Manual con las políticas de seguridad y privacidad de la información. Instituto Nacional de Formación Técnica Profesional

INFOTEP
SAN JUAN DEL CESAR, ENERO DE 2021

Manual con las políticas de seguridad y privacidad de la información.

Rector: Luis Alfonso Pérez Guerra

Documento preparado Por: Esp. Antonio Rafael Gallo Oñate

Contacto:
Email: contactenos@infotep.edu.co
www.infotep.edu.co
Telefax: +57 (5) 7740404 - 7740098
San Juan del Cesar, La Guajira - Colombia
INFOTEP, 2017
Actualización enero de 2021

Índice

1. Generalidades

1.1. Objetivos Estratégicos

Dotar a la Institución, de acuerdo con su Plan Estratégico, de un modelo organizativo e infraestructura tecnológica que contribuya a mejorar continuamente la eficiencia, la eficacia, el control, la continuidad y la seguridad de sus operaciones administrativas, de acuerdo con la norma de control interno.

Establecer los lineamientos para el desarrollo de los sistemas de información del INFOTEP para garantizar la adecuada administración de los recursos tecnológicos, infraestructura de datos y comunicaciones en la institución a la vez que su seguridad en la información.

Desarrollar capacidades orientadas a modernizar los procesos organizacionales básicos, la planificación, el control y la evaluación para mejorar continuamente el proceso de toma de decisiones institucionales.

Diseñar y desarrollar servicios basados en tecnología de información “web”, que permitan llevar los servicios institucionales a la mayor cantidad de usuarios del INFOTEP.

1.2. Glosario de términos.

Para efectos de la comprensión de los diferentes aspectos que consagra en la presente Política general de seguridad y privacidad de la información del Instituto Nacional de Formación Técnica Profesional, se establecen los siguientes significados de las palabras y expresiones empleadas en el texto:

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Ciberespacio: Ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701, Tomado de la Academia de la lengua Española).

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

Estándar: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la

implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Política: Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Procedimiento: Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia

para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la entidad, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro del a dependencia donde ellos se aplican.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

Parte interesada (Stakeholder): Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

1.3. Alcance/Aplicabilidad.

Este manual aplica a todos los colaboradores tanto de planta como contratistas sin excepción, que posean algún tipo de acceso o sean responsables por los activos de información, activos físicos, infraestructura física y recurso humano que se encuentre disponible en cualquier formato ya sea de manera digital, impresa, en medio audiovisual o archivados del Instituto Nacional de Formación Técnica Profesional.

.

1.4. Nivel de cumplimiento.

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

2. Descripción de la Política general de seguridad y privacidad de la información

La dirección del instituto Nacional de Formación Técnica Profesional de San Juan del Cesar, entendiendo la importancia de una adecuada gestión de la

información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para Instituto Nacional de Formación Técnica Profesional de San Juan del Cesar, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.

- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de El Instituto Nacional de Formación Técnica Profesional de San Juan del Cesar
- Garantizar la continuidad del negocio frente a incidentes.
- El Instituto Nacional de Formación Técnica Profesional de San Juan del Cesar ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

Finalmente es de gran ayuda incluir la descripción general de otras políticas relevantes para el cumplimiento de los Objetivos planteados dentro del proyecto del SGSI ya que éstas son el apoyo sobre el cual se desarrolla; éstas deben ser descritas de forma sencilla, puntual y muy efectiva.

Dentro de las temáticas que se tocan en este punto se encuentran por ejemplo la gestión de activos, seguridad física y ambiental, control de accesos, etc. Para abordar este punto es necesario remitirse a la “Guía de políticas específicas de seguridad y privacidad de la información” y mencionar aquellas que la Entidad haya establecido como necesarias y primordiales.

A continuación, se establecen 12 principios de seguridad que soportan el SGSI de El Instituto Nacional de Formación Técnica Profesional de San Juan del Cesar:

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los grupos de interés que forman parte de la institución.

- El Instituto Nacional de Formación Técnica Profesional de San Juan del Cesar protegerá la información generada, procesada o resguardada por los procesos institucionales, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.

- El Instituto Nacional de Formación Técnica Profesional de San Juan del Cesar protegerá la información creada, procesada, transmitida o resguardada por sus procesos institucionales, con el fin de minimizar

impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- El Instituto Nacional de Formación Técnica Profesional de San Juan del Cesar protegerá su información de las amenazas originadas por parte del personal.

- El Instituto Nacional de Formación Técnica Profesional de San Juan del Cesar protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

- El Instituto Nacional de Formación Técnica Profesional de San Juan del Cesar controlará la operación de sus procesos institucionales garantizando la seguridad de los recursos tecnológicos y las redes de datos.

- El Instituto Nacional de Formación Técnica Profesional de San Juan del Cesar implementará control de acceso a la información, sistemas y recursos de red.

- El Instituto Nacional de Formación Técnica Profesional de San Juan del Cesar garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

- El Instituto Nacional de Formación Técnica Profesional de San Juan del Cesar garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

- El Instituto Nacional de Formación Técnica Profesional de San Juan del Cesar garantizará la disponibilidad de sus procesos institucionales y la continuidad de su operación basada en el impacto que pueden generar los eventos.

- El Instituto Nacional de Formación Técnica Profesional de San Juan del Cesar garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

3. Procedimientos que apoyan la Política de Seguridad de la Información.

Los procedimientos son uno de los elementos dentro de la documentación del Manual de la Política de Seguridad para las Tecnologías de la Información y las comunicaciones. Un procedimiento describe de forma más detallada lo que se hace en las actividades de un proceso, en él se especifica cómo se deben desarrollar las actividades, cuáles son los recursos, el método y el objetivo que se pretende lograr o el valor agregado que genera y caracteriza el proceso.

Es recomendable el uso de instructivos para detallar aún más las tareas y acciones puntuales que se deben desarrollar dentro de un procedimiento, como son los instructivos de trabajo y de operación; los primeros para la ejecución de la tarea por la persona y los segundos para la manipulación o la operación de un equipo.

Los usuarios del INFOTEP pueden consultar las descripciones detalladas de cada procedimiento a través del sistema integrado de gestión SIGC o en el Área de Sistemas y comunicación de la Institución.

3.1. Gestión del programa de seguridad de la información

La gestión de la seguridad de la información dentro del INFOTEP puede dividirse en tres componentes de la siguiente manera:

- La dependencia de Sistemas y Comunicación es responsable de la dirección y liderazgo en Todos los aspectos de la seguridad de la información.

- Las dependencias que alojan servicios de datos son responsables de crear

Políticas y directrices para complementar, pero no contradecir las emitidas por el área de Sistemas y Comunicación.

- Todas las dependencias deben desarrollar procedimientos específicos para sus flujos de procesos para proteger la integridad de la información y protegerse contra la pérdida.

3.2. Uso personal de los equipos de computo

Los equipos de cómputo del IINFOTEP se proveen para actividades relacionadas con el trabajo. El INFOTEP proporciona apoyo en redes y recursos de información para sus diferentes procesos.

Todos los usuarios tienen acceso a computadoras para tareas relacionadas con el trabajo y este uso deben cumplir con las políticas del INFOTEP, así como las leyes que rigen el uso y la comunicación de la información.

La denegación de los privilegios de acceso puede dar lugar a acciones disciplinarias incluyendo el despido. Para