REGLAMENTO DE ASEGURAMIENTO Y GESTIÓN DE LA INFORMACIÓN

Versión 1-2018

ESPAM

ESCUELA SUPERIOR POLITÉCNICA
AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ

Contenido

I. INTRODUCCIÓN 7

II. ALCANCE 7

III. MARCO LEGAL 7

IV. OBJETIVO 8

V. POLÍTICAS DE SEGURIDAD INFORMÁTICA 8

5.1. POLÍTICAS DE SEGURIDAD FÍSICA 8

5.1.2. Protección física 9

5.1.3. Instalación de Equipos de Cómputo 10

5.1.4. Sustracción o Pérdidas de Equipos de Cómputo 10

5.1.5. Respaldo de Información 11

5.1.6. Recurso de los Usuarios 11

5.2. POLÍTICAS DE SEGURIDAD LÓGICA 12

5.2.1. Control de acceso lógico y uso de la red 12

5.2.2. Uso de los servicios de red 16

5.2.3. Control de acceso lógico a los sistemas informáticos institucionales 18

5.2.4. Administración de los Servidores 19

5.2.5. Acceso a la información de la ESPAM MFL. 20

5.2.6. Uso del antivirus institucional 20

6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 21

6.1. Compromiso de la máxima autoridad de la institución con la seguridad de la información 21

6.2. Coordinación de la Gestión de la Seguridad de la Información 21

6.2.1. Funciones del responsable de Seguridad del Área de Tecnologías de la Información: 22

7. GESTIÓN DE LOS ACTIVOS 23

7.1. Inventariar los activos de soporte de Hardware 23

7.2. Inventariar los activos de soporte de Software 24

7.3. Inventariar los activos de soporte de redes 24

7.4. Inventariar los activos referentes a la estructura organizacional 24

7.5. Responsable de los activos 25

7.6. Uso aceptable de los activos 25

7.7. Reglamentar el acceso y uso de la Internet y sus aplicaciones/servicios 26

8. SEGURIDAD DE LOS RECURSOS HUMANOS 26

8.1. Términos y condiciones laborales 26

8.2. Responsabilidades de la dirección a cargo del funcionario 27

8.3. Retiro de los privilegios de acceso 27

9. SEGURIDAD FÍSICA Y DEL ENTORNO 27

9.1. Controles de acceso físico 27

9.2. Ubicación y protección de los equipos 27

9.3. Seguridad del cableado 28

9.4. Mantenimiento de los equipos 28

9.5. Seguridad de los equipos fuera de las instalaciones 28

9.6. Seguridad en la reutilización o eliminación de los equipos 29

9.7. Retiro de activos de la propiedad 29

10. GESTIÓN DE COMUNICACIONES Y OPERACIONES 29

10.1. Gestión del Cambio 29

10.2. Separación de las instancias de Desarrollo, Pruebas, Capacitación y Producción. 30

10.3. Monitoreo y revisión de los servicios, por terceros. 30

10.4. Gestión de los cambios en los servicios ofrecidos por terceros. 30

DIRECCIÓN DE SECRETARÍA GENERAL

10.5. Aceptación del Sistema. 31
10.6. Controles contra código malicioso 31
10.7. Controles contra códigos móviles 31
10.8. Respaldo de la información. 32
10.9. Controles de las redes 32
10.10. Seguridad de los servicios de la red. 32
10.11. Gestión de los medios removibles. 33
10.12. Eliminación de los medios 33
10.13. Procedimientos para el manejo de la información 33
10.14. Seguridad de la documentación del sistema. 33
10.15. Mensajería electrónica 34
10.16. Transacciones en línea. 34
10.17. Información disponible al público. 34
10.18. Registros de auditorías. 34
10.19. Monitoreo de uso del sistema 35
10.20. Protección del registro de la información. 35
11. CONTROL DE ACCESO 35
11.1. Política de control de acceso 35
11.2. Registro de usuarios 35
11.3. Gestión de contraseñas para usuarios 36
11.4. Revisión de los derechos de acceso de los usuarios 36
11.5. Uso de contraseñas 36
11.6. Equipo de usuario desatendido 36
11.7. Autenticación de usuarios para conexiones externas 37
11.8. Protección de los puertos de configuración y diagnóstico remoto 37
11.9. Separación en las redes 37

DIRECCIÓN DE

11.10. Control del enrutamiento en la red 38

11.11. Limitación del tiempo de conexión 38

11.12. Control de acceso a las aplicaciones y a la información 38

11.13. Computación y comunicaciones móviles 38

11.14. Trabajo remoto 39

12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN 40

12.1. Análisis y especificaciones de los requerimientos de seguridad 40

12.2. Validación de datos de entrada 40

12.3. Control de procesamiento interno 40

12.4. Integridad del mensaje 41

12.5. Política sobre el uso de controles criptográficos. 41

12.6. Se debe garantizar: 41

12.7. Gestión de claves 42

12.8. Control del software operativo 42

12.9. Protección de los datos de prueba del sistema 43

12.10. Control de acceso al código fuente de los programas 43

12.11. Procedimiento de control de cambios 44

12.12. Revisión técnica de las aplicaciones después de los cambios en el sistema operativo 44

12.13. Restricción del cambio de paquetes de software 45

12.14. Fuga de información 45

12.15. Desarrollo de software contratado externamente 45

12.16. Control de las vulnerabilidades técnicas 46

13. GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN 46

13.1. Control de las vulnerabilidades técnicas 46

SUPERIOR
AGROPECUARIA DE MANABÍ MANUEL FELIX LOPEZ
DIRECCIÓN DE
SECRETARÍA GENERAL

13.2. Reporte sobre las debilidades en la seguridad 47

13.3. Responsabilidades y procedimientos 47

13.4. Recolección de evidencias 48

14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO 48

14.1. Continuidad del negocio y evaluación de riesgos 49

15. CUMPLIMIENTO 49

15.1. Identificación de la legislación aplicable 49

15.2. Derechos de Propiedad Intelectual 50

15.3. Protección de registros en cada entidad 51

15.4. Protección de los datos y privacidad de la información personal 51

15.5. Reglamentación de controles criptográficos 51

15.6. Verificación del cumplimiento técnico 52

DIRECCIÓN DE

I. INTRODUCCIÓN

La Unidad de Tecnología determina la información como un activo de alta importancia para la institución de educación superior que permite el desarrollo continuo de las actividades que se desarrollan diariamente con la finalidad de dar cumplimiento de los objetivo institucionales, lo cual genera la necesidad de implementar mecanismos que permitan proteger la confidencialidad, integridad y disponibilidad durante el ciclo de vida de la información. El presente Reglamento se establecen las políticas que integran el Sistema de Gestión de Seguridad de la Información SGSI, las cuales deben ser aplicados y adoptadas por los funcionarios, contratistas, personal en comisión administrativa, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con la ESPAM MFL; las mismas que se encuentran enfocadas a dar cumplimiento de la normatividad legal Ecuatoriana vigente.

II. ALCANCE

El reglamento de aseguramiento y gestión de la información cubre los aspectos administrativos y de control que se deben cumplir por los directivos, funcionarios y terceras personas que laboren o tengan relación con la ESPAM MFL, para el adecuado cumplimiento de sus funciones y conseguir un alto nivel de protección de la información y los datos, las características de calidad y seguridad de la información aportando en la toma de decisiones, medidas preventivas y correctivas, siendo un punto clave para lograr los objetivos institucionales. Los usuarios tienen la obligación de dar cumplimiento a las políticas emitidas y aprobadas por la máxima autoridad de la Institución de educación superior ESPAM MFL.

III. MARCO LEGAL

En base a las normas de control interno de la contraloría general del estado. Acuerdo de la Contraloría General del Estado, 39 Registro Oficial Suplemento 87 de 14-dic.-2009 Ultima modificación: 16-dic.-2014 Estado: Vigente CONTRALORÍA GENERAL DEL ESTADO NORMAS DE CONTROL INTERNO PARA LAS ENTIDADES, ORGANISMOS DEL SECTOR PÚBLICO Y PERSONAS JURÍDICAS DE DERECHO PRIVADO QUE DISPONGAN DE RECURSOS PÚBLICOS Oficio No. 22784 SGEN Quito, 2 de diciembre del 2009.

El Art. 410 TECNOLOGÍA DE LA INFORMACIÓN 410-01 Organización informática Las entidades y organismos del sector público deben estar acopladas en un marco de trabajo para procesos de tecnología de información que aseguren la transparencia y el control, así como el involucramiento de la alta dirección, por lo que las actividades y procesos de tecnología de información de la organización deben estar bajo la responsabilidad de una unidad que se encargue de regular y estandarizar los temas tecnológicos a nivel institucional.

La Unidad de Tecnología de Información, estará posicionada dentro de la estructura organizacional de la entidad en un nivel que le permita efectuar las actividades de asesoría y apoyo a la alta dirección y unidades usuarias; así como

ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ
DIRECCIÓN DE SECRETARÍA GENERAL

participar en la toma de decisiones de la organización y generar cambios de mejora tecnológica. Además debe garantizar su independencia respecto de las áreas usuarias y asegurar la cobertura de servicios a todas las unidades de la entidad u organismo.

Las entidades u organismos del sector público, establecerán una estructura organizacional de tecnología de información que refleje las necesidades institucionales, la cual debe ser revisada de forma periódica para ajustar las estrategias internas que permitan satisfacer los objetivos planteados y soporten los avances tecnológicos. Bajo este esquema se dispondrá como mínimo de áreas que cubran proyectos tecnológicos, infraestructura tecnológica y soporte interno y externo de ser el caso, considerando el tamaño de la entidad y de la unidad de tecnología.

410-02 Segregación de funciones. Las funciones y responsabilidades del personal de tecnología de información y de los usuarios de los sistemas de información serán claramente definidas y formalmente comunicadas para permitir que los roles y responsabilidades asignados se ejerzan con suficiente autoridad y respaldo.

La descripción documentada y aprobada de los puestos de trabajo que conforman la Unidad de Tecnología de Información, contemplará los deberes y responsabilidades, así como las habilidades y experiencia necesarias en cada posición, a base de las cuales se realizará la evaluación del desempeño. Dicha descripción considerará procedimientos que eliminen la dependencia de personal clave.

IV. OBJETIVO

Desarrollar políticas de seguridad de la información significa que permita planear, organizar, dirigir y controlar las actividades para mantener y garantizar la integridad física de los recursos informáticos de la ESPAM MFL.

V. POLÍTICAS DE SEGURIDAD INFORMÁTICA

8.1 POLÍTICAS DE SEGURIDAD FÍSICA

5.1.1. Acceso Físico.

1. La institución deberá destinar un área apropiada para alojar los equipos de telecomunicaciones y servidores.
2. Los sistemas de comunicaciones y servidores deberán estar protegidos con una infraestructura adecuada que cumplan las normas y estándares actuales, con el fin de evitar que los usuarios tengan libre acceso físico al área.

3. Se restringirá el acceso a las áreas que contengan información valiosa para la ESPAM MFL y las salas donde se alojan los equipos de telecomunicaciones y servidores.
4. El acceso de terceras personas deberá ser identificado, controlado y registrado en la bitácora, detallando el nombre, empresa o departamento, motivo, fecha/hora de ingreso y salida de las áreas restringidas, por el personal de la Unidad de Tecnología.
5. El Coordinador de la Unidad de Tecnología es el que autoriza el ingreso de personas internas o externas de la ESPAM MFL, a las áreas restringidas y acompañadas por personal de la Unidad de Tecnología, mediante aprobación de la máxima Autoridad.
6. El personal de la Unidad de Tecnología, personal administrativo de otros departamentos y terceras personas, deberán portar su credencial institucional, al momento de ingresar a las áreas restringidas.
7. El departamento de Talento Humano informará a la Unidad de Tecnología, las personas que no tienen relación laboral con la universidad, para proceder a revocar los permisos de acceso.
8. Se establecerán horarios de visitas a las áreas físicas restringidas (cuarto de telecomunicaciones, sala de servidores)
9. Se debe definir y autorizar el personal que tendrá acceso a las salas de telecomunicaciones y servidores, para mover, cambiar o extraer los equipos de estos sitios, mediante identificaciones y formularios de entrada/salida, notificando al departamento correspondiente y al personal de seguridad de la ESPAM MFL que se encuentra en la entrada y salida del campus.

5.1.2. Protección física

1. Las puertas de acceso a la sala de servidores y al cuarto de telecomunicaciones (Data Center), deben ser de vidrio transparente, con el fin de facilitar el control de los equipos.
2. La Unidad de Tecnología con todas sus áreas deberán contar con un plano actualizado de las instalaciones eléctricas y de comunicación.
3. La sala de servidores y telecomunicaciones (Data Center), se deben definir como áreas restringidas, las mismas que deben contar con un sistema de control de acceso del personal del Unidad de Tecnología, como, por ejemplo: sistema biométrico, tarjetas magnéticas, otros.
4. La sala de servidores y telecomunicaciones (Data Center), debe recibir limpieza por lo menos una vez a la semana, para evitar la acumulación de polvo, el mismo que puede provocar ineficiencia o daños a equipos servidores y de telecomunicaciones.
5. La sala de servidores, telecomunicaciones y el cableado estructurado, deben estar diseñados bajo las normas y estándares actuales que ayuden a preservar la vida útil de los equipos que se alojan en los mismos.
6. Se deberán realizar mantenimientos cada tres meses a los sistemas de protección y eléctricos de las áreas restringidas.

