de sus vulnerabilidades.

ARCHIVO: Al conjunto organizado de documentos producidos o recibidos por los servidores públicos en el ejercicio de sus atribuciones y funciones, con independencia del soporte, espacio o lugar que se resguarden.

CONFIDENCIALIDAD: Propiedad de la información para evitar su acceso, divulgación o revelación, no autorizados.

HACKER: significa en inglés "romper" o "quebrar" los sistemas de seguridad informáticos. Los hackers son una comunidad que invade sistemas, descifra claves y contraseñas de programas, roban datos o cometen cualquier otra actividad ilícita.

INCIDENTE DE SEGURIDAD: Cualquier violación a las medidas de seguridad físicas, técnicas o administrativas de un responsable, que afecte la confidencialidad, la integridad o la disponibilidad de la información.

INFORMÁTICA: Departamento de Informática del Instituto de Psiquiatría del Estado de Baja California.

IPEBC: Instituto de Psiquiatría del Estado de Baja California.

MAATIC-SI: Manual de aplicación de Tecnologías, Comunicación y Seguridad de la Información.

MEDIDAS DE SEGURIDAD: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.

RIESGO: Potencial o probabilidad de que ocurra un escenario donde una amenaza explote una o varias vulnerabilidades existentes en un activo o grupo de activos, y que éste cause un impacto negativo o daño.

SERVIDORES PÚBLICOS: Todos y cada uno de las personas que laboran en el ***"IPEBC"***.

VULNERABILIDAD: Circunstancia o condición propia de un activo, que puede ser explotada por una o más amenazas para causarle daño.

IV. GUÍA DE SEGURIDAD INFORMÁTICA

El presente manual recomienda acciones para la seguridad Informática de los activos de información del ***"IPEBC".***

IV.I ALCANCE

Este manual está dirigido, de aplicación y observancia a todo servidor público del ***"IPEBC"*** que tenga acceso o bajo su resguardo cualquier activo de información de la Entidad.

- Los servidores públicos no otorgarán acceso a familiares, amigos, vecinos, clientes, proveedores, vendedores y otros visitantes desconocidos, a los servicios de red del ***"IPEBC"*** mediante su cuenta institucional. En situaciones en las que se deba dar o requiera dar acceso a estas personas, los servidores públicos deberán considerar los siguientes puntos:

    - Verificar que las personas ajenas al **"IPEBC"** cuando se encuentren dentro de las instalaciones de ésta, accedan a los activos de información con la supervisión y monitoreo de los servidores públicos de la Entidad.

    - En caso de requerir transmitir información que se contengan en los activos de información, los servidores públicos del **"IPEBC"** evaluarán y bajo su consentimiento podrán otorgarle la información, misma que deberán verificar que sea únicamente la aprobada para ser extraída.

    - No instalarán en los equipos de cómputo programas destructivos o maliciosos (ejemplo: virus, gusanos, caballos de troya, puertas traseras, y en general, herramientas de hacking) que puedan causar daños, interferencias con otros sistemas, accesos no autorizados o disminución en el desempeño de los sistemas del ***"IPEBC".***

- Los servidores públicos que tengan equipo de cómputo asignado, se responsabilizará de su uso y de la información contenida en los mismos, por lo que se recomienda no compartirlos y estar en cumplimiento de los requerimientos de seguridad física y lógica establecidos.

- Los servidores públicos bloquearán sus pantallas o monitores cuando dejen desatendido su sistema de cómputo.

- En caso de que los servidores públicos tengan asignado un equipo de cómputo portátil (laptop, equipo móvil, entre otros) y sea víctima de robo o pérdida, debe reportar a la brevedad el incidente con su jefe inmediato y al área de ***"INFORMATICA".***

- Los servidores públicos del ***"IPEBC"*** revisarán todos los medios de almacenamiento removibles que sean introducidos o conectados a sus equipos de cómputo utilizando el programa antivirus instalado por ***"INFORMÁTICA".***

V.II USO DE CONTRASEÑAS

- Los servidores públicos son responsables de la custodia y manejo de sus identificadores de usuario y contraseñas (claves de acceso a los sistemas y aplicaciones).

