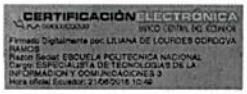
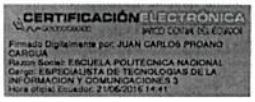
DGIP-CSIRT-005

DIRECTRICES DE SEGURIDAD DE LA RED DE COMPUTADORAS

Elaborado por:	Dirección de Gestión de la Información y Procesos	Ing. Liliana Córdova	
Revisado por:	Dirección de Gestión de la Información y Procesos	Ing. Juan Carlos Proaño	
		Ing. David Quinchaguano	
		Ing. Kléber Serrano	

Aprobado por:	Director DGIP	Ing. Roberto Andrade	

DGIP-CSIRT-005

HOJA DEL ESTADO DEL DOCUMENTO

TITULO DEL DOCUMENTO: **DIRECTRICES DE SEGURIDAD DE LA RED DE COMPUTADORAS** ESTADO DEL DOCUMENTO: Para aprobación			
1. QUIEN EDITA	**2. QUIEN REVISA**	**3. FECHA**	**4. RAZONES DE CAMBIO/QUIEN CAMBIA**
L.Córdova	Ing. Kléber Serrano Ing.David Quinchaguano, Ing. Juan Carlos Proaño	10/jun/2016	Creación documento

1. OBJETO

El objeto del presente documento es establecer los lineamientos de seguridad de todos los activos informáticos de la red de computadoras de la Escuela Politécnica Nacional (EPN), para asegurar que no se divulgue información confidencial, que las tecnologías no estén comprometidas y que las actividades de los laboratorios estén protegidas.

2. ALCANCE

El propósito de esta política es proporcionar una protección adecuada contra las amenazas de malware, virus, gusanos, SPAM y aplicaciones spyware entre otros, en los equipos institucionales, así como también el buen uso de los equipos del laboratorio, y de la red Institucional.

3. RESPONSABILIDAD Y AUTORIDAD

El responsable de elaborar esta directriz es :

Responsable de Seguridad

El responsable de revisar esta directriz son los:

Técnicos de Seguridad

El responsable de aprobar esta directriz es:

Director de la DGIP

La autoridad para hacer cumplir esta directriz es:

Director de la DGIP,
Responsables Seguridad.

Los responsables de cumplir esta directriz son:

4. MARCO LEGAL

Normas de Control Interno para las entidades, organismos del sector público y de las personas jurídicas de derecho privado que dispongan de recursos públicos

Norma 410-10 Seguridad de las Tecnologías de Información

"Implementación y administración de seguridades a nivel de software y hardware, que se realizará con monitoreo de seguridad, pruebas periódicas y acciones correctivas sobre las vulnerabilidades o incidentes de seguridad identificados. "

Instructivo general de seguridad y uso adecuado de las tecnologías de la información y comunicación

Del ámbito de uso de los activos de información:

Art. 2.- Propiedad y uso de los activos de información institucional:

Los activos de información institucionales son: el software, hardware, aplicaciones, sistemas informáticos institucionales y la información generada y/o contenida en éstos, siempre y cuando sean parte del inventario institucional.

Es propiedad de la EPN, toda la información contenida en los activos de información institucionales, excluyendo la información personal de los empleados, trabajadores, personal académico y estudiantes.

Es responsabilidad de los empleados, trabajadores, personal académico y estudiantes, el uso adecuado de la información generada y/o contenida en los activos de información institucionales.

Los activos de información definidos como propiedad de la EPN se utilizarán exclusivamente al servicio de los intereses de la Institución y de sus dependencias.

La DGIP notificará a las autoridades institucionales acerca de acciones sospechosas o ilegales que atenten contra la Constitución, leyes de la República, el Estatuto, normas internas y/o la imagen Institucional; y solicitará autorización al rectorado, para acceder a información confidencial y/o personal que se encuentre almacenada en activos de información de propiedad de la EPN y que esté ligada a dichas acciones.

La EPN, por medio de la DGIP, se encargará de gestionar la protección de los activos de información institucionales, en caso de pérdida, robo, o siniestros accidentales, mediante seguros de bienes de la institución.

La DGIP definirá y difundirá las directrices y/o procedimientos al personal informático de la Institución de las diferentes unidades académicas y administrativas, para que los sistemas de gestión de información siempre se encuentren actualizados, y asegurados.