7. Se deberán realizar inventarios y controles de los equipos servidores y de telecomunicaciones que encuentren distribuidos en los diferentes edificios de la ESPAM MFL.
8. Se deberá revisar y comprobar el voltaje de la toma eléctrica donde se requiera conectar un equipo de cómputo.
9. El personal autorizado de acceder a las salas de servidores y telecomunicaciones (Data Center), deben controlar las condiciones ambientales como temperatura y humedad, para verificar que no afecte al funcionamiento del equipamiento.
10. Los equipos servidores y de telecomunicaciones (Data Center), deberán recibir mantenimiento físico por lo menos dos veces al año.

5.1.3. Instalación de Equipos de Cómputo

La instalación de los equipos de cómputo deberá seguir las siguientes acciones:

1. Los equipos de cómputo para uso interno se instalarán en lugares adecuados, lejos de polvo, luz solar y tráfico de personas.
2. Las instalaciones eléctricas y de comunicaciones, deben estar fijas o protegidas del paso de personas o materiales, y libres de cualquier interferencia eléctrica o magnética.
3. Las instalaciones se apegarán estrictamente a los requerimientos de los equipos de cómputo, cuidando las especificaciones del cableado y de los circuitos de protección necesarios.
4. No se permitirán instalaciones improvisadas o sobrecargadas.
5. La supervisión y control de las instalaciones se llevará a cabo en los plazos y mediante los mecanismos que establezca la Unidad de Tecnología.

5.1.4. Sustracción o Pérdidas de Equipos de Cómputo

1. La Unidad de Tecnología llevará un inventario físico para control interno del departamento, que se lo realizará junto con el Plan de Mantenimiento Preventivo – Correctivo.
2. La Unidad de Tecnología al asignar equipos de cómputo lo realizará mediante "Acta de Entrega/Recepción", que quedará como evidencia óptica de la aceptación de responsabilidad sobre el equipo por parte del usuario.
3. El equipo de cómputo quedará bajo el custodio del área o persona que lo usa, el mismo que será responsable de proteger el bien.
4. El Cuarto de Telecomunicaciones y la sala de Servidores (Data Center), así como las áreas que cuenten con equipos de misión crítica deberán contar con un sistema de vigilancia de control de acceso mediante cámaras o equipo biométrico, que ayude a obtener evidencia de accesos físicos a las instalaciones e identificar los responsables de la desaparición de los equipos.
5. El Usuario es el responsable por la pérdida o destrucción del equipo de cómputo, por mal uso de este, salvo el caso que sea por causas naturales,

así mismo, será responsable terceras personas que tengan acceso al equipo que realicen actividades de mantenimiento o reparación.

6. El Usuario es el responsable del equipo de cómputo y sus accesorios, deberá notificar por escrito al Coordinador Inmediato y a la máxima autoridad de la ESPAM MFL, sobre el extravío, robo o desaparición de este, actuando de acuerdo al Art. 77 del Reglamento General para la Administración, Utilización, Manejo y Control de los bienes y existencias del sector público.
7. El equipo de cómputo asignado al Usuario, en el caso de extraviarse o sufrir daños por el uso, será de responsabilidad del departamento o del usuario administrativo/docente; es decir, quien esté a cargo del mismo deberá restituir o reemplazar el equipo por otro, de acuerdo a lo mencionado en el Art.77 del Reglamento General para la Administración, Utilización, Manejo y Control de los bienes y existencias del sector público.

5.1.5. Respaldo de Información

1. Los usuarios tienen la responsabilidad de almacenar documentos digitalizados y la información que generen, en los equipos lógicos designados en el disco duro del equipo de cómputo (Disco Local D:) o en medios de almacenamiento externo, evitando que los datos puedan ser dañados, sustraídos o eliminados.
2. La Unidad de Tecnología como responsable de la seguridad de la información, deberá establecer los mecanismos de respaldos tanto de sistemas, base de datos y configuraciones en almacenamientos en la nube con la seguridad requerida.
3. Se deben realizar respaldos periódicamente de la información importante y relevante, contenida en la base de datos que generan los sistemas de información institucional.
4. Para realizar los respaldos de la información se utilizarán repositorios locales o remotos, discos duros externos, CD´s o DVD´s, y almacenados en un lugar seguro distante de las áreas de servidores y telecomunicaciones.
5. Los usuarios deberán proteger y cuidar los medios o unidades de almacenamiento (CD´s o DVD´s, Tarjetas de Memoria, Pen drives, otros) que estén bajo su responsabilidad y que contengan información confidencial e importante.
6. Los usuarios podrán solicitar asesoría o capacitación a la Unidad de Tecnología, en el procedimiento para respaldar la información.

5.1.6. Recurso de los Usuarios

1. Los usuarios deberán cuidar, respetar y hacer buen uso de los recursos informáticos de la ESPAM MFL, de acuerdo con las políticas que en este documento se mencionan.

2. La información de trabajo generada en los recursos informáticos de la institución deberá ser almacenada en el espacio lógico asignado a los usuarios.
3. Es responsabilidad del usuario interno, mantener seguras las contraseñas de sus cuentas de usuario de correo electrónico o de sistemas informáticos, y no compartirlas con terceras personas.
4. Se debe mantener conectado el equipo de cómputo a un UPS o regulador de voltaje, para evitar daños en el mismo, en casos de variaciones de voltaje o cortes de energía eléctrica.
5. Los usuarios no deberán conectar los equipos de cómputo en toma eléctrica que no sean destinadas para estos, ni desconectarlos de la toma regularizada.
6. Todo usuario al finalizar su día de trabajo debe apagar los equipos de cómputo asignados. No se permite dejar equipos de cómputo encendidos de un día para otro. Esta regla no aplica a equipos que estén realizando procesos nocturnos, procesos de prueba o diagnósticos cuyo conocimiento lo tenga la Unidad de Tecnología.
7. Los medios de almacenamiento externo (Pen Drives, Flash Memory, Disco Duro, DVD, CD externo) provistos por la ESPAM MFL, son exclusivamente para trabajos dentro de la institución, y no podrá salir dichos dispositivos, salvo autorización escrita de la máxima autoridad.
8. No se debe instalar o manipular software, imágenes, videos o sonidos no autorizados, que puedan afectar la seguridad e integridad de la información, de los equipos de cómputo o la red de datos.

8.2 POLÍTICAS DE SEGURIDAD LÓGICA

5.1.7. Control de acceso lógico y uso de la red

1. La Unidad de Tecnología controlará el acceso a la red y servidores de la ESPAM MFL, de acuerdo a las necesidades del usuario.
2. Los usuarios tendrán acceso a la red de datos mediante la autenticación de usuario y contraseña provistos por la Unidad de Tecnología.
3. La infraestructura de la red de datos institucional de la ESPAM MFL, solo será utilizada para actividades de investigación, académica, técnica y administrativa.
4. El departamento de Talento Humano o Coordinador de cada unidad solicitará a la Unidad de Tecnología la creación de credenciales de red (usuarios y contraseña), para el nuevo personal administrativo o docente.
5. El personal administrativo y docente no deberá revelar la clave de su cuenta de usuario de red a terceras personas, esto incluye a cualquier miembro de su familia, compañero de trabajo o persona externa que se encuentre realizando actividades propias dentro de la institución.
6. Los usuarios de la red no deberán interrumpir las comunicaciones en la red de datos, o cambiar la configuración de la red utilizando cualquier tipo de software que monitoree, analice, o perturbe las actividades normales de la misma.

7. Los usuarios tienen prohibido acceder a datos en algún servidor a través de la red de datos para los cuales no estén autorizados.
8. Los usuarios no deben ingresar con una cuenta que no esté asignada para acceder a la red, a menos que estas actividades estén dentro del alcance de sus actividades normales de trabajo.
9. Los usuarios no deberán evadir la autenticación de usuario o cualquier seguridad de algún equipo, red o cuenta de usuario propiedad de la ESPAM MFL.
10. Los usuarios tienen prohibido manipular la infraestructura de red y telecomunicaciones, salvo el caso que sea realizado por personal autorizado de La Unidad de Tecnología.
11. Está prohibido que el personal administrativo o docente revise los recursos compartidos en la red, en busca de información no autorizada, para alterarla, copiarla, modificarla, robarla o destruirla.
12. La Unidad de Tecnología empleará dispositivos de red para el monitoreo, bloqueo, enrutamiento o filtrado de tráfico, evitando el acceso a información confidencial que pueda ser enviada desde la red interna hacia el exterior.
13. Los usuarios tienen prohibido utilizar cualquier equipo de cómputo propiedad de la ESPAM MFL conectado a la red de datos, para la distribución de cualquier tipo de software maligno o material no permitido que vaya en contra de la moral y las buenas costumbres.
14. Se prohíbe interferir con las actividades normales de cualquier usuario o negarle el acceso a algún servicio de red que él necesite para poder realizar sus labores normales.
15. Está prohibido utilizar algún programa, script, o comando para enviar mensajes de cualquier índole, con la intención de interferir o deshabilitar el equipo de algún usuario, sea esto localmente, a través de internet o alguna conexión remota.
16. La Unidad de Tecnología o administrador de redes no serán responsables por el contenido de los datos que circulen en la red, el usuario emisor será el único responsable por la información que envíe o intercambie con los demás usuarios.

SERVICIOS DE LA UNIDAD DE TECNOLOGÍA - ESPAM MFL

#	SERVICIO	DESCRIPCION	USUARIO
1	FACTURACION	Permite la contabilización en línea de las facturas que recepta la institución de educación superior	Departamento de Contabilidad de la ESPAM MFL
2	TALENTO HUMANO	Sistema web para llevar el control de los empleados y docentes de la ESPAM MFL	Departamento de Talento Humano ESPAM MFL

3	LABORATORIOS		
4	CONVENIOS		
5	SISTEMA INTEGRADO DE BIBLIOTECA KOHA	Sistema bibliotecario para dar soporte a los estudiantes de la ESPAM MFL y a nivel mundial	Comunidad politécnica
6	PORTAL Y SITIOS WEB	Página web institucional para dar a conocer los diferentes acontecimientos que se efectúan dentro de la institución de educación superior.	Comunidad politécnica
7	REPOSITORIO DIGITAL INSTITUCIONAL DSPACE	Brinda un servicio de publicación y difusión de información académica de datos abiertos, servicio disponible para todas las unidades, direcciones, departamentos de la ESPAM MFL.	Comunidad politécnica
8	SISTEMA DE GESTIÓN ACADEMICA	Sistema que permite a directivos, docentes y estudiantes estar al día de las diferentes actividades curriculares que se realizan académicamente	Comunidad politécnica
9	SISTEMA VIRTUAL DE APRENDIZAJE	Sistema de enseñanza-aprendizaje virtual, donde los docentes pueden crear sus clases y matricular los estudiantes para así brindar mayor disponibilidad de aprendizaje a los estudiantes de la ESPAM MFL	Comunidad politécnica
10	SISTEMA DEL CENTRO DE APLICACIONES INFORMATICAS CAAI	Sistema que permite la matriculación y seguimientos a los estudiantes que realizan los cursos de computación de la ESPAM MFL	Comunidad politécnica

11	SISTEMA DE LA REVISTA DE INVESTIGACION	Sistema Open Journal System, que permite publicar los diferentes artículos científico escritos por docentes de la ESPAM como de otras instituciones del país y del mundo	Comunidad politécnica
12	SISTEMA DE CORREO ELECTRONICO INSTITUCIONAL	El sistema de correo electrónico permite una comunicación bidireccional entre docentes, personal administrativo y estudiantes ya que pueden acceder desde cualquier parte del mundo a los recursos y aplicaciones sincronizadas con el correo electrónico institucional	Comunidad politécnica
13	SISTEMA DE GESTIÓN DOCUMENTAL QUIPUX	QUIPUX es un servicio web que el departamento de tecnología de la ESPAM MFL ha implementado para la administración de documentos.	Comunidad politécnica
14	SISTEMA DE POSGRADO	Sistema que permite mantener informados de las diferentes actividades como nuevas maestría que oferta la ESPAM MFL	Comunidad politécnica
15	SISTEMA DE ATO PORCINO	Sistema que permite el control y seguimiento del área porcicultor	Comunidad politécnica
16	SISTEMA DE ATO BOVINO	Sistema que permite el control y seguimiento del área de bovinos	Comunidad politécnica
17	CENTRAL TELEFONICA	Este sistema permite que fluyan las comunicaciones en la carrera de computación de la ESPAM MFL	Comunidad politécnica, carrera de COMPUTACION

5.1.8. Uso de los servicios de red

5.1.8.1. Uso del Internet

1. El servicio de internet solo será utilizado por personal administrativo, docentes y estudiantes para fines laborales, consultas e investigaciones, accediendo a sitios de carácter académico y científico.
2. Se solicitará mediante oficio a la Unidad de Tecnología las credenciales de la red para tener acceso al servicio de internet.
3. Los usuarios no deben ingresar a páginas con contenido no permitido, de entretenimiento u otros que no estén relacionados con las actividades laborales de la ESPAM MFL.
4. Los usuarios no deberán descargar videos, imágenes, música o programas gratuitos sin licencias que oferten en la web.
5. Los usuarios tienen prohibido el uso de chat o acceder a páginas de redes sociales como Facebook, linkedin, instagram, twitter, entre otros excepto personal considerado por la máxima autoridad.