- Los servidores públicos son responsables de todas las actividades que se realicen con sus identificadores de usuario y contraseñas, incluyendo la recepción y transmisión de información, la ejecución de transacciones que se hagan entre los sistemas de información del ***"IPEBC"*** y la ejecución de transacciones en las aplicaciones del ***"IPEBC".***

- Las contraseñas serán consideradas como información confidencial y no deben ser divulgadas o transferidas por ningún medio a ninguna persona. Cuando, por requerimiento de algún proceso del ***"IPEBC"*** requiera solicitar y proporcionar la contraseña personal, al término de su uso será cambiada de inmediato.

- Las contraseñas utilizadas por los servidores públicos deberán ser diferentes a las últimas 5 que se hayan utilizado durante el curso de su uso.

- En caso de que los servidores públicos intenten acceder al equipo de cómputo por más de 3 veces sin lograrlo y su cuenta sea bloqueada, lo notificará a su enlace informático para solicitar su reactivación.

- Los servidores públicos seleccionará contraseñas diferentes para los distintos sistemas a los que tienen acceso autorizado.

- Las contraseñas iníciales sólo serán válidas para el primer acceso.

- los servidores públicos son responsables de cambiarla después de acceder al sistema por primera vez.

- los servidores públicos utilizarán una nomenclatura robusta, considerando los siguientes elementos:

    a. Se utilizará una combinación de al menos 8 caracteres alfanuméricos.
    b. Incluirá en la contraseña el uso de letras minúsculas, mayúsculas, caracteres especiales, espacios, puntuación y números.
    c. No utilizará solo letras, solo números, solo mayúsculas o el mismo carácter repetido.
    d. La mejor guía para seleccionar una contraseña es que ésta debe ser fácil de recordar para quien la selecciona pero prácticamente imposible adivinar por otra persona.
    e. No se utilizará el nombre del identificador de usuario en ninguna forma (escrito al revés, doble, igual, etc.).
    f. No utilizarán nombres o apellidos del usuario en ninguna forma.
    g. No utilizarán el nombre del cónyuge, hijos, familiares, novias, mascotas, fechas, etc.

h. No utilizará información que pueda ser obtenida fácilmente como Registro Federal de Contribuyentes (RFC), números telefónicos, placas de automóvil, dirección, etc.
i. No utilizarán palabras de diccionario (en cualquier idioma o de alguna disciplina específica como medicina, química, etc.).
j. Se recomienda utilizar un método para elaborar contraseñas que sea fácil de aprender y de recordar, ejemplos de estos métodos son:
k. Seleccionar una o varias líneas de una canción o libro y formar la contraseña con la primera letra de cada palabra.
l. Alternar entre una consonante y una o dos vocales, produciendo una palabra que sea pronunciable y de esta forma fácil de recordad.

V.III USO DE INTERNET

- Los servidores públicos no publicarán ningún tipo de información clasificada como: (documentos, archivos, expedientes, fotografías) del ***"IPEBC"*** en Internet.

- Los servidores públicos notificarán a ***"INFORMÁTICA"*** en forma inmediata cualquier actividad sospechosa o evidencia de violaciones a la seguridad relacionadas con la conectividad hacia Internet (acceso no autorizado a la red, telecomunicaciones o sistemas de cómputo, transmisión aparente o real de un virus o gusano a través de la red, sabotaje aparente o real de cualquier archivo para el que el personal haya definido un usuario y contraseña).

- No se transmitirá información confidencial y reservada a través de Internet sin un mecanismo apropiado como encripción y sin previa autorización.

- El uso de los servicios de Internet se limita únicamente a las actividades propias del puesto necesarias para el desempeño de sus labores de los servidores públicos del ***"IPEBC".***

- No se usarán servicios de mensajería electrónica (ejemplo: Microsoft Messenger, Yahoo Messenger, AOL Messenger, ICQ, Trillian, entre otros) en los recursos de cómputo asignados al personal.

- Los servidores públicos no utilizarán los servicios de Internet para fines ilegales, en caso de no estar seguro de la legalidad de sus acciones, deberán solicitar información al personal de ***"INFORMÁTICA".***

- Los servidores públicos no puede levantar servidores ejemplo (servidores de web, dhcp, dns, entre otros) en los recursos de cómputo que no fueron asignados para ese fin.