Art. 3.- Uso de los activos de información contratados:

Es responsabilidad de la DGIP el gestionar los acuerdos con los proveedores de activos de información contratados, con el fin de proveer un adecuado nivel de servicio a los usuarios de la Institución.

Art. 4.- Uso de antivirus:

Es responsabilidad de la DGIP desarrollar y difundir las directrices y procedimientos para el uso del antivirus institucional.

Aquellos computadores institucionales infectados con virus deben ser desconectados de la red hasta que se notifiquen como libres de virus.

Los empleados, trabajadores, personal académico, estudiantes que utilicen computadoras que formen parte de los activos de información de la EPN, deberán utilizar el antivirus institucional programado para correr en intervalos regulares, para proteger la integridad, disponibilidad de la información institucional. La DGIP se reserva el derecho de verificar el uso del antivirus institucional.

Art. 8.- Instalaciones de Software:

Se notificará a la autoridad correspondiente cualquier incidente registrado en los activos de información que no considere los derechos registrados en la Ley de Propiedad Intelectual (LPI).

Art. 10.- Seguridades de redes LAN internas, servidores y laboratorios:

Toda conexión de comunicaciones externa a cualquier dependencia de la EPN en caso de ser requerida, debe ser aprobada por la DGIP.

Es responsabilidad de la DGIP mantener un filtro de todo el tráfico entre el Internet y la Red de Datos Institucional.

Art. 13.- Auditoría y Evaluación de vulnerabilidades:

Los auditores internos y/o externos de la Escuela Politécnica Nacional realizarán inspecciones de seguridad del tráfico sin previo aviso, para capturar evidencia de técnicas maliciosas realizadas sobre los activos de información de la EPN.

Los empleados, trabajadores, personal académico y estudiantes deben facilitar el acceso de usuario y/o sistema para cualquier computadora o dispositivo de comunicación; acceso a la información almacenada en los equipos de la EPN; acceso a las áreas de trabajo como laboratorios, áreas de almacenamiento; y, el acceso para monitorear los registros de tráfico en las redes de la EPN.

La EPN, por medio de la DGIP, se reserva el derecho de utilizar, monitorear e investigar el uso inadecuado de sus activos de información, siempre y cuando se tenga evidencia que establezca sospechas acerca del mal uso de la información generada y/o almacenada en éstos.

La evidencia admisible que la DGIP puede utilizar debe ser aquella que pueda ser capturada de forma accidental y/o como resultado de actividades de monitoreo o auditoría interna.

La DGIP puede iniciar una investigación interna sujeta a directrices y procedimientos, por el mal uso de activos de información, siempre y cuando se establezcan fundamentos basados en la evidencia recolectada, que establezcan que cualquier empleado, trabajador, personal académico, estudiante, haya infringido las normas institucionales, las políticas internas, los reglamentos institucionales, el Estatuto institucional, y/o las leyes de la República del Ecuador.

5. DIRECTRICES

5.1. DIRECTRIZ DE LABORATORIOS

Art. 1- Requisitos de la Configuración General de la Red.

Todo el tráfico entre la Red institucional incluyendo la red del CSIRT-EPN debe pasar por una lista de control de acceso, cortafuego o similar. Los dispositivos de red de laboratorio (incluyendo wireless) no deben realizar un bypass a otras redes institucionales.

Cualquier cambio en las configuraciones originales de la lista de control de acceso, del cortafuego o dispositivo similar, será realizado por la DGIP.

Se prohíbe en la Red Institucional la exploración de puertos de red no autorizada, (la autoexploración de la Red, generar tráfico SPAMming/flooding) y otras actividades similares que afecten negativamente el desempeño de la red. Estas actividades deben estar restringidas dentro del laboratorio del CSIRT, o laboratorios con fines académicos.

El tráfico entre la Red del CSIRT, la Red Institucional, el laboratorio del CSIRT y otras redes de laboratorios, así como el tráfico entre redes de laboratorios separadas, se basa en las necesidades de la institución y será permitido siempre que este tráfico no impacte negativamente en otras redes. Los laboratorios no deben anunciar los servicios de red o poner la información confidencial del laboratorio en riesgo.