5.1.8.2. Uso de la red Inalámbrica (WIFI)

1. La Unidad de Tecnología proveerá del servicio de red inalámbrica, a los docentes, áreas administrativas y a la comunidad estudiantil de la ESPAM MFL.
2. Los usuarios que cuenten con un dispositivo móvil, sea este un celular, Tablet o laptop, podrán acceder a la red inalámbrica, para realizar trabajos académicos como investigación y consultas.
3. La Unidad de Tecnología para evitar que intrusos puedan acceder a la red inalámbrica, ha creado el portal cautivo para la autenticación de acceso a los estudiantes, personal administrativo y docentes de la ESPAM MFL.
4. La Unidad de Tecnología proporcionará el usuario y clave de acceso al portal cautivo a los estudiantes, personal administrativo y docentes de la ESPAM MFL.
5. Los usuarios deberán ingresar a la red inalámbrica a través del portal cautivo de la ESPAM MFL, ingresando el usuario y clave entregada por la Unidad de Tecnología.
6. La Unidad de Tecnología realizará el monitoreo de la red inalámbrica mediante análisis de tráfico, detectando usos indebidos del servicio y así mantener en buen funcionamiento la red.
7. La Unidad de Tecnología bloqueará páginas web de redes sociales, entretenimiento u otras, para evitar el consumo excesivo de ancho de banda del internet.
8. Los usuarios no deberán proporcionar las credenciales (usuario y clave) del portal cautivo a personas ajenas a la ESPAM MFL.
9. Los usuarios tienen prohibido hacer uso del servicio de red inalámbrica para:
   a. Acosar, amenazar o intimidar a otras personas.

b. Interferir con asunto de la ESPAM MFL.
c. Realizar acciones de rastreo, difusión de virus o acceder a recursos informáticos de la ESPAM MFL.
d. Descargar programas, juegos, música, videos o imágenes inapropiadas.
e. Enviar información personal como números de tarjetas, claves etc.
f. Transferir información que viole el derecho de autor, material pornográfico, mensajes amenazantes u obscenos.

10. La Unidad de Tecnología tendrá el deber de dar mantenimiento a los equipos y puntos de acceso a la red inalámbrica.
11. La Unidad de Tecnología no será responsable de la información que se transmita por la red inalámbrica, que realizan los estudiantes o docentes.
12. Los usuarios deberán tener cuidado de ingresar a sitios web no seguros o descargar información que pueda contener virus informáticos.

5.1.8.3. Uso del correo electrónico institucional

1. El correo electrónico institucional asignado al personal administrativo y docentes, será para uso obligatorio y exclusivo del envío y recepción de mensajes relacionados con las actividades laborales y académicas.
2. Los usuarios que requieran de la creación del correo electrónico la solicitarán a la Unidad de Tecnología con la debida autorización del Coordinador del departamento solicitante, mediante formato de solicitud, oficio o correo electrónico.
3. La Unidad de Tecnología se encargará de depurar los contactos que se encuentran registrados en el correo electrónico institucional, de tal forma que solo estén registrados los usuarios que actualmente laboran en la ESPAM MFL, respaldados y autorizados por el departamento de Talento Humano.
4. Las cuentas de correo electrónico provistas a los usuarios por la ESPAM MFL, no se deberán utilizar para formar parte de grupos, como: chat, música, tarjetas virtuales, discusión, entre otros, además de listas de suscripción en sitios web con contenido sexual o pornográfico.
5. Los usuarios no deberán abrir mensajes o descargar archivos de dudosa procedencia, para tal caso deberán comunicar a la Unidad de Tecnología para su revisión.
6. Los usuarios deben tener extrema precaución cuando revisen archivos adjuntos recibidos en mensajes de correo electrónico que provengan de remitentes conocidos o desconocidos, pues estos deben contener algún tipo de virus. Se recomienda que esos mensajes sean eliminados (Esta política aplica a cuentas de correo electrónico propias de la ESPAM MFL o cuentas de correo electrónico en internet que sean revisadas desde la red de la Universidad).
7. Los usuarios no deberán crear o reenviar a través de correo electrónico cadenas o cualquier otro tipo de esquemas de pirámides (Ej. Mensajes de ayuda, colaboración, otros.).
8. Los usuarios de correo electrónico son responsables de mantener segura la clave y la información contenida en el mismo. La Unidad de Tecnología

no se hace responsable por perdida de información del correo institucional.

5.1.8.4. Uso de impresoras en Red

1. Las impresoras conectadas en red, solo se utilizarán para trabajos relacionados con las actividades laborales del personal administrativo y docente.
2. Los usuarios no deberán utilizar las impresoras en red, para imprimir trabajos, imágenes o documentos personales.
3. Los usuarios deberán solicitar a la Unidad de Tecnología la configuración de la impresora en red a un nuevo equipo de cómputo, para poder acceder a este servicio.

5.1.8.5. Uso de sistemas informáticos institucionales

1. Los usuarios autorizados podrán tener acceso a los sistemas informáticos institucionales, para realizar sus labores diarias.
2. Los usuarios no podrán cambiar datos del sistema informático como notas, valores, entre otros sin la previa autorización y por escrito.
3. Los usuarios no podrán hacer mal uso de la información descargada de los sistemas informáticos.

5.1.9. Control de acceso lógico a los sistemas informáticos institucionales

1. Se definirá las funciones y restricciones que hace uso de los sistemas informáticos institucionales, es decir, cada usuario solo podrá acceder a las funciones del sistema que le corresponden.
2. Los Coordinadores departamentales, solicitarán a la Unidad de Tecnología la creación o eliminación de credenciales (usuario y contraseña) para el acceso a los sistemas informáticos por parte del personal administrativo o docente, así como el personal entrante o saliente de la institución.
3. La Unidad de Tecnología se encargará de depurar las credenciales de autenticación de acceso a los sistemas informáticos, de acuerdo al personal que se encuentra laborando actualmente basado en los registros proporcionados por el Departamento de Talento Humano, el mismo que informará al área de Tecnología a través de oficio en el momento que ingrese o se retire de la institución.
4. Los usuarios no deberán compartir sus credenciales de autenticación para el ingreso a los sistemas informáticos institucionales, a terceras personas no autorizadas.
5. El Coordinador de la Unidad de Tecnología, designará a la persona autorizada y responsable de la Administración de las Bases de Datos, en este caso el analista/programador.

6. El administrador de la Base de Datos (BD), es la persona autorizada y responsable de acceder a la información contenida en las bases para realizar las siguientes actividades:
   a. Respaldo de las BD´s de los Sistemas Informáticos Institucionales.
   b. Resolver problemas que los usuarios no pueden solucionar mediante la plataforma.
   c. Monitorear y diagnosticar los Sistemas Informáticos Institucionales.
7. El administrador de la BD´s no podrán eliminar información de los sistemas, salvo el caso que este dañada o pongan en riesgo el funcionamiento del sistema. Así mismo no podrá sustraer, divulgar, destruir o suprimir información contenida en las Bases de Datos, en caso de cometer alguno de estos delitos, será sancionado según las leyes ecuatorianas.

5.1.10. Administración de los Servidores

1. La Unidad de Tecnología a través del administrador de Servidores tendrá la responsabilidad de controlar, verificar y comprobar la instalación, configuración e implementación de la seguridad de los servidores en la red de datos de la ESPAM MFL.
2. El Coordinador de la Unidad de Tecnología, designará a la persona autorizada y responsable de la Administración de los servidores de la Institución.
3. Se deberá notificar a la Unidad de Tecnología mediante oficio la instalación y/o configuración de cualquier equipo servidor que deseen conectar a la red de la Universidad, para ser asesorados y brindarles los permisos requeridos por el administrador de servidores.
4. Los equipos servidores que serán destinados para uso y bajo custodio de la Unidad de Tecnología, solo será responsabilidad del Administrador de Servidores.
5. El administrador de servidores al momento de realizar configuraciones, debe aplicar las normas y estándares establecidos, para la correcta operación de los mismos, así como la restricción de directorios, permisos y programas que serán usados por los usuarios.
6. Los servidores que brindan servicios de internet, correo electrónico, impresión, entre otros; deberán:
   a. Funcionar las 24 horas del día y durante todo el año.
   b. Recibir mantenimiento preventivo físico y lógico dos veces al año.
   c. Deben ser monitoreados por el administrador de servidores.
   d. La información contenida en los servidores deberá ser respaldada según el cronograma provisto por la Unidad de Tecnología.
7. Los equipos servidores deberán ser ubicados dentro de un área que cumpla todas las normas y estándares actuales, para mantenerlos seguros.

5.1.11. Acceso a la información de la ESPAM MFL.

1. Los usuarios que tienen acceso a información generada por cualquier actividad de investigación realizada por la Universidad tendrán prohibido efectuar copias de la misma y realizar ventas fraudulentas en formato digital.
2. Los usuarios tienen prohibido sustraer y divulgar información confidencial de la ESPAM MFL a terceras personas ajenas a la Institución.
3. Los usuarios tienen prohibido falsificar información en nombre de la ESPAM MFL.
4. La información institucional contenida en los servidores (Repositorio de datos), deberá ser asegurada por parte del administrador de servidores, mediante cifrado, niveles de control de acceso y contraseñas de usuario.
5. Para tener acceso a información confidencial contenida en los servidores (Repositorio de datos), deberá existir una autorización de uso por parte de la máxima autoridad de la Universidad y del Coordinador del Unidad de Tecnología.
6. El usuario es responsable de evitar la fuga de información confidencial de la ESPAM MFL, contenida en los equipos de cómputo que estén bajo su administración.
7. Es obligación de los usuarios proteger cualquier información que consideren sensible o vulnerable mediante derechos de acceso si el programa donde lo desarrolló lo permite (permisos lectura, escritura, contraseñas).

5.1.12. Uso del antivirus institucional

1. Todo equipo que se conecte a la red de datos o algún sistema de información de la ESPAM MFL debe estar ejecutando un antivirus actualizado.
2. Todos los equipos de cómputo pertenecientes a la Institución deberán tener instalado el antivirus con licencia, adquirido por la Universidad.
3. Los usuarios al detectar algún virus informático no deberán tomar acciones para eliminar el virus, debe contactarse con La Unidad de Tecnología para que el técnico delegado proceda a dar solución al incidente.
4. Los usuarios antes de utilizar medios de almacenamiento extraíble, debe ejecutar el antivirus en estos medios.
5. Los técnicos de la Unidad de Tecnología son los únicos autorizados para instalar y actualizar el software antivirus, solo en los equipos de cómputo pertenecientes a la Universidad.
6. Los usuarios tienen prohibido instalar o descargar software, programas o aplicativos que no cuenten con licencia o provengan de algún sitio web desconocido, lo cual podría ocasionar la infección del equipo de cómputo por virus informáticos.
7. La Unidad de Tecnología es el encargado y responsable de la administración de la plataforma del software antivirus.

8. La Unidad de Tecnología se encargará de realizar revisiones periódicas a los equipos y sistemas, con el fin de mantener protegidos los recursos informáticos y evitar futuros inconvenientes, realizando lo siguiente:
   a. Actualización automática de las bases de virus y análisis al equipo de cómputo que se encuentran conectados a la red de datos institucional.
   b. Actualización manual de las bases y análisis al equipo que no están conectados a la red.
9. Los usuarios tienen prohibido desinstalar el antivirus del equipo que se encuentre bajo su responsabilidad, ya que podría ocasionar la vulnerabilidad del mismo.

6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

6.1. Compromiso de la máxima autoridad de la institución con la seguridad de la información

1. Realizar el seguimiento de la puesta en marcha de las normas de este documento.
2. Disponer la difusión, capacitación y sensibilización del contenido de este documento.
3. Conformar oficialmente el Comité de Gestión de la Seguridad de la Información de la institución (CSI) y designar a los integrantes.

6.2. Coordinación de la Gestión de la Seguridad de la Información

1. La coordinación estará a cargo del Comité de Gestión de Seguridad de la Información el cual tendrá las siguientes funciones
2. Definir y mantener la política y normas institucionales particulares en materia de seguridad de la información y GESTIÓNar la aprobación y puesta en vigencia por parte de la máxima autoridad de la institución, así como el cumplimiento por parte de los funcionarios de la institución.
3. Monitorear cambios significativos de los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
4. Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.
5. Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área.
6. Acordar y aprobar metodologías y procesos específicos a la seguridad de la información "Gestión de la seguridad de la información" GSI.
7. Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios, en base al GSI.