V.IV USO DE CORREO ELECTRÓNICO

El uso del correo electrónico sólo será a través del dominio institucional (ipebc.gob.mx); siempre y cuando sea a solicitud o autorización de su Jefe inmediato; por lo cual no se emplearán cuentas personales para fines laborales.

V.V ESTÁNDARES Y NORMAS PARA ASEGURAR LA INFORMACIÓN

El conjunto de las medidas de seguridad y protección de la información y de disciplina informática constituirán la Seguridad Informática, que comprende medidas administrativas, organizativas, físicas, técnicas, legales y educativas dirigidas a prevenir, detectar y responder a acciones que pongan en riesgo o constituyan una amenaza para la confidencialidad, integridad y disponibilidad de la información que se procese, intercambie, reproduzca y conserve a través de las tecnologías informáticas y de comunicaciones; así como el correcto uso y conservación de las mismas.

Para la correcta administración de la Seguridad de la Información, se mantendrán acciones para cumplir con los tres requerimientos de mayor importancia para la información, estos son:

1. **Confidencialidad:** Busca prevenir el acceso no autorizado ya sea en forma intencional o no intencional a la información. La pérdida de la confidencialidad puede ocurrir de muchas maneras, como por ejemplo con la publicación intencional de información confidencial de la Entidad.

2. **Integridad:** Busca asegurar que no se realicen modificaciones por personas no autorizadas a los datos o procesos y/o que no se realicen modificaciones no autorizadas por personal autorizado a los datos o procesos; así como que los datos sean consistentes tanto interna como externamente.

3. **Disponibilidad:** Busca asegurar acceso confiable y oportuno a los datos o recursos para el personal apropiado.

VI. TIPOS DE AMENAZAS: Las amenazas se pueden clasificar principalmente como:

Tipos de	Ejemplos
Suplantación	Falsificar mensajes de correo electrónico.
Alteración	Alterar datos durante la transmisión; cambiar datos en archivos.
Repudio	Eliminar un archivo esencial y denegar este hecho.
Divulgación de información	Exponer la información en mensajes de error y exponer el código de los sitios Web.
Denegación de servicio	Inundar una red con diversas peticiones por ejemplo solicitudes de acceso a una página web institucional logrando saturarla y que se encuentre sin servicio.
Elevación de privilegios	Explotar vulnerabilidades para obtener privilegios en el sistema y obtener privilegios de administrador de forma ilegítima.

VII. ENTRENAMIENTO Y CONCIENCIACIÓN

Los servidores públicos que manejen activos de información asistirán a los programas de entrenamiento y concienciación en el tema de seguridad de la información provistos por el ***"IPEBC",*** cuando así se requiera.

VIII. MONITOREO DE USUARIOS

El ***"IPEBC"*** a través de ***"INFORMÁTICA"*** podrá reservarse el derecho de monitorear el correo electrónico, los directorios personales de archivos y otra información almacenada en los equipos del ***"IPEBC"*** en cualquier momento y sin previo aviso, aún y cuando éstos contengan información personal, en cumplimiento al marco legal y regulatorio vigente en materia.

Los sistemas del ***"IPEBC"*** y toda la información contenida en ellos, (incluyendo archivos, mensajes de correo electrónico y correo de voz, registros de acceso a Internet, etc.) son propiedad de ***"IPEBC"*** y son auditables. La información contenida en los sistemas puede ser revisada, divulgada o interceptada por ***"IPEBC"*** en cualquier momento y sin previo aviso para propósitos de revisión.

IX. VIRUS Y CÓDIGO MALICIOSO

No podrán los servidores públicos obtener archivos de Internet directamente de un servidor o equipo de producción. Los archivos obtenidos de Internet se colocarán en un ambiente aislado o en medios de almacenamiento de sólo lectura para ser revisados por el software antivirus antes de ser colocados en los directorios de trabajo.

No podrán abrir cualquier archivo adjunto de correos electrónicos provenientes de una fuente desconocida, sospechosa o no confiable. Estos correos se borrarán inmediatamente del buzón de correo electrónico.