La DGIP, el CSIRT-EPN se reservan el derecho de intervenir todos los datos de las redes internas y su administración a cualquier hora, incluye pero no se limita a los paquetes entrantes y salientes y los dispositivos periféricos de la red institucional.

Las contraseñas de administración de todos los dispositivos del laboratorio deben ser diferentes de todas las otras contraseñas de equipos del laboratorio. La contraseña debe registrarse conforme con la directriz de contraseñas institucional. La contraseña sólo se proporcionará a aquéllos usuarios autorizados para administrar la red.

Todas las peticiones de conexión externa del laboratorio deben ser autorizadas por la DGIP.

Art. 2- Responsabilidades de Uso del Laboratorio.

Por cada laboratorio institucional, se debe asignar el personal encargado del laboratorio un punto de contacto y uno de reserva. Los responsables del laboratorio deben mantener la información de los computadores actualizada y el equipo de gestión de la red. El contacto con los encargados del laboratorio o personal de reserva, se debe mantener disponible en caso de contingencia, si no las acciones serán tomadas sin su participación.

Los administradores del laboratorio son responsables de la seguridad del laboratorio y del impacto del mismo en las actividades de la red. Los administradores de laboratorio son responsables de la adhesión a esta política y los procesos asociados.

Donde las políticas y procedimientos son indefinidos, los administradores del laboratorio deben actuar en forma proactiva, para salvaguardar la información.

Los administradores de laboratorio son responsables de la conformidad del laboratorio con todas las políticas de seguridad. Las siguientes son particularmente importantes: La directriz de contraseñas para conectar dispositivos a una red de computadoras, directriz de seguridad inalámbrica, directriz de anti-virus, de cifrado, el Instructivo de Seguridad, entre otros.

Los administradores de laboratorio son responsables de controlar el acceso al laboratorio. Esto incluye supervisar la lista de acceso continuamente para asegurar que aquéllos que ya no requieran el acceso sean eliminados.

La DGIP debe mantener un dispositivo que controle el acceso entre la Red Institucional y los equipos del laboratorio.

La DGIP se reserva el derecho de interrumpir las conexiones del laboratorio que impactan negativamente o son un riesgo de seguridad a la Institución.

La DGIP debe registrar todas las direcciones IP del laboratorio que son ruteadas dentro de la Institución en la base de datos correspondiente junto con la información actual del contacto para ese laboratorio.

Cualquier dependencia que quiera agregar una conexión externa debe proporcionar un diagrama y la documentación requerida a la DGIP con la

Art.2- Consolas Esclavas

En caso de que el anti-virus institucional necesite de la instalación de consolas esclavas (Laboratorios), los administradores de las consolas deben cumplir con las siguientes condiciones:

- Cada consola utilizará exclusivamente el número de licencias asignadas en la instalación, si se desea un número mayor de licencias, el administrador de la consola esclava debe comunicarse con el personal técnico de la DGIP.
- En caso de formatear el servidor donde está instalada la consola, debe comunicarse con el personal técnico de la DGIP y respaldar la configuración de la consola a su cargo.
- Es obligación de los administradores:
  - Revisar que exista una conexión activa entre la consola esclava y la consola máster.
  - Revisar que se realicen los respaldos de la configuración de la consola esclava.
  - Revisar las actualizaciones de la consola esclava.
  - Revisar que exista una conexión activa entre la consola esclava y las estaciones de trabajo registradas a la misma.

Art. 3- Anti-Spyware

Todos los servidores deberán tener una aplicación anti-spyware instalada, que ofrezca protección en tiempo real al sistema objeto del ataque si se cumple una o más de las siguientes condiciones:

- Cualquier sistema en el que usuarios no-técnicos o no-administrativos tienen acceso remoto a la red y cualquier acceso de salida permitido al Internet.
- Cualquier sistema en el que usuarios no técnicos o no administrativos tienen la capacidad de instalar software.

Art. 4- Antispam

Todos los servidores de correo deberán tener una aplicación antispam instalada, que ofrezca protección en tiempo real.

justificación correspondiente. La DGIP revisará la seguridad antes de aprobarla.

Las cuentas de usuario individuales de cualquier dispositivo de laboratorio deben eliminarse cuando el usuario deje de pertenecer a la institución. Las contraseñas de cuentas grupales deben ser cambiadas al menos una vez en forma trimestral.