8. Promover la difusión y apoyo a la seguridad de la información dentro de la institución.
9. Coordinar el proceso de gestión de la continuidad de la operación de los servicios y sistemas de información de la institución frente a incidentes de seguridad imprevistos.
10. Designar a los custodios o responsables de la información de las diferentes áreas de la entidad, que deberá ser formalizada en un documento físico o electrónico.
11. GESTIÓNar la provisión permanente de recursos económicos, tecnológicos y humanos para la gestión de la seguridad de la información.
12. Velar por la aplicación de la familia de normas técnicas ecuatorianas INEN ISO/IEC 27000 en la institución según el ámbito de cada norma.
13. Designar formalmente a un funcionario como Oficial de Seguridad de la Información quien actuará como coordinador. El Oficial de Seguridad no pertenecerá al área de Tecnologías de la Información y reportará a la máxima autoridad de la institución.
14. Designar formalmente al responsable de seguridad del área de Tecnologías de la Información en coordinación con el director o responsable del área de Tecnologías de la Información de la Institución.

6.2.1. Funciones del responsable de Seguridad del Área de Tecnologías de la Información:

1. Controlar la existencia de documentación física o electrónica actualizada relacionada con los procedimientos de comunicaciones, operaciones y sistemas.
2. Evaluar el posible impacto operativo a nivel de seguridad de los cambios previstos a sistemas y equipamiento y verificar su correcta implementación, asignando responsabilidades.
3. Administrar los medios técnicos necesarios para permitir la segregación de los ambientes de procesamiento.
4. Monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad para soportar potenciales amenazas a la seguridad de la información que procesan
5. Controlar la obtención de copias de resguardo de información, así como la prueba periódica de su restauración.
6. Asegurar el registro de las actividades realizadas por el personal operativo de seguridad de la información, para su posterior revisión.
7. Desarrollar y verificar el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas.
8. Implementar los controles de seguridad definidos (ej.: evitar software malicioso, accesos no autorizados, etc.)
9. Definir e implementar procedimientos para la administración de medios informáticos de almacenamiento (ej.: cintas, discos, etc.) e informes impresos, y verificar la eliminación o destrucción segura de los mismos, cuando proceda.

10. Gestionar los incidentes de seguridad de la información de acuerdo a los procedimientos establecidos.
11. Otras que por naturaleza de las actividades de gestión de la seguridad de la información deban ser realizadas.

7. GESTIÓN DE LOS ACTIVOS

Inventariar los activos primarios, en formatos físicos y/o electrónicos

1. Los manuales e instructivos de sistemas informáticos: instalación, guía de usuario, operación, administración, mantenimiento, entre otros.
2. De la operación de los aplicativos informáticos de los servicios informáticos: datos y meta-datos asociados, archivos de configuración, código fuente, respaldos, versiones, etc.
3. Del desarrollo de aplicativos de los servicios informáticos: actas de levantamiento de requerimientos, documento de análisis de requerimientos, modelos entidad - relación, diseño de componentes, casos de uso, diagramas de flujo y estado, casos de prueba, etc.
4. Del soporte de aplicativos de los servicios informáticos: tickets de soporte, reportes físicos y electrónicos, evaluaciones y encuestas, libros de trabajo para capacitación, etc.

7.1 Inventariar los activos de soporte de Hardware

1. Equipos móviles: teléfono inteligente (smartphone), teléfono celular, tableta, computador portátil, asistente digital personal (PDA), etc.
2. Equipos fijos: servidor de torre, servidor de cuchilla, servidor de rack, computador de escritorio, computadoras portátiles, etc.
3. Periféricos de entrada: teclado, ratón, micrófono, escáner plano, escáner de mano, cámara digital, cámara web, lápiz óptico, pantalla de toque, etc.
4. Periféricos de salida: monitor, proyector, audífonos, parlantes, impresora láser, impresora de inyección de tinta, impresora matricial, impresora térmica, plotter, máquina de fax, etc.
5. Periféricos y dispositivos de almacenamiento: sistema de almacenamiento (NAS, SAN), librería de cintas, cintas magnéticas, disco duro portátil, disco flexible, grabador de discos (CD, DVD, Blu-ray), CD, DVD, Blu-ray, memoria USB, etc.
6. Periféricos de comunicaciones: tarjeta USB para redes inalámbricas (Wi-Fi, Bluetooth, GPRS, HSDPA), tarjeta PCMCIA para redes inalámbricas (Wi-Fi, Bluetooth, GPRS, HSDPA), tarjeta USB para redes alámbricas/inalámbricas de datos y de telefonía, etc.
7. Tableros: de transferencia (bypass) de la unidad ininterrumpible de energía (UPS), de salidas de energía eléctrica, de transferencia automática de energía, etc.
8. Sistemas: de control de accesos, de aire acondicionado, automático de extinción de incendios, de circuito cerrado de televisión, etc.

7.2 Inventariar los activos de soporte de Software

1. Sistemas operativos.
2. Software de servicio, mantenimiento o administración de: gabinetes de servidores de cuchilla, servidores (estantería/rack, torre, virtuales), sistema de redes de datos, sistemas de almacenamiento (NAS, SAN), telefonía, sistemas (de UPS, grupo electrógeno, de aire acondicionado, automático de extinción de incendios, de circuito cerrado de televisión), etc.
3. Paquetes de software o software base de: suite de ofimática, navegador de Internet, cliente de correo electrónico, mensajería instantánea, edición de imágenes, vídeo conferencia, servidor (proxy, de archivos, de correo electrónico, de impresiones, de mensajería instantánea, de aplicaciones, de base de datos), etc.
4. Aplicativos informáticos del negocio.

7.3 Inventariar los activos de soporte de redes

1. Cables de comunicaciones (interfaces: RJ-45 o RJ-11, SC, ST o MT-RJ, interfaz V35, RS232, USB, SCSI, LPT), panel de conexión (patch panel), tomas o puntos de red, racks (cerrado o abierto, de piso o pared), etc.
2. Switchs (de centros de datos, de acceso, de borde, de gabinete de servidores, access-ppoint, transceiver, equipo terminal de datos, etc.).
3. Ruteador (router), cortafuego (firewall), controlador de red inalámbrica, etc.
4. Sistema de detección/prevención de intrusos (IDS/IPS), firewall de aplicaciones web, balanceadoras de carga, switch de contenido, etc.

7.4 Inventariar los activos referentes a la estructura organizacional

1. Estructura organizacional del área de las TIC, con los cargos y nombres del personal: administrador (de servidores, de redes de datos, de respaldos de la información, de sistemas de almacenamiento, de bases de datos, de seguridades, de aplicaciones del negocio, de recursos informáticos, etc.), líder de proyecto, personal de capacitación, personal de mesa de ayuda, personal de aseguramiento de calidad, programadores (PHP, Java, etc.).
2. Inventario referente a los sitios y edificaciones de la institución: planos arquitectónicos, estructurales, eléctricos, sanitarios, de datos, etc.
3. Dirección física, dirección de correo electrónico, teléfonos y contactos de todo el personal de la institución.
4. De los servicios esenciales: número de líneas telefónicas fijas y celulares, proveedor de servicios de Internet y transmisión de datos, proveedor del suministro de energía eléctrica, proveedor del suministro de agua potable, etc.

5. Los activos deberán ser actualizados ante cualquier modificación de la información registrada y revisados con una periodicidad no mayor a seis meses.

7.5 Responsable de los activos

1. Elaborar el inventario de los activos a su cargo y mantenerlo actualizado.
2. Clasificar, documentar y mantener actualizada la información y los activos, y definir los permisos de acceso a la información.
3. Consolidar los inventarios de los activos a cargo del responsable del Activo, por área o unidad organizativa.

7.6 Uso aceptable de los activos

1. Reglamentar el uso de correo electrónico institucional.
2. Este servicio debe utilizarse exclusivamente para las tareas propias de las funciones que se desarrollan en la institución y no debe utilizarse para ningún otro fin.
3. Cada persona es responsable tanto del contenido del mensaje enviado como de cualquier otra información que adjunte.
4. Todos los mensajes deben poder ser monitoreados y conservados permanentemente por parte de la institución.
5. Toda cuenta de correo electrónico debe estar asociada a una única cuenta de usuario.
6. La conservación de los mensajes se efectuará en carpetas personales, para archivar la información de acceso exclusivo del usuario y que no debe compartirse con otros usuarios. Debe definirse un límite de espacio máximo.
7. Todo sistema debe contar con las facilidades automáticas que notifiquen al usuario cuando un mensaje enviado por él no es recibido correctamente por el destinatario, describiendo detalladamente el motivo del error.
8. Deben utilizarse programas que monitoreen el accionar de virus informáticos tanto en mensajes como en archivos adjuntos, antes de su ejecución.
9. Todo usuario es responsable por la destrucción de los mensajes con origen desconocido, y asume la responsabilidad por las consecuencias que pueda ocasionar la ejecución de los archivos adjuntos. En estos casos, no deben contestar dichos mensajes y deben enviar una copia al Oficial de Seguridad de la Información para que efectúe el seguimiento y la investigación necesaria.
10. Todo usuario es responsable de la cantidad y tamaño de mensajes que envíe. Debe controlarse el envío no autorizado de correos masivos.

7.7 Reglamentar el acceso y uso de la Internet y sus aplicaciones/servicios

1. Este servicio debe utilizarse exclusivamente para las tareas propias de la función desarrollada en la institución, y no debe utilizarse para ningún otro fin.
2. Cada usuario es responsable de la información y contenidos a los que accede y de aquella que copia para conservación en los equipos de la institución.
3. Debe limitarse a los usuarios el acceso a portales, aplicaciones o servicios de la Internet y la Web que pudieren perjudicar los intereses y la reputación de la institución. Específicamente, se debe bloquear el acceso por medio de dispositivos fijos y/o móviles a aquellos portales, aplicaciones o servicios de la Internet y la Web sobre pornografía, racismo, violencia, delincuencia o de contenidos ofensivos y contrarios a los intereses, entre otros, y valores de la institución o que impacten negativamente en la productividad y trabajo de la institución (ej., mensajería instantánea-chats, redes sociales, video, otros) y particularmente a los que atenten a la ética y moral.
4. Todos los accesos deben poder ser sujetos de monitoreo y conservación permanente por parte de la institución.
5. La institución podrá en cualquier momento bloquear o limitar el acceso y uso de la Internet a los funcionarios o a terceros que accedan tanto por medio alámbrico como inalámbrico.
6. Se debe bloquear y prohibir el acceso y uso de servicios de correo electrónico de libre uso tales como: Gmail, Hotmail, Yahoo, Facebook, entre otros.

8. SEGURIDAD DE LOS RECURSOS HUMANOS

8.1 Términos y condiciones laborales

1. Realizar la firma de un acuerdo de confidencialidad o no-divulgación, antes de que los empleados, contratistas y usuarios de terceras partes, tengan acceso a la información. Dicho acuerdo debe establecer los parámetros tanto de vigencia del acuerdo, información confidencial referida, formas de acceso, responsabilidades y funciones.
2. Socializar los derechos y responsabilidades legales de los empleados, los contratistas y cualquier otro usuario sobre la protección de datos; dejando constancia de lo actuado a través de hojas de registro, informes o similares, que evidencie la realización de la misma.
3. Responsabilizar al personal sobre el manejo y creación de la información resultante durante el contrato laboral con la institución.

8.2. Responsabilidades de la dirección a cargo del funcionario

1. Explicar y definir las funciones y las responsabilidades respecto a la seguridad de la información, antes de otorgar el acceso a la información, contraseñas o sistemas de información sensibles.
2. Lograr la concienciación sobre la seguridad de la información correspondiente a sus funciones y responsabilidades dentro de la institución.
3. Acordar los términos y las condiciones laborales, las cuales incluyen la política de la seguridad de la información de la institución y los métodos apropiados de trabajo.
4. Verificar el cumplimiento de las funciones y responsabilidades respecto a la seguridad de la información mediante la utilización de reportes e informes.

8.3. Retiro de los privilegios de acceso

1. Retirar los privilegios de acceso a los activos de información y a los servicios de procesamiento de información (ej., sistema de directorio, correo electrónico, accesos físicos, aplicaciones de software, etc.,) inmediatamente luego de que se comunique formalmente al Oficial de Seguridad de la Información formalmente la terminación de la relación laboral por parte del área correspondiente

9. SEGURIDAD FÍSICA Y DEL ENTORNO

9.1. Controles de acceso físico

1. Supervisar la permanencia de los visitantes en las áreas restringidas y registrar la hora y fecha de su ingreso y salida.
2. Controlar y limitar el acceso, exclusivamente a personal autorizado, a la información clasificada y a las instalaciones de procesamiento de información. Se debe utilizar controles de autenticación como tarjetas de control de acceso más el número de identificación personal.