Todos los archivos adjuntos (incluyendo el contenido de archivos comprimidos) que se reciban vía correo electrónico serán revisados a través de las herramientas que ***"INFORMÁTICA"*** implemente para detectar la presencia de virus y de otros programas destructivos antes de ser abiertos o almacenados en los equipos o sistemas del ***"IPEBC".***

Los servidores públicos revisarán todos los medios de almacenamiento removibles con el software antivirus antes de ser utilizados y de acceder a la información contenida en ellos. Así como, no modificará la configuración, eliminará, desactivará o forzará por alguna otra manera el software antivirus.

Los servidores públicos utilizarán el software antivirus autorizado e instalado por ***"INFORMÁTICA"*** y no podrán instalar cualquier software antivirus diferente a éste.

Los servidores públicos reportarán de forma inmediata todos los incidentes de virus o códigos maliciosos (detectados por el software antivirus instalado).

Los servidores públicos evitarán compartir información de sus equipos con acceso de lectura/escritura a menos que sea absolutamente necesario por requerimientos de trabajo, en tal caso, se revisarán ambos equipos con el software antivirus del ***"IPEBC"*** antes de compartir recursos.

Los servidores públicos borrarán el correo electrónico NO solicitado (basura, cadenas, etc.)

X. HERRAMIENTAS DE HACKEO

Los servidores públicos no realizarán hackeo y actividades relacionadas o similares a éstas. El hackeo incluye, pero no está limitado a las siguientes actividades: acceso ilegal o no autorizado a computadoras, redes, cuentas y otros sitios restringidos, o intento de evadir medidas de seguridad y zonas restringidas en la red.

No se descargarán, instalará o ejecutará herramientas de hackeo, como son sniffers: programas de escaneo sobre diferentes puertos, caballos de Troya, herramientas de interrogación de puertos y vulnerabilidades, entre otros.

XI. PORNOGRAFÍA

Los servidores públicos no introducirán, almacenarán, desplegarán, anunciarán, procesarán o transmitirán material pornográfico en cualquier activo de información del ***"IPEBC".***

Los servidores públicos no accederán en el equipo de cómputo asignado a sitios relacionados o de material pornográfico en Internet durante y fuera el desempeño de sus labores.

XII. RESPALDOS

Los servidores públicos respaldarán periódicamente sus archivos con información clasificada como confidencial o reservada y será responsable de mantener organizada su información en carpetas electrónicas para facilitar el respaldo y recuperación del mismo.

XIII. USO DE MEDIOS REMOVIBLES

Los servidores públicos no utilizarán medios removibles que sean propiedad del personal para descargar, almacenar o transmitir información del ***"IPEBC".***

XIV. DECÁLOGO DE SEGURIDAD

Es responsabilidad de cada usuario el uso de su cuenta y contraseña con la que tiene acceso a los equipos y servicios institucionales.

El servidor público que concluya su empleo, cargo o comisión, deberá garantizar la entrega de los archivos a quien lo sustituya debiendo estar organizados y descritos que faciliten e identifiquen la información de cada documento.

La configuración de los equipos de cómputo institucionales no podrá ser modificada, no descargará programas ajenos a las actividades laborales.

El servicio de Internet es para fines laborales, por lo que no se accederá a sitios o descarga de programas; tales como: juegos, música, vídeos, películas, series, etc.). La información considerada como confidencial se almacenará y transmitirá de forma segura, y cada usuario es responsable de la información que maneja, por lo que es importante realizar respaldos frecuentemente.

El uso de equipo de comunicación de voz (teléfonos fijos, móviles, terminales cifradas, radiocomunicación) es responsabilidad de cada usuario asignado para fines institucionales.

La impresión de documentos se limitará a lo indispensable y es responsabilidad de cada usuario, empleando los esquemas que la Institución proporciona el uso de papelería y reciclaje del mismo.

Se recomienda que todo documento que se considere como inservible sea evaluado para su baja a través del triturado de papel y conforme a lo establecido en la Ley General de Archivos y/o normatividad vigente en la materia.

XV. OBLIGACIONES Y RESPONSABILIDADES DEL DEPARTAMENTO DE INFORMÁTICA

A) SEGURIDAD EN EL DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Todas las aplicaciones desarrolladas para el ***"IPEBC",*** considerarán la seguridad como un aspecto a cubrir por los involucrados en el desarrollo de sistemas en todas sus fases.

Antes de adquirir o desarrollar una aplicación, ***"INFORMÁTICA"*** deberá solicitar las especificaciones y requerimientos mínimos de seguridad claramente que contará la aplicación.