5.2. DIRECTRIZ DE PROTECCIÒN DE SERVIDORES CONTRA MALWARE

Art. 1- Antivirus

Todos los servidores que forman parte de los activos institucionales deben tener instalado el antivirus institucional que ofrezca escaneo en tiempo real para la protección de archivos y aplicaciones que se ejecutan en el sistema destino.

Si el antivirus escogido no es el institucional el personal a cargo del equipo asume la responsabilidad de la solución del problema de virus; en este caso la DGIP se reserva el derecho de retirar al equipo de la red para evitar el contagio con el resto de usuarios.

En caso de que un servidor sea dado de baja, es obligación del administrador del servidor informar al Personal de la DGIP para que se pueda reutilizar la licencia.

Si el rendimiento del servidor es precario a raíz de la instalación del antivirus, es obligación del administrador del servidor informar al personal de la DGIP, de manera que se realicen configuraciones alternativas o se pueda recurrir a versiones especiales del antivirus que permitan un mejor rendimiento.

Las configuraciones sobre actualizaciones y análisis del servidor se coordinarán en el momento de la instalación, sin embargo es obligación del administrador del servidor revisar que el equipo esté actualizado correctamente y que se realicen los análisis necesarios.

Si desde una cuenta del dominio de la EPN, se envían mensajes no solicitados, en el momento que se detecten dichos envíos no autorizados la cuenta será dada de baja inmediatamente sin mediar aviso previo.

No se deberá enviar ningún mail a una dirección para ser "removido". El CSIRT-EPN no solicita confirmaciones masivas para remover direcciones de cadenas de correo electrónico.

Art. 5- Excepciones

Las excepciones a las reglas establecidas las registra el CSIRT-EPN.

5.3 DIRECTRIZ DE SEGURIDAD DE SERVIDORES

Art. 1- Configuraciones generales

Todos los servidores internos deben ser manejados por un grupo operacional responsable de la administración del sistema.

Las guías de configuración de servidores aprobadas deben ser respetadas y aplicadas por cada grupo operacional responsable, basado en las políticas institucionales. Los grupos operacionales deben supervisar el cumplimiento de la configuración y de ser necesario solicitar la aprobación de las excepciones a la política para ser adaptada a su ambiente, esto será revisado y aprobado por el director de la DGIP.

Los servidores deben ser registrados dentro del sistema de gestión de la DGIP. Como mínimo, se requiere la siguiente información que lo identifique:

- Identificar el responsable o contacto y la localización del servidor y un contacto de reserva.
- El Hardware y la versión del Sistema operativo.
- Funciones Principales y usos, de ser aplicable. Identificar si el servidor es crítico.

La Información en el sistema de gestión del servidor debe mantenerse actualizada.

Los Cambios de Configuración en los servidores de producción deben seguir la Directriz de cambios apropiados.

La configuración del Sistema operativo debe ser conforme a las directrices aprobadas.

Los servicios y aplicaciones que no sean usados deben ser deshabilitados.

El acceso a servicios debe ser registrado y/o protegido por métodos de control de acceso como encapsulamiento, de ser posible.

Los parches de seguridad más recientes deben ser instalados sobre el sistema tan pronto como sean liberados, la única excepción se da cuando el uso inmediato interfiera con la funcionalidad de los servicios institucionales, el servicio deberá entrar a fase de monitoreo de seguridad permanente hasta que el sistema sea parchado.

Las relaciones de confianza entre sistemas son un riesgo de seguridad y su empleo debería ser evitado. No usar una relación de confianza cuando exista algún otro método de comunicación.

No utilizar cuentas privilegiadas como root cuando una cuenta no privilegiada pueda ser usada.

Si una metodología para la conexión de canal seguro está disponible, deberá ser aplicada, y el acceso privilegiado debe ser realizado sobre canales seguros, (por ejemplo cifrado conexiones de red que usan SSH o IPSEC).

Los servidores físicamente deben ser ubicados en un ambiente cuyo acceso sea controlado.

Los servidores antes de su puesta en producción deben registrar un análisis de vulnerabilidades y su remediación.

Los servidores expresamente tienen prohibido funcionar dentro de ambientes que no estén controlados.