9.2. Ubicación y protección de los equipos

1. Ubicar los equipos de modo que se elimine el acceso innecesario a las áreas de trabajo restringidas.
2. Aislar los servicios de procesamiento de información con datos sensibles y elementos que requieran protección especial, para reducir el riesgo de visualización de la información de personas no autorizadas.

3. Establecer directrices para no comer, beber y fumar en las cercanías de las áreas de procesamiento de información.
4. Monitorear las condiciones ambientales de temperatura y humedad.
5. Tener protección contra descargas eléctricas en todas las edificaciones de la institución y disponer de filtros protectores en el suministro de energía y en las líneas de comunicación.

9.3. Seguridad del cableado

1. Proteger el cableado de la red contra la interceptación o daño.
2. Separar los cables de energía de los cables de comunicaciones.
3. Identificar y rotular los cables de acuerdo a normas locales o internacionales para evitar errores en el manejo.
4. Disponer de documentación, diseños/planos y la distribución de conexiones de: datos alámbricas/inalámbricas (locales y remotas), voz, eléctricas polarizadas, etc.
5. Controlar el acceso a los módulos de cableado de conexión (patch panel) y cuartos de cableado.

9.4. Mantenimiento de los equipos

- ✓ Brindar mantenimientos periódicos a los equipos y dispositivos, de acuerdo a las especificaciones y recomendaciones del proveedor.
- ✓ Realizar el mantenimiento de los equipos únicamente con personal calificado y autorizado.
- ✓ Conservar los registros de los mantenimientos preventivos, correctivos y fallas relevantes o sospechosas.
- ✓ Establecer controles apropiados para realizar mantenimientos programados y emergentes.
- ✓ GESTIÓNar mantenimientos planificados con hora de inicio, fin, impacto y responsables y poner previamente en conocimiento de administradores y usuarios finales.

9.5. Seguridad de los equipos fuera de las instalaciones

1. Custodiar los equipos y medios que se encuentren fuera de las instalaciones de la institución. Tomar en cuenta las instrucciones del fabricante para la protección de los equipos que se encuentran fuera de estas instalaciones.

9.6. Seguridad en la reutilización o eliminación de los equipos

1. Destruir, borrar o sobrescribir los dispositivos que contienen información sensible utilizando técnicas que permitan la no recuperación de la información original.
2. Evaluar los dispositivos deteriorados que contengan información sensible antes de enviar a reparación, borrar la información o determinar si se debería eliminar físicamente el dispositivo.

9.7. Retiro de activos de la propiedad

1. Tener autorización previa para el retiro de cualquier equipo, información o software.
2. Identificar a los empleados, contratistas y usuarios de terceras partes, que tienen la autorización para el retiro de activos de la institución.
3. Establecer límites de tiempo para el retiro de equipos y verificar el cumplimiento en el momento de la devolución.
4. Registrar cuando el equipo o activo sea retirado y cuando sea devuelto.

10. GESTIÓN DE COMUNICACIONES Y OPERACIONES

1. Documentar el proceso de respaldo y restauración de la información.
2. Documentar todos los procesos de los servicios de procesamiento de datos, incluyendo la interrelación con otros sistemas.
3. Documentar los contactos de soporte, necesarios en caso de incidentes.
4. Documentar los procedimientos para reinicio y recuperación del sistema en caso de fallas.
5. Documentar los registros de auditoría y de la información de registro del sistema.

10.1. Gestión del Cambio

1. Evaluar el impacto de dichos cambios.
2. Aprobar de manera formal los cambios propuestos.
3. Planificar el proceso de cambio.
4. Realizar pruebas del cambio.
5. Comunicar el detalle de cambios a todas las personas involucradas.
6. Identificar responsabilidades por la cancelación de los cambios fallidos y la recuperación respecto de los mismos.
7. Establecer responsables y procedimientos formales del control de cambios en los equipos y software. Los cambios deben efectuarse únicamente cuando haya razón válida para el negocio, como: cambio de versión, corrección de vulnerabilidades, costos, licenciamiento, nuevo hardware, etc.

10.2. Separación de las instancias de Desarrollo, Pruebas, Capacitación y Producción.

1. Definir y documentar diferentes entornos para desarrollo, pruebas, capacitación y producción. Para el caso que no se pueda definir diferentes entornos con recursos físicos independientes, se debe mantener diferentes directorios con su respectiva versión y delegación de acceso.
2. Aislar los ambientes de desarrollo, pruebas, capacitación y producción.
3. Controlar la instalación y uso de herramientas de desarrollo de software y/o acceso a bases de datos y redes en los equipos informáticos, salvo que sean parte de las herramientas de uso estándar o su instalación sea autorizada de acuerdo a un procedimiento expresamente definido.
4. Implantar ambientes de prueba, iguales en capacidad, a los ambientes de producción.
5. Utilizar sistemas de autenticación y autorización independientes para las diversas instancias o ambientes.
6. Definir perfiles de usuario para las diferentes instancias o ambientes.
7. Aislar los datos sensibles de los ambientes de desarrollo, pruebas y capacitación.
8. Permitir al personal de desarrollo de software el acceso al entorno de producción, únicamente en caso de extrema necesidad, con la autorización explícita correspondiente.

10.3. Monitoreo y revisión de los servicios, por terceros.

1. Identificar los sistemas sensibles o críticos que convenga tener dentro o fuera de la institución.
2. Analizar los reportes de servicios, reportes de incidentes elaborados por terceros y acordar reuniones periódicas según los acuerdos.
3. Revisar y verificar los registros y pruebas de auditoría de terceros, con respecto a eventos de seguridad, problemas de operación, fallas relacionados con el servicio prestado.

10.4. Gestión de los cambios en los servicios ofrecidos por terceros.

1. Establecer un proceso de gestión de cambios en los servicios ofrecidos por terceros, en el desarrollo de aplicaciones, provisión de servicios de hardware, software, redes, otros.
2. Coordinar el proceso de cambio cuando se necesita realizar cambios o mejoras a las redes y uso de nuevas tecnologías en los servicios ofrecidos por terceros.
3. Coordinar el proceso de cambio cuando se realice cambio de proveedores, cambio de ubicación física en los servicios ofrecidos por terceros.

10.5. Aceptación del Sistema.

1. Considerar procedimientos de recuperación y planes de contingencia.
2. Asegurar que la instalación del nuevo sistema no afecte negativamente los sistemas existentes, especialmente en períodos pico de procesamiento.
3. Considerar el efecto que tiene el nuevo sistema en la seguridad global de la institución.
4. Capacitar sobre el funcionamiento y utilización del nuevo sistema.
5. Para nuevos desarrollos, se debe involucrar a los usuarios y a todas las áreas relacionadas, en todas las fases del proceso, para garantizar la eficacia operativa del sistema propuesto.

10.6. Controles contra código malicioso

1. Prohibir el uso de software no autorizado por la institución. Elaborar un listado del software autorizado.
2. Establecer procedimientos para evitar riesgos en la obtención/descarga de archivos y software desde o a través de redes externas o por cualquier otro medio.
3. Instalar y actualizar periódicamente software de antivirus y contra código malicioso.
4. Mantener los sistemas operativos y sistemas de procesamiento de información actualizados con las últimas versiones de seguridad disponibles.
5. Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos de la institución.
6. Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos o en archivos recibidos a través de redes no confiables.
7. Redactar procedimientos para verificar toda la información relativa a software malicioso.
8. Emitir boletines informativos de alerta con información precisa.
9. Concienciar al personal acerca del problema de los virus y cómo proceder frente a los mismos.
10. Contratar con el proveedor de Internet o del canal de datos los servicios de filtrado de: virus, spam, programas maliciosos (malware), en el perímetro externo.

10.7. Controles contra códigos móviles

1. Aislar de forma lógica los dispositivos móviles en forma similar a lo que ocurre con las VLANs.
2. Bloquear códigos móviles no autorizados.
3. Gestionar el código móvil mediante procedimientos de auditoría y medidas técnicas disponibles.
4. Establecer controles criptográficos para autenticar de forma única el código móvil.

10.8. Respaldo de la información.

1. Los responsables del área de Tecnologías de la Información, Oficial de Seguridad de la Información junto con el propietario de la información, determinarán los procedimientos para el resguardo y contención de la información.
2. Definir el procedimiento de etiquetado de las copias de respaldo, identificando su contenido, periodicidad y retención.
3. Definir la extensión (completo/diferencial) y la frecuencia de los respaldos, de acuerdo a los requisitos del negocio de la institución.
4. Establecer procedimientos de los medios de respaldo, una vez concluida su vida útil recomendada por el proveedor y la destrucción de estos medios.
5. Guardar los respaldos en un sitio lejano, a una distancia suficiente para evitar cualquier daño debido a desastres en la sede principal de la institución.
6. Proporcionar un grado apropiado de protección física y ambiental.
7. Establecer procedimientos regulares de verificación y restauración de los medios de respaldo para garantizar sean confiables para uso de emergencia.
8. Proteger la información confidencial por medio de encriptación.
9. Considerar los respaldos a discos y en el mismo sitio si se tiene suficientes recursos, ya que, en caso de mantenimientos de los sistemas de información, es más rápida su recuperación.

10.9. Controles de las redes.

1. Separar el área de redes del área de operaciones, cuando la capacidad y recursos lo permitan.
2. Designar procedimientos y responsabilidades para la gestión de equipos remotos como el caso de redireccionamiento de puertos y accesos por VPNs, incluyendo el área de operaciones y el área de usuarios finales.
3. Establecer controles especiales para salvaguardar la confidencialidad y la integridad de los datos que pasan por las redes públicas, redes locales e inalámbricas; así como la disponibilidad de las redes.
4. Garantizar la aplicación de los controles mediante actividades de supervisión.
5. Disponer de un esquema de red de los enlaces de datos, Internet y redes locales, así como la documentación respectiva.

10.10. Seguridad de los servicios de la red.

1. Incorporar tecnología para la seguridad de los servicios de red como la autenticación, encriptación y controles de conexión de red.
2. Implementar soluciones que proporcionen valor agregado a las conexiones y servicios de red, como la implementación de firewalls, antivirus, etc.

3. Definir procedimientos para la utilización de los servicios de red para restringir el acceso a los servicios de red cuando sea necesario.

10.11. Gestión de los medios removibles.

1. Establecer un procedimiento para la gestión de todos los medios removibles.
2. Tener autorización para la conexión de los medios removibles y registrar la conexión y retiro, para pruebas de auditoría.
3. Almacenar los medios removibles en un ambiente seguro, según las especificaciones de los fabricantes.
4. Evitar la pérdida de información por deterioro de los medios.

10.12. Eliminación de los medios

1. Identificar los medios que requieran eliminación segura.
2. Almacenar y eliminar de forma segura los medios que contienen información sensible, como la incineración, trituración o borrado de los datos.
3. Establecer procedimientos para selección del contratista que ofrece servicios de recolección y eliminación del papel, equipos y medios.
4. Registrar la eliminación de los medios para mantener pruebas de auditoría.

10.13. Procedimientos para el manejo de la información

1. Establecer procedimientos para el manejo y etiquetado de todos los medios de acuerdo a su nivel de clasificación.
2. Establecer controles de acceso para evitar el acceso de personal no autorizado.
3. Tener un registro actualizado de los receptores de los medios.
4. Establecer controles de protección según el nivel de sensibilidad de los datos que reside en la memoria temporal.
5. Almacenar los medios según especificaciones del fabricante.

10.14. Seguridad de la documentación del sistema.

1. Guardar con seguridad toda la documentación de los sistemas informáticos.
2. Mantener una lista de acceso mínima a la documentación del sistema y con su debida autorización.
3. Mantener una protección adecuada de la documentación del sistema expuesta en la red pública.

10.15. Mensajería electrónica

1. Establecer lineamientos para proteger los mensajes contra los accesos no autorizados, modificación o denegación de los servicios.
2. Supervisar que la dirección y el transporte de mensajes sean correctos.
3. Tomar en cuenta consideraciones legales como la de firmas electrónicas.
4. Encriptar los contenidos y/o información sensible que puedan enviarse por mensajería electrónica; utilizando firmas electrónicas reconocidas por el Estado Ecuatoriano u otras tecnologías evaluadas y aprobadas por la entidad o el Gobierno Nacional.

10.16. Transacciones en línea.

1. Definir procedimientos para el uso de certificados de firmas electrónicas por las partes implicadas en la transacción.
2. Establecer procedimientos para garantizar todos los aspectos en la transacción como credenciales de usuario, confidencialidad de la transacción y privacidad de las partes.
3. Cifrar o encriptar el canal de comunicaciones entre las partes involucradas (por ejemplo, utilizando SSL/TLS).
4. Establecer protocolos seguros en la comunicación de las partes involucradas, por ejemplo, utilizando SSL/TLS).
5. Establecer procedimientos para que las transacciones se encuentren fuera del entorno de acceso público.
6. Utilizar los servicios de una entidad certificadora confiable.