Las diferentes alternativas serán revisadas con los desarrolladores o proveedores para obtener un balance adecuado entre los requerimientos de seguridad y la funcionalidad (facilidad de uso, simplicidad operativa, actualizaciones, costos, entre otros); buscando mantener la confidencialidad, integridad y disponibilidad de la información.

La aceptación de nuevas soluciones tecnológicas, actualizaciones, reconfiguraciones y cambios a nuevas versiones, tendrán una base de criterios de aceptación, tomando en consideración los siguientes puntos:

- Requerimientos de capacidad y desempeño de los equipos.
- Procedimientos para recuperación de errores y planes de contingencia.
- Revisión de procedimientos operativos de rutina.
- Manuales de procedimientos.
- Controles de seguridad.
- Evidencia de que la adquisición, actualización, reconfiguración y cambios de versiones, no afectan la operación normal ni la seguridad de la organización.
- Capacitación en la operación y uso de nuevos sistemas.

B) AMBIENTES DE DESARROLLO, PRUEBA Y PRODUCCIÓN

Las herramientas para el desarrollo de sistemas o aplicaciones serán accesibles solo para ***"INFORMÁTICA"*** autorizados de desarrollo de sistemas.

Las herramientas para el desarrollo de sistemas o aplicaciones que se proponga eliminarse de cualquier equipo de cómputo que no sea utilizado para el desarrollo de sistemas, o bien, justificar su uso mediante la elaboración de un análisis de riesgos, deberá dar aviso a ***"INFORMÁTICA"***.

Los ambientes de desarrollo y pruebas, estarán separados de los de producción, tomando en consideración la parte física y de redes. Al no ser posible esta separación de ambientes por que los sistemas no lo permitan, se llevará a cabo separaciones lógicas de redes, directorios y archivos.

C) ESTÁNDAR DE SEGURIDAD PARA PRUEBA Y LIBERACIÓN DE APLICACIONES

Se realizarán pruebas a los controles de seguridad y de código antes de ser liberada la aplicación por parte de los involucrados en el desarrollo de sistemas.

Se llevarán a cabo pruebas de estrés y pruebas de carga para asegurar que la aplicación cumple con los requisitos de disponibilidad.

Se recomienda que bajo ninguna circunstancia, el código fuente de la aplicación se copie, y mucho menos se modifique, en el ambiente de pruebas.

No se liberará ningún sistema o aplicación sin antes haber realizado las pruebas pertinentes (pruebas de funcionalidad, de estrés, de seguridad, entre otras).

D) ESTÁNDAR DE SEGURIDAD PARA EL MANTENIMIENTO DE SISTEMAS

Se recomienda disponer de procedimientos para el mantenimiento de los sistemas, los cuales especificarán las actividades a realizar con base a la clasificación del sistema.

Las modificaciones a los sistemas serán probadas antes de entrar a los ambientes de producción

Todos los cambios a los sistemas se llevarán a cabo bajo procedimientos establecidos y revisados por las áreas responsables de realizar el desarrollo.

DISPOSICIONES COMPLEMENTARIAS

PRIMERA: El presente "Manual de aplicación de Tecnologías, Comunicación y Seguridad de la Información (MAATIC-SI)" del Instituto de Psiquiatría del Estado de Baja California, el cual tendrá vigencia a partir de su presentación ante Junta de Gobierno y será de aplicación a todos los servidores públicos del IPEBC al día siguiente de su autorización.

SEGUNDA: La Dirección General, Dirección de Administración y Finanzas, Departamento de Informática y el Departamento de Programación y Desarrollo Institucional, serán quienes lleven a cabo el proceso de revisión, elaboración y validación del presente; mismo que establecerá un periodo mínimo de actualización anual para hacerse del conocimiento de los servidores públicos que integran el recurso humano del Instituto de Psiquiatría del Estado de Baja California.

TERCERA: El presente Manual se dará a conocer por medios electrónicos a través de la página: http://www.ipebc.gob.mx/transparencia/manuales.html.

Dado en la ciudad de Mexicali, Baja California al mes de Octubre del 2019.

ATENTAMENTE

Víctor Salvador Rico Hernández
Director General del Instituto de Psiquiatría de Baja California