El tiempo de análisis de vulnerabilidades de servidores críticos luego del aseguramiento del servidor no debe ser mayor a 1 mes.

El tiempo de análisis de vulnerabilidades de servidores no críticos luego del aseguramiento del servidor no debe ser mayor a 6 meses.

Art. 2- Monitoreo de seguridad

Todos los acontecimientos de seguridad relacionados con sistemas críticos o sensibles deben ser registrados y los rastros de auditorías guardados conforme las directrices institucionales.

Los eventos relacionados con la seguridad serán reportados al CSIRT-EPN, que informará de incidentes de activos críticos al Comité de Seguridad de la Información. Se tomarán las medidas correctivas como sean necesarias. Cualquier evento relacionado con la seguridad incluye, pero no se limita, a:

- Ataques y Exploración de puertos.
- Evidencias de accesos no autorizados con cuentas privilegiadas.
- Uso indebido o robo de información crítica
- Fraude o phishing.
- Modificación no autorizada de: un sitio, una página web, datos.
- Robo o pérdida de un recurso informático.
- Ataque o infección por código malicioso.
- Uso prohibido de un recurso informático o de red.
- Acceso o intento de acceso no autorizado a un sistema informático.
- Ocurrencias anómalas que no son relacionadas con usos específicos sobre el servidor.

Art. 3- Auditorias

- Las auditorias serán realizadas regularmente por personal de seguridad de la DGIP dentro de la Escuela Politécnica Nacional.
- Las auditorias serán manejadas por un grupo interno de auditoria designado por la DGIP, conforme a la política de auditoria. La DGIP presentará las conclusiones al personal de apoyo apropiado para la nueva mediación o la justificación.
- Se hará el esfuerzo necesario para impedir que las auditorias causen fallas operacionales o interrupciones.

5.4 DIRECTRIZ DE BASES DE DATOS DE CREDENCIALES

Art. 1- Resguardo de credenciales de autenticación

Para mantener la seguridad de las bases de datos internas de la EPN, el acceso a programas solo debe concederse a través de la autenticación por medio de credenciales, las mismas que no deben estar en texto plano dentro del cuerpo principal del programa, así como también no deberán ser almacenadas en lugares que puedan ser accedidos a través de un servidor Web.

Art. 2- Almacenamiento de Nombres de Usuario y Contraseñas en la base de datos

- Los nombres de usuario y las contraseñas de la base de datos deben ser guardados en un archivo independiente del cuerpo del código del programa. Este archivo no debe ser legible, debe seguir los lineamientos de cifrado.
- Las credenciales de la base de datos pueden residir en el servidor de base de datos, siempre y cuando se encuentren cifradas y firmadas (hash).
- Las credenciales de la base de datos pueden ser almacenadas como parte de un servidor de autenticación como un servidor de LDAP o Directorio Activo, usado para la autenticación de usuarios.
- El paso de autenticación no debe permitir el acceso a la base de datos basándose solamente en la autenticación de un usuario de manera remota. Contraseñas o frases de paso usadas para el acceso a la base de datos deberían ser incluidas.

Art. 3- Recuperación de Nombres y Contraseñas

- El medio dentro del cual se guardan las credenciales de la base de datos debe estar separado físicamente de los directorios del código fuente.
- Los lenguajes que ejecutan código fuente y validan las credenciales, no deben residir en el mismo árbol de directorios en el que reside el cuerpo del código ejecutado.

Art. 4- Acceso a la base de datos de Nombres y Contraseñas

- Los grupos de desarrollo deben tener un proceso interno para asegurar que las contraseñas de la base de datos sean controladas y cambiadas. Este proceso debe incluir un método para restringir el conocimiento de contraseñas de la base de datos ante personas no autorizadas.
- El periodo de cambio de contraseñas del acceso a la base de datos debe regirse a la directriz de contraseñas Institucional.

Art. 5- Monitoreo de seguridad

Todos los eventos de seguridad relacionados con bases de datos críticos o sensibles deben ser registrados y los rastros de auditorías guardados conforme las directrices institucionales.

El análisis de vulnerabilidades de las bases de datos de sistemas críticos se ejecutará cada 3 meses y cada seis meses de los sistemas considerados no críticos.