10.17. Información disponible al público.

1. Establecer controles para que la información disponible al público se encuentre conforme a la normativa vigente.
2. Definir controles para que la información de entrada sea procesada completamente y de forma oportuna.
3. Establecer procedimientos para que la información sensible sea protegida durante la recolección, procesamiento y almacenamiento.

10.18. Registros de auditorías.

1. Identificar el nombre de usuario.
2. Registrar la fecha, hora y detalles de los eventos clave, como registro de inicio y registro de cierre.
3. Registrar la terminal si es posible.
4. Registrar los intentos aceptados y rechazados de acceso al sistema.
5. Registrar los cambios de la configuración.
6. Registrar el uso de privilegios.
7. Registrar el uso de las aplicaciones y sistemas.
8. Registrar los accesos y tipos de acceso.
9. Registrar las direcciones y protocolos de red.

10. Definir alarmas originadas por el sistema de control de acceso.
11. Activación y desactivación de los sistemas de protección como antivirus y los sistemas de detección de intrusos (IDS).

10.19. Monitoreo de uso del sistema.

1. Identificación del ID de usuarios
2. Fecha y hora de eventos clave
3. Archivos a los que se han tenido acceso
4. Programas y utilitarios utilizados.
5. Monitorear las operaciones privilegiadas
6. Monitorear intentos de acceso no autorizados
7. Revisar alertas o fallas del sistema
8. Revisar cambios o intentos de cambio en la configuración y los controles de la seguridad del sistema.

10.20. Protección del registro de la información.

1. Proteger de alteraciones en todos los tipos de mensaje que se registren.
2. Proteger archivos de registro que se editen o se eliminen.
3. Precautelar la capacidad de almacenamiento que excede el archivo de registro.
4. Realizar respaldos periódicos del registro del servicio.

11. CONTROL DE ACCESO

11.1. Política de control de acceso

1. Gestionar los accesos de los usuarios a los sistemas de información, asegurando el acceso de usuarios autorizados y previniendo los accesos no autorizados.
2. Definir responsabilidades para identificar, gestionar y mantener perfiles de los custodios de información.

11.2. Registro de usuarios

1. Establecer un procedimiento formal, documentado y difundido, en el cual se evidencie detalladamente los pasos y responsables.
2. Definir el administrador de accesos que debe controlar los perfiles y roles.
3. Crear los accesos para los usuarios, para lo cual la institución debe generar convenios de confidencialidad y responsabilidad con el usuario solicitante; además, validar que el usuario tenga los documentos de ingreso con Recursos Humanos (o quien haga estas funciones) en orden y completos.
4. Modificar los accesos de los usuarios.

5. Eliminar los accesos de los usuarios.
6. Suspender temporalmente los accesos de los usuarios en caso de vacaciones, comisiones, licencias, es decir, permisos temporales.
7. Proporcionar accesos temporales a usuarios externos o terceros de acuerdo al tiempo de su permanencia y limitados según las actividades para las que fueron contratados y firmar un convenio de confidencialidad.
8. Mantener un registro de la gestión de accesos a aplicaciones, redes, que evidencie, fecha de creación, eliminación, suspensión, activación o eliminación del acceso; al igual que de cada usuario, disponer de los permisos de acceso que han sido asignados.

11.3. Gestión de contraseñas para usuarios

1. Establecer un proceso formal para la asignación y cambio de contraseñas.

11.4. Revisión de los derechos de acceso de los usuarios

1. Realizar las depuraciones respectivas de los accesos de los usuarios, determinando un período máximo de 30 días; en casos de presentar cambios estructurales, esta gestión deberá hacerse inmediatamente que se ejecute el cambio organizacional.
2. Evidenciar los cambios sobre los derechos de acceso en archivos de log o registro de los sistemas, los cuales deben estar disponibles en caso de que se requieran.

11.5. Uso de contraseñas

1. Documentar, en el procedimiento de accesos, las responsabilidades de los usuarios tanto internos como externos, sobre el uso de la cuenta y la contraseña asignadas.
2. Recomendar la generación de contraseñas con letras mayúsculas, minúsculas, con caracteres especiales, difíciles de descifrar, es decir, que cumplen una complejidad media y alta.
3. Evitar contraseñas en blanco o que viene por defecto según el sistema el fabricante del producto, puesto que son fácilmente descifrables; por ejemplo: admin, administrador, administrador, user, usuario, entre otros.
4. Controlar el cambio periódico de contraseñas de los usuarios.
5. Generar y documentar revisiones periódicas de la gestión de usuarios incluidos los administradores de tecnología, por parte del Oficial de Seguridad de la Información.

11.6. Equipo de usuario desatendido

1. Implementar medidas para que, en un determinado tiempo (ej., no mayor a 10 minutos), si el usuario no está realizando ningún trabajo en el equipo,

este se bloquee, y se desbloquee únicamente si el usuario ingresa nuevamente su clave

11.7. Autenticación de usuarios para conexiones externas

1. Generar mecanismos para asegurar la información transmitida por los canales de conexión remota, utilizando técnicas como encriptación de datos, implementación de redes privadas virtuales (VPN) y Servicio de Acceso Remoto (SAR).
2. Realizar un mecanismo diferenciado para la autenticación de los usuarios que requieren conexiones remotas, que permita llevar control de registros (logs) y que tenga limitaciones de accesos en los segmentos de red.

11.8. Protección de los puertos de configuración y diagnóstico remoto

1. Establecer un procedimiento de soporte, en el cual se garantice que los puertos de diagnóstico y configuración sean sólo accesibles mediante un acuerdo entre el administrador del servicio de computador y el personal de soporte de hardware/ software que requiere el acceso.
2. Los puertos, servicios (ej., fftp) que no se requieren por necesidades de la institución, deberán ser eliminados o deshabilitados.

11.9. Separación en las redes

1. Realizar una evaluación de riesgos para identificar los segmentos de red donde se encuentren los activos críticos para la institución.
2. Dividir las redes en dominios lógicos de red, dominios de red interna, dominios de red externa e inalámbrica.
3. Documentar la segregación de red, identificando las direcciones IP que se encuentran en cada segmento de red.
4. Configurar la puerta de enlace (gateway) para filtrar el tráfico entre dominios y bloquear el acceso no autorizado.
5. Controlar los flujos de datos de red usando las capacidades de enrutamiento/conmutación (ej.,listas de control de acceso).
6. La separación de las redes debe ejecutarse en base a la clasificación de la información almacenada o procesada en la red, considerando que el objetivo es dar mayor protección a los activos de información críticos en función del riesgo que éstos podrían presentar.
7. Separar redes inalámbricas procedentes de redes internas y privadas, para evitar el acceso a terceros y de usuarios externos a las redes privadas internas.

11.10. Control del enrutamiento en la red

1. Configurar políticas de control de acceso para el enrutamiento en la red, basándose en los requerimientos de la institución.
2. Las puertas de enlace de la seguridad (gateway) se pueden usar para validar la dirección fuente/destino en los puntos de control de las redes internas y externas, si se emplean tecnologías proxy y/o de traducción de direcciones de red.
3. Las instituciones que utilizan proxys y quienes definen las listas de control de acceso (LCA), deben estar conscientes de los riesgos en los mecanismos empleados, a fin de que no existan usuarios o grupos de usuarios con salida libre y sin control, en base a las políticas de la institución.

11.11. Limitación del tiempo de conexión

1. Utilizar restricciones en los tiempos de conexión para brindar seguridad adicional para las aplicaciones de alto riesgo. Los siguientes son algunos ejemplos de estas restricciones.
2. Configurar espacios de tiempo predeterminados para procesos especiales (por ejemplo, transmisiones de datos o archivos, obtención de respaldos, mantenimientos programados, entre otros.)
3. Restringir los tiempos de conexión a las horas normales de oficina, si no se requiere tiempo extra u operaciones de horario prolongado.
4. Requerir la autenticación a intervalos determinados cuando lo amerite.
5. Proporcionar accesos temporales para ciertas operaciones (por ejemplo, mediante tickets o tokens electrónicos temporales)

11.12. Control de acceso a las aplicaciones y a la información

1. Controlar el acceso de usuarios a la información y a las funciones del sistema de aplicación, de acuerdo con una política definida de control de acceso.
2. Suministrar protección contra acceso no autorizado por un programa utilitario, software del sistema operativo, software malicioso o cualquier otro software que pueda anular o desviar los controles de seguridad del sistema.
3. Evitar poner en riesgo otros sistemas con los que se comparten los recursos de información.

11.13. Computación y comunicaciones móviles

1. Evitar exposición de equipos portátiles en sitios inseguros, públicos y de alto riesgo.

2. La información sensible, de alta criticidad o confidencial, debe estar en una partición específica del disco del equipo portátil, y resguardada bajo métodos de cifrado.
3. En la política para uso de equipos portátiles y comunicaciones móviles de la institución, deberá definir rangos de tiempo máximo que el equipo puede permanecer sin conexión a la red de la institución, a fin de que este actualice el antivirus y las políticas aplicadas por la institución.
4. En el proceso de respaldos de la institución, debe estar considerado específicamente los documentos definidos como críticos, sensibles o confidenciales de las diferentes áreas; además, en el proceso de respaldo del equipo portátil deberá definirse el responsable y procedimiento de acceso a esta información.
5. Dentro de la institución el equipo portátil deberá estar asegurado con medios físicos, mediante el uso de candados.
6. El personal que utiliza computadores portátiles y equipos móviles deberá estar alerta de los riesgos adicionales que se originan y los controles que se deberán implementar.

11.14. Trabajo remoto

1. El funcionario deberá observar la seguridad física de la edificación y del entorno local existente en el sitio de trabajo remoto.
2. Deberá evitarse la conexión a redes inalámbricas que no presten la seguridad de acceso y autenticación adecuados.
3. No se permite el uso de equipo de propiedad privada que no esté bajo el control y monitoreo de la institución.
4. Deberá definirse el trabajo que se permite realizar, las horas laborables, la confidencialidad de la información que se conserva y los sistemas y servicios internos para los cuales el trabajador tiene acceso autorizado.
5. Deberá considerarse la protección de antivirus y reglas del Firewall.
6. Deberán estar documentadas las reglas y directrices sobre el acceso de familiares y visitantes al equipo y a la información.
7. La institución deberá observar la disposición de una póliza de seguros para esos equipos.
8. Determinar procesos de monitoreo y auditoría de la seguridad del trabajo remoto que se realice.
9. Permitir al personal realizar trabajo remoto empleando tecnologías de comunicaciones cuando requiere hacerlo desde un lugar fijo fuera de su institución.

12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

12.1. Análisis y especificaciones de los requerimientos de seguridad

1. Definir los requerimientos de seguridad. Por ejemplo: criptografía, control de sesiones, etc.
2. Definir los controles apropiados, tanto automatizados como manuales. En esta definición deben participar personal del requerimiento funcional y personal técnico que trabajarán en el sistema. Evaluar los requerimientos de seguridad y los controles requeridos, teniendo en cuenta que éstos deben ser proporcionales en costo y esfuerzo al valor del bien que se quiere proteger y al daño potencial que pudiera ocasionar a las actividades realizadas por falla o falta de seguridad.
3. Si se adquieren productos, los contratos con el proveedor deben contemplar los requisitos de la seguridad identificados.

12.2. Validación de datos de entrada

1. Especificar y utilizar controles que aseguren la validez de los datos ingresados, en el punto de entrada de los mismos, controlando también parámetros de los sistemas (ej., %IVA, dirección IP del servidor).
2. Definir el estándar de respuesta ante errores de validación.

12.3. Control de procesamiento interno

1. Incorporar controles de validación a fin de eliminar o minimizar los riesgos de fallas de procesamiento y/o vicios por procesos de errores.
2. Utilizar controles de sesión en los sistemas.
3. Utilizar funciones de agregar, modificar y borrar para implementar los cambios en los datos. El borrado a través de los sistemas será siempre un borrado lógico de los datos.
4. Crear registros de auditoría, al insertar y actualizar datos; y, si se requiere según el sistema, se mantendrá el registro (logs) de consultas de datos.
5. Crear el procedimiento y/o herramientas para la revisión periódica de los registros de auditoría para detectar cualquier anomalía en la ejecución de las transacciones.
6. Identificar, crear y utilizar programas para la recuperación de datos después de fallas, con el fin de garantizar el procesamiento correcto de los datos.
7. Utilizar controles para mantener integridad de registros y archivos.
8. Utilizar controles para protección contra ataques por desbordamiento/exceso en el buffer.
9. Definir y ejecutar periódicamente, procedimientos de recuperación de sistemas, que verifiquen la ejecución de los sistemas en caso de una falla

o desastre, esto estará a cargo del administrador técnico de la aplicación o sistema.