Los eventos relacionados con la seguridad serán reportados al CSIRT-EPN, que informará de incidentes de activos críticos al Comité de Seguridad de la Información. Se tomarán las medidas correctivas como sean necesarias. Cualquier acontecimiento relacionado con la Seguridad incluye, pero no se limita, a:

- Accesos no autorizados con cuentas privilegiadas.
- Modificación no autorizada de datos.
- Divulgación no autorizada de información personal.
- Ataque o infección por código malicioso.
- Eventos anómalos que no son relacionados con usos específicos sobre la Base de Datos.

5.5 DIRECTRIZ DE SEGURIDAD DE SISTEMAS INFORMÁTICOS

Art. 1- Requerimientos de autenticación y gestión de usuarios

Los sistemas informáticos deben autenticarse contra el Directorio Activo institucional.

Los sistemas informáticos deben contar con módulos para gestionar la creación, eliminación, desactivación de usuarios y la gestión de privilegios asignados.

Art. 2- Requerimientos de seguridad en la etapa de análisis

Incorporar los requerimientos para evaluar cumplimiento con las normativas de la Contraloría, SRI, Leyes de la República, Leyes de la Educación Superior, Derecho de Propiedad Intelectual, instructivos y normatividad institucional entre otras.

Identificar el tipo de información que se transmitirá y procesará en especial la información pública y la confidencial.

Incorporar registros de cambios, información de fecha y hora del cambio atada al usuario que la registra, la aplicación debe proporcionar pistas para Auditoría.

Art. 3- Requerimientos de seguridad en la etapa de diseño

En esta etapa se definirá el diseño de autorización, la definición de roles, permisos y privilegios de la aplicación.

Se debe realizar el diseño de la forma de autenticación de los usuarios así como los mecanismos para evitar posibles ataques.

Se debe realizar el diseño de los mensajes de advertencia y error con la finalidad de evitar que estos brinden demasiada información, la misma que puede ser aprovechada por atacantes.

Art. 4- Requerimientos de seguridad en la etapa de codificación

En esta etapa se realizará la identificación de los tipos de vulnerabilidades.

Vulnerabilidades clásicas: errores de manejo de sesiones, desbordamiento, denegación de servicios. Se debe realizar un análisis de vulnerabilidades al finalizar la etapa de codificación.

Vulnerabilidades funcionales: estas vulnerabilidades se refieren a la funcionalidad de la aplicación con respecto a los requerimientos de la aplicación, el sistema debe realizar las funciones para las que fue diseñado.

Art. 5- Requerimientos de seguridad en la etapa de pruebas

Evaluar los controles definidos en las etapas de análisis, diseño y codificación.

Evaluar la seguridad de la aplicación en escenarios que incluya:

- Evaluación de seguridad con valores fuera de rango.

- Evaluación se seguridad con valores incorrectos.
- Evaluación de seguridad con acciones fuera de orden.

Los datos de pruebas no deben ser los mismos datos de producción.

Elaborar procedimientos formales para la validación de los datos de entrada, procesamiento y salida de los sistemas, elaborar un informe de resultados de validación y entregarlos a la Dirección de la DGIP.

Art. 6- Requerimientos de seguridad en la etapa de producción

Las modificaciones en ambientes de producción deberán regirse por la directriz de control de cambios.

Garantizar que la no continuidad de las actividades sea mínima durante la implementación de cambios.

Se debe realizar copias de respaldo según la directriz institucional.

Los programadores o analistas de desarrollo y mantenimiento de aplicaciones no pueden acceder a los ambientes de producción.

Se debe mantener un control de versiones para todas las actualizaciones de software.

Asignar un técnico para administrar y custodiar los programas fuentes, el cual es responsable de:

Proveer los programas fuentes solicitados para su modificación.

Llevar un registro formal y actualizado de todos los programas fuentes en uso, en el que se debe incluir mínimo la siguiente información: nombre del programa, programador, Analista, Responsable que autorizó la actualización, versión, fecha de última modificación y estado del programa.

Administrar las distintas versiones de una aplicación.

Asegurar que un mismo programa fuente no sea modificado simultáneamente por más de un desarrollador.

Verificar que el Analista Responsable que autoriza la solicitud de un programa fuente sea el designado para la aplicación, caso contrario se deberá rechazar el pedido

El técnico responsable de administrar los programas fuentes no puede modificar el código de los programas fuente bajo su custodia.