12.4. Integridad del mensaje

1. Cuando una aplicación tenga previsto el envío de mensajes que contengan información reservada o confidencial, se implementarán los controles criptográficos determinados en el punto "

12.5. Política sobre el uso de controles criptográficos.

1. Identificar el nivel requerido de protección de datos que se almacenará en el sistema, considerando: el tipo, fortaleza y calidad del algoritmo de cifrado (encriptación) requerido.
2. Utilizar controles criptográficos para la protección de claves de acceso a: sistemas, datos y servicios. Las claves deberán ser almacenadas de manera codificada, cifrada (encriptada) en la base de datos y/o en archivos de parámetros.
3. Los responsables del área de Tecnologías de la Información propondrán la siguiente asignación de funciones: Implementación de la Política de Controles, Administración de claves: gestión de claves, incluyendo su generación.

12.6. Se debe garantizar:

1. Confidencialidad: uso de cifrado (encriptación) de la información para proteger información sensible o crítica, bien sea almacenada o transmitida
2. Integridad / autenticidad: uso de firmas electrónicas o códigos de autenticación de mensajes para proteger la autenticidad e integridad de información sensible o crítica transmitida o almacenada.
3. No-repudio: uso de técnicas de cifrado (criptográficas) para obtener prueba de la ocurrencia o no ocurrencia de un evento o acción.
4. Utilizar certificados electrónicos de Entidad de Certificación de Información reconocidas por el Estado Ecuatoriano para la firma de cualquier tipo de documento, mensaje de dato, transacción que se procese electrónicamente o para comunicaciones entre sistemas, aplicaciones y medios físicos.
5. Utilizar los certificados electrónicos emitidos bajo estándares por las Entidades de Certificación de Información, las cuales deben ser instituciones u organizaciones reconocidas, con controles y procedimientos idóneos establecidos para proporcionar el grado requerido de confianza.
6. Uso de los certificados electrónicos según el ámbito para la cual fue generado.

12.7. Gestión de claves

Protección de claves cifradas (criptográficas):

1. Implementar un sistema de administración de claves cifradas (criptográficas) para respaldar la utilización por parte de la institución, de los dos tipos de técnicas criptográficas: técnicas de clave secreta (criptografía simétrica) y técnicas de clave pública (criptografía asimétrica).
2. Proteger todas las claves contra modificación y destrucción, y las claves secretas y privadas serán protegidas contra copia o divulgación no autorizada.
3. Proporcionar una protección adecuada al equipamiento utilizado para generar, almacenar y archivar claves, considerándolo crítico o de alto riesgo.
4. Distribuir la primera clave a los usuarios, incluyendo la forma de activar y confirmar la recepción de la clave. Luego, a través de un correo electrónico recibirá un acceso al sistema, el cual validará la entrega de la clave y la obligatoriedad de cambiar dicha clave.
5. Incorporar funcionalidad para cambiar o actualizar las claves, incluyendo reglas sobre cuándo cambiarlas, cómo hacerlo y la forma en que los usuarios autorizados tendrán acceso a ellas.
6. Incorporar funcionalidad para tratar las claves perdidas. Bajo pedido del usuario que pierde una clave se generará una nueva, la entrega será a través del procedimiento definido para la entrega de la primera clave.
7. Permitir revocar las claves, incluyendo la forma de retirarlas o desactivarlas cuando las claves se han puesto en peligro o cuando un usuario se retira de la institución.
8. Incorporar funcionalidad para recuperar claves pérdidas o corruptas como parte de la gestión de continuidad de los servicios informáticos.
9. Registrar y auditar las actividades relacionadas con la gestión de claves.

12.8. Control del software operativo

1. Definir y aplicar procesos de control de cambios para la implementación del software en producción, a fin de minimizar el riesgo de alteración de los sistemas.
2. Ningún programador o analista de desarrollo y mantenimiento de aplicaciones podrá acceder a los ambientes de producción.
3. Asignar un responsable de la implantación de cambios por sistema (no podrá ser personal que pertenezca al área de desarrollo o mantenimiento), quien tendrá como funciones principales
4. Coordinar la implementación de modificaciones o nuevos programas en el ambiente de Producción.
5. Asegurar que los aplicativos en uso, en el ambiente de Producción, sean los autorizados y aprobados de acuerdo a las normas y procedimientos vigentes.

6. Instalar las modificaciones, controlando previamente la recepción de la prueba aprobada por parte del Analista Responsable, del área encargada del testeo y del usuario final.
7. Rechazar la implementación en caso de encontrar defectos
8. Definir un procedimiento que establezca los pasos a seguir para implementar las autorizaciones para el paso a producción, el informe de pruebas previas y el informe de paso a producción.
9. Disponer del informe de paso a producción, el cual contendrá información de todos los cambios a realizar y el plan de contingencia.
10. Guardar o instalar únicamente los ejecutables y cualquier elemento necesario para la ejecución de un software en el ambiente de producción.
11. Llevar un registro de auditoría de las actualizaciones realizadas.
12. Retener las versiones previas del sistema, como medida de contingencia.
13. Denegar permisos de modificación a los desarrolladores, sobre los programas fuentes bajo su custodia.
14. Entregar acceso físico o lógico al ambiente producción únicamente para propósitos de soporte, cuando sea necesario y con aprobación del responsable del área de Tecnologías de la información, esto se realizará tanto para usuarios internos de la dirección como para proveedores.

12.9. Protección de los datos de prueba del sistema

1. Identificar por cada sistema, los datos que pueden ser copiados de un ambiente de producción a un ambiente de pruebas.
2. Efectuar pruebas de los sistemas en el ambiente de pruebas, sobre datos extraídos del ambiente de producción.
3. Solicitar autorización formal para realizar una copia de la base de datos de producción como base de datos de prueba.
4. Identificar los datos críticos que deberán ser modificados o eliminados del ambiente de pruebas.
5. Aplicar los mismos procedimientos de control de acceso que existen en la base de producción.
6. Registrar la copia y la utilización de la información para futuras auditorías.
7. Controlar que la modificación, actualización o eliminación de los datos operativos (de producción) serán realizados a través de los sistemas que procesan esos datos, y de acuerdo al esquema de control de accesos implementado en los mismos
8. Se designará un encargado de implementar los cambios, el cual no será personal del área de Desarrollo. En el caso de que esta función no pueda ser separada del área de Desarrollo, se aplicarán controles adicionales de acuerdo a la separación de funciones.

12.10. Control de acceso al código fuente de los programas

1. Asignar a un Administrador de programas fuentes, quien tendrá en custodia los programas fuentes y deberá

2. Utilizar un manejador de versiones para los códigos fuente, proporcionar permisos de acceso a los desarrolladores bajo autorizaciones.
3. Llevar un registro actualizado de todos los programas fuentes en uso, indicando nombre del programa, programador, autorizador, versión, fecha de última modificación y fecha/hora de compilación y estado (en modificación o en producción).
4. Asegurar que un mismo programa fuente no sea modificado simultáneamente por más de un desarrollador, sin un manejador de versiones.
5. Establecer que todo programa objeto o ejecutable en producción tenga un único programa fuente asociado que garantice su origen.
6. Establecer que el responsable de implantación en producción efectuará la generación del programa objeto o ejecutable que estará en producción (compilación), a fin de garantizar tal correspondencia.
7. Desarrollar un procedimiento que garantice que cuando se migre a producción el módulo fuente, de preferencia se cree el código ejecutable correspondiente de forma automática de preferencia.
8. Evitar que la función de Administrador de programas fuentes, sea ejercida por personal que pertenezca al área de desarrollo y/o mantenimiento.
9. Prohibir el acceso a todo operador y/o usuario de aplicaciones a los ambientes y a las herramientas que permitan la generación y/o manipulación de los programas fuentes.
10. Realizar las copias de respaldo de los programas fuentes cumpliendo los requisitos de seguridad establecidos como respaldos de información.
11. El personal de soporte no debe tener acceso al código fuente de programas.
12. La actualización del código fuente de programas y de los elementos asociados, así como la emisión de fuentes de programa a los programadores, solamente se deberá efectuar después de recibir la autorización apropiada.

12.11. Procedimiento de control de cambios

1. Verificar que los cambios sean propuestos por usuarios autorizados y se respete los términos y condiciones que surjan de la licencia de uso, en caso de existir.
2. Elaborar el informe de paso de pruebas a producción, que deberá contener el detalle de los cambios y acciones a ejecutar, tanto de software, bases de datos y hardware:

12.12. Revisión técnica de las aplicaciones después de los cambios en el sistema operativo

1. Revisar los procedimientos de integridad y control de aplicaciones para garantizar que no hayan sido comprometidas por el cambio.
2. Probar que los cambios realizados retornen la funcionalidad esperada.

3. Realizar las pruebas inmediatamente después de realizar el cambio y durante la ventana de mantenimiento definida para el cambio.
4. Identificar si existen problemas con los cambios, para aplicar el plan de contingencia o realizar el retorno al estado anterior al cambio.

12.13. Restricción del cambio de paquetes de software

1. Disponer de la autorización del responsable del área de Tecnologías de la Información que apruebe el cambio
2. Analizar los términos y condiciones de la licencia, si es del caso, a fin de determinar si las modificaciones se encuentran autorizadas.
3. Retener el software original realizando los cambios sobre una copia perfectamente identificada, documentando exhaustivamente por si fuera necesario aplicarlo a nuevas versiones.
4. Conservar el software original que se va a cambiar y los cambios se deberán aplicar a una copia claramente identificada
5. Probar y documentar en su totalidad todos los cambios, de manera que se puedan volver a aplicar, si es necesario, para mejoras futuras del software.

12.14. Fuga de información

1. Explorar los medios y comunicaciones de salida para determinar la información oculta.
2. Garantizar que un tercero no pueda deducir, extraer información de las comunicaciones, sistemas de modulación o de enmascaramiento, a partir de un comportamiento específico.
3. Adquirir o desarrollar programas acreditados o productos ya evaluados.
4. Realizar un monitoreo regular de las actividades del personal y del sistema.
5. Realizar un monitoreo del uso de los recursos en los sistemas de computador y transmisión de datos por la red.
6. Restringir el envío de información a correos externos no institucionales.
7. Prevenir y restringir el acceso no autorizado a la red.
8. Examinar los códigos fuentes (cuando sea posible) antes de utilizar los programas.

12.15. Desarrollo de software contratado externamente

1. Definir acuerdos de licencias, acuerdos de uso, propiedad de código y derechos conferidos.
2. Definir los requerimientos contractuales con respecto a la calidad del código y la existencia de garantías.
3. Verificar el cumplimiento de las condiciones de seguridad requeridas.
4. Definir acuerdos de custodia de las fuentes del software o convenios de fideicomiso (y cualquier otra información requerida) en caso de quiebra de la tercera parte.

5. Realizar pruebas antes de la instalación para detectar códigos troyanos o maliciosos.

12.16. Control de las vulnerabilidades técnicas

1. Disponer de un inventario completo y actual de los activos de software. El inventario servirá para dar soporte a la gestión de la vulnerabilidad técnica e incluye los siguientes datos: vendedor del software, números de versión, estado actual de despliegue y las personas de la institución responsables del software.
2. Identificar los recursos de información que se van a utilizar para identificar las vulnerabilidades técnicas pertinentes y para mantener la concienciación sobre ellas para el software y otras tecnologías, con base en la lista de inventario de activos.
3. Definir una línea de tiempo para reaccionar ante la notificación de vulnerabilidades técnicas potenciales pertinentes.
4. Identificar los riesgos asociados a una vulnerabilidad potencial y las acciones que se han de tomar; tales acciones podrían involucrar el uso de parches en los sistemas vulnerables y/o la aplicación de otros controles.
5. Evaluar los riesgos asociados con la instalación de un parche para cubrir vulnerabilidades. Los riesgos impuestos por la vulnerabilidad se deberán comparar con los riesgos de instalar el parche.
6. Apagar los servicios o capacidades relacionadas con la vulnerabilidad.
7. Adaptar o agregar controles de acceso; por ejemplo, cortafuegos (firewalls), en las fronteras de la red.
8. Aumentar el monitoreo para detectar o prevenir los ataques reales.
9. Monitorear y evaluar a intervalos regulares las vulnerabilidades técnicas, para garantizar eficacia y eficiencia.

13. GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN

13.1. Control de las vulnerabilidades técnicas

1. Instaurar un procedimiento formal para el reporte de los eventos de seguridad de la información junto con un procedimiento de escala y respuesta ante el incidente, que establezca la acción que se ha de tomar al recibir el reporte sobre un evento que amenace la seguridad de la información.
2. Cuando un incidente se produzca, el funcionario en turno responsable del equipo o sistema afectado debe realizar las siguientes acciones en su orden
   - Identificar el incidente
   - Registrar el incidente en una bitácora de incidentes (reporte de eventos) incluyendo fecha, hora, nombres y apellidos del funcionario

en turno, departamento o área afectada, equipo o sistema afectado y breve descripción del incidente.

- Notificar al Oficial de Seguridad de la Información de la institución.
- Clasificar el incidente de acuerdo al tipo de servicio afectado y al nivel de severidad.
- Asignar una prioridad de atención al incidente en el caso de que se produjeran varios en forma simultánea.
- Realizar un diagnóstico inicial, determinando mensajes de error producidos, identificando los eventos ejecutados antes de que el incidente ocurra, recreando el incidente para identificar sus posibles causas.
- Investigar y diagnosticar en forma definitiva las causas por las cuales se produjo el incidente.
- Resolver y restaurar el servicio afectado por el incidente cuando se detiene un equipo o un sistema, incluyendo un registro de la solución empleada en la bitácora de incidentes.
- Cerrar el incidente, actualizando el estado del registro del incidente en la bitácora de incidentes a "Resuelto". Confirmar con el funcionario en turno, responsable del equipo o del sistema de que el incidente ha sido resuelto.

13.2. Reporte sobre las debilidades en la seguridad

1. Notificar a su Coordinador inmediato y este al Oficial de Seguridad de la Información de la debilidad o vulnerabilidad detectada.
2. Registrar la fecha, hora, apellidos y nombres del funcionario que detectó la debilidad o vulnerabilidad, descripción de la debilidad, descripción de posibles incidentes de seguridad que pudieran ocurrir producto de esta debilidad. El responsable de llevar este reporte denominado "Reporte de vulnerabilidades o debilidades de la seguridad de la información" es el Oficial de Seguridad de la Información.
3. El Oficial de Seguridad de la Información deberá tomar las medidas pertinentes para prevenir o eliminar la vulnerabilidad o debilidad detectada.

13.3. Responsabilidades y procedimientos

1. Identificar y clasificar los diferentes tipos de incidentes de seguridad de la información.
2. Identificar y analizar las posibles causas de un incidente producido.
3. Planificar e implementar acciones correctivas para evitar la recurrencia del incidente.
4. Notificar a todos los funcionarios afectados por el incidente de la restauración del equipo, sistema o servicio afectado, una vez esté solucionado el incidente.
5. Recolectar y asegurar pistas de auditoría y toda la evidencia relacionada con el incidente.

6. Determinar el costo promedio por incidente.
7. Determinar el número de incidentes recurrentes.
8. Determinar la frecuencia de un incidente recurrente.

13.4. Recolección de evidencias

1. Desarrollar y cumplir procedimientos internos cuando se recolecta y se presenta evidencia con propósitos de acción disciplinaria dentro de la institución.
2. Asegurar que los sistemas de información cumplan con las normas legales para la producción de evidencia, para lograr la admisibilidad, calidad y cabalidad de la misma.
3. Se debe proteger la integridad de todo el material de evidencia. El proceso de copia del material de evidencia debe estar supervisado por personal de confianza y se debe registrar la información sobre cuándo y cómo se realizó dicho proceso, quién ejecutó las actividades de copiado y qué Herramientas o programas se utilizaron.

14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

1. Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.
2. El responsable del área de Tecnologías de la Información o su similar será designado como coordinador de continuidad de los servicios informáticos, que se encargará de supervisar el proceso de elaboración e implantación del plan de continuidad, así como de la seguridad del personal.
3. Identificar los activos involucrados en los procesos críticos de los servicios informáticos, así como de las actividades que se deben realizar.

4. Elaborar la política de continuidad de los servicios informáticos determinando los objetivos y el alcance del plan, así como las funciones y responsabilidades; un documento que establezca a alto nivel los objetivos, el alcance y las responsabilidades en la gestión de la continuidad. Por ejemplo, la plantilla del documento debería contener:

    a. INTRODUCCION: Detallando de forma resumida de que se trata, la estructura del documento y que se persigue.

    b. OBJETIVOS: que se satisfacen con la aplicación de la política, como se garantizará continuidad de las actividades y de los servicios, planes adicionales de contingencia.

    c. ALCANCE: Procesos y operaciones que son cubiertos y recursos que utilizan los procesos u operaciones.

    d. RESPONSABILIDADES: Diferentes responsables implicados en la gestión de la continuidad de los servicios informáticos.

e. Garantizar la continuidad incorporando los procesos generados en la estructura de la institución.

14.1. Continuidad del negocio y evaluación de riesgos

1. Definir los procesos y actividades de los servicios y aplicaciones
2. Entender las complejidades e interrelaciones existentes entre equipamiento, personas, tareas, departamentos, mecanismos de comunicación y relaciones con proveedores externos, los cuales pueden prestar servicios críticos que deben ser considerados.
3. Identificar y valorar el impacto de las interrupciones de los procesos, aplicaciones y servicios de los servicios informáticos, para cuantificar y calificar los impactos y saber sus efectos.
4. Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información.
5. Logística: responsable de reunir todos los medios para ayudar a la puesta en operación de las actividades.
6. Recuperación: puesta en servicio de la infraestructura.
7. Desarrollar los procedimientos indicando el objetivo y el alcance, considerando las actividades y los tiempos de recuperación.
8. Difundir y capacitar al personal responsable en los conceptos que contemplan la continuidad de los servicios informáticos.
9. Seleccionar los sitios alternos y de almacenamiento externo.
10. Duplicado de los registros tanto físicos como electrónicos
11. Incorporar RAID en los discos de los servidores
12. Duplicar el suministro eléctrico.
13. Contratos de mantenimiento preventivo y correctivo.
14. Estrategia adecuada de respaldos
15. Seguros para los activos

15. CUMPLIMIENTO

15.1. Identificación de la legislación aplicable

1. Inventariar todas las normas legales, estatutarias, reglamentarias y contractuales pertinentes para cada programa de software, servicio informático y en general todo activo de información que utiliza la institución.
2. Organizar para cada activo de información las normas legales, estatutarias, reglamentarias y contractuales pertinentes.
3. Considerar las normas y leyes más generales relacionadas a la gestión de los datos e información electrónica en el gobierno. A saber:
4. Constitución de la República del Ecuador
5. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos
6. Ley Orgánica de Transparencia y Acceso a la Información Pública

7. Ley del Sistema Nacional de Registro de Datos Públicos
8. Estatuto del Régimen Jurídico Administrativo de la Función Ejecutiva
9. Ley Orgánica y Normas de Control de la Contraloría General del Estado
10. Decreto Ejecutivo No. 1014 sobre el uso de Software Libre en la Administración Pública.
11. Decreto Ejecutivo No. 1384 sobre interoperabilidad Gubernamental en la Administración Pública.

15.2. Derechos de Propiedad Intelectual

1. Adquirir software únicamente a proveedores reconocidos para garantizar que no se violen derechos de propiedad intelectual. Si el Software es Libre Opensource se considerará los términos de las licencias públicas generales.
2. Implementar mecanismos para concienciar sobre las políticas para proteger derechos de propiedad intelectual y las acciones disciplinarias para el personal que las viole. Se aplica tanto al software libre como al privativo.
3. Mantener registros apropiados de los activos de información para proteger los derechos de propiedad intelectual. Se aplica tanto al software libre como al privativo.
4. Custodiar evidencia de la propiedad de licencias o suscripciones, contratos, discos maestros, manuales y toda la información relevante del software que se utiliza.
5. Controlar y asegurar que no se exceda el número máximo de usuarios permitidos para un programa de software. Se aplica tanto al software libre como al privativo, donde corresponda.
6. Cumplir los términos y condiciones de uso para el software y la información, obtenidos de la Internet o proveedores (programas freeware, shareware, demostraciones o programas para pruebas).
7. Controlar que no se duplique, convierta en otro formato, ni extraiga contenidos de grabaciones de audio y video, si no está expresamente permitido por su autor o la persona que tenga los derechos sobre el material.
8. Controlar que no se copie total ni parcialmente software privativo, códigos fuente y la documentación de programas de software con derechos de propiedad intelectual. Se exceptúa los programas de software libre bajo los términos de sus licencias públicas.
9. Definir y aplicar una licencia pública general al software desarrollado por la institución o contratado a terceros como desarrollo, para proteger la propiedad intelectual.
10. Exigir a los funcionarios que utilicen solo software desarrollado, provisto o aprobado por la institución.

15.3. Protección de registros en cada entidad

1. Clasificar los registros electrónicos y físicos por tipos, especificando los periodos de retención y los medios de almacenamiento, como discos, cintas, entre otros.
2. Mantener la documentación y especificaciones técnicas de los algoritmos y programas utilizados para el cifrado y descifrado de archivos y toda la información relevante relacionada con claves, archivos criptográficos o firmas electrónicas, para permitir el descifrado de los registros durante el periodo de tiempo para el cual se retienen.
3. Establecer un procedimiento para revisar el nivel de deterioro de los medios utilizados para almacenar los registros. Los procedimientos de almacenamiento y manipulación se deberán implementar según las recomendaciones del fabricante. Para almacenamiento a largo plazo, se recomienda considerar el uso cintas y discos digitales utilizando formatos de archivos y datos abiertos.
4. Establecer un procedimiento para garantizar el acceso a los datos e información registrada, tanto el medio como el formato, durante todo el periodo de retención.
5. Establecer un procedimiento para cambiar o actualizar la tecnología del medio en el cual se almacenan los activos de información y registros de acuerdo a las innovaciones tecnológicas disponibles en el mercado.
6. Los sistemas de almacenamiento de datos se deberán seleccionar de manera que los datos requeridos se puedan recuperar en el periodo de tiempo y en formatos legibles, dependiendo de los requisitos que se deben cumplir.

15.4. Protección de los datos y privacidad de la información personal

El Oficial de Seguridad de la Información deberá controlar la aplicación de la política de protección de datos y privacidad de la información personal.

15.5. Reglamentación de controles criptográficos

1. Restringir importaciones y/o exportaciones de hardware y software de computadores para la ejecución de funciones criptográficas; o diseñados para adicionarles funciones criptográficas.
2. Restringir el uso de encriptación, y especificar y documentar los ámbitos en dónde se aplicarán tales procesos (ej., comunicaciones, firma de documentos, trasmisión de datos, entre otros).
3. Restringir métodos obligatorios o discrecionales de acceso por parte de las autoridades del país a la información encriptada mediante hardware o software para brindar confidencialidad al contenido.

4. Garantizar el cumplimiento con las leyes y los reglamentos nacionales antes de desplazar información encriptadas o controles criptográficos a otros países.

15.6. Verificación del cumplimiento técnico

1. Verificar el cumplimiento técnico bien sea manualmente (con soporte de las herramientas de software apropiadas, si es necesario) por un ingeniero de sistemas con experiencia, y/o con la ayuda de herramientas automáticas que generen un informe técnico para la interpretación posterior por parte del especialista técnico.
2. Analizar los sistemas operativos para asegurar que los controles de hardware y software se han implementado correctamente. Este tipo de verificación del cumplimiento requiere experiencia técnica especializada.

3. Ejecutar o contratar pruebas de penetración y evaluaciones de la vulnerabilidad, las cuales pueden ser realizadas por expertos independientes especialmente contratados para este propósito. Ello puede ser útil para detectar vulnerabilidades en el sistema y verificar qué tan efectivos son los controles evitando el acceso no autorizado debido a estas vulnerabilidades. Las pruebas de penetración y las evaluaciones de vulnerabilidad no deben substituir las evaluaciones de riesgos.

GLOSARIO DE TÉRMINOS Y SIGLAS

BD: Base de datos.
CSI: Comité de Gestión de la Seguridad de la Información.
EGSI: Esquema Gubernamental de Seguridad de la Información.
SNAP: Secretaría Nacional de la Administración Pública.
NAS: Network Attached Storage.
SAN: Storage Area Network.
IDS: Intrusion Detection System.
IPS: Intrusion Prevention System.
SPAM: o información basura, hace referencia a aquellos mensajes, con remitente desconocido, que no son solicitados ni deseados por el usuario y que, además, por norma general, son enviados en grandes cantidades.
MALWARE: El término se utiliza para hablar de todo tipo de amenazas informáticas o software hostil, y existen distintos tipos de malware en función de su origen y consecuencias.
VLAN: acrónimo de virtual LAN (red de área local virtual).
VPN: Virtual Private Network es una tecnología de red de computadoras que permite una extensión segura de la red de área local sobre una red pública o no controlada como Internet.
SSL: Secure Sockets Layer (capa de sockets seguros), la tecnología estándar para mantener segura una conexión a Internet, así como para proteger cualquier

información confidencial que se envía entre dos sistemas e impedir que los delincuentes lean y modifiquen cualquier dato que se transfiera, incluida información que pudiera considerarse personal.
TLS: Transport Layer Security (seguridad de la capa de transporte) es solo una versión actualizada y más segura de SSL.
CIFRADO: [mensaje] Que está escrito con letras, símbolos o números que solo pueden comprenderse si se dispone de la clave necesaria para descifrarlos.
CRIPTOGRAFÍA: Arte y técnica de escribir con procedimientos o claves secretas o de un modo enigmático, de tal forma que lo escrito solamente sea inteligible para quien sepa descifrarlo.

Certifico.- Que el presente Reglamento de Aseguramiento y Gestión de la Información de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, fue aprobado por el pleno del Honorable Consejo Politécnico en sesión ordinaria del 17 de diciembre de 2018, mediante resolución Nº 017-2018, numeral 16.

Ab. Lya Villafuerte Vélez Mg. P.E.S
SECRETARIA GENERAL DE LA ESPAM MFL