Todo programa ejecutable en producción debe tener un único programa fuente asociado a este.

Control de transacciones

La actualización de los permisos de acceso a los datos de producción debe ser autorizada por el propietario de información y otorgada por un periodo limitado.

Los programas compiladores no deben ser instalados en los sistemas en producción, todo el código debe ser compilado antes de ser transferido al ambiente de producción.

Todos los reportes de auditoría de transacciones sensibles o de alto valor deben ser revisados por el responsable del servicio y por el propietario del servicio en intervalos regulares apropiados. Los reportes deben incluir la identidad del usuario, la fecha y la hora del evento.

El acceso para ejecución de transacciones sensibles debe ser controlado mediante una adecuada segregación de tareas. Por ejemplo los usuarios que tengan permisos para registrar pagos no deben poder verificar o aprobar su propio trabajo. Para estos casos se debe contar con la directriz de segregación de funciones.

Los funcionarios deben tener acceso únicamente al conjunto de transacciones en línea requeridas para ejecutar las tareas

asignadas. Este conjunto de transacciones debe estar claramente definido para prevenir ocurrencia de fraude o cambio de información. Los controles de acceso deben ser revisados periódicamente por el responsable del servicio con notificación al propietario de la información y al oficial de seguridad.

Para las transacciones en la nube es recomendable que se transfiera el riesgo al proveedor en nube; sin embargo, no todos los riesgos pueden ser transferidos. Por lo tanto en última instancia, se puede subcontratar la responsabilidad, pero el responsable del servicio, está en la obligación de solicitar una rendición de cuentas.

Art. 7- Externalización del Desarrollo de Software

Toda aplicación desarrollada por terceros tendrá un responsable designado por el director de la DGIP.

Se establecerán acuerdos de Licencias, propiedad de código y derechos conferidos (Derechos de propiedad intelectual).

Si se intercambia información que es confidencial, se deberá generar un documento/acuerdo de confidencialidad entre la EPN y el proveedor de servicios.

Se establecerá procedimientos de auditorías, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software establecidos, entre otros.

Art. 8- Monitoreo de seguridad

Los requisitos de seguridad que debe cumplir el software deben ser revisados por el Oficial de Seguridad.

Se tomarán las medidas correctivas como sean necesarias. Cualquier evento relacionado con la Seguridad incluye, pero no se limita, a:

- Ataques y Exploración de puertos.
- Evidencias de accesos no autorizados con cuentas privilegiadas.
- Uso indebido o robo de información crítica.
- Fraude o Phishing.
- Modificación no autorizada de: un sitio, una página web, datos.
- Robo o pérdida de un recurso informático.
- Ataque o infección por código malicioso.
- Uso prohibido de un recurso informático o de red.
- Acceso o intento de acceso no autorizado a un sistema informático.
- Eventos anómalos que no son relacionados con funcionalidades del sistema.

Art. 9- Auditorias

- Las auditorias serán realizadas regularmente y manejadas por un grupo interno de auditoria designado por la DGIP, conforme a la política de auditoria. La DGIP filtrará conclusiones no relacionadas con un grupo específico operacional y luego presentará las conclusiones al personal de apoyo apropiado para la nueva mediación o la justificación.
- Se hará el esfuerzo necesario para impedir que las auditorías causen fallas operacionales o interrupciones.

DEL AMBITO DE LAS SANCIONES

La DGIP debe notificar el incumplimiento de lo establecido en la presente política, a la autoridad correspondiente para los fines legales respectivos.

DISPOSICIONES GENERALES

PRIMERA.- En todo lo no previsto en este instructivo, de acuerdo a la naturaleza de control y administración de bienes y normativa que la regula, se aplicarán según corresponda las leyes y reglamentos vigentes y demás instrumentos jurídicos que tengan relación con los mismos.

SEGUNDA.- De la ejecución del presente instructivo, que entrará en vigencia a partir de su suscripción, encárguese al Director de la Dirección de Gestión de la Información y Procesos.

DEROGATORIA

Se derogan las normas de igual o menor jerarquía emitidas con anterioridad, que se opongan al presente Instructivo.

Dado en la ciudad de Quito, D.M. a los 21 días del mes de junio del 2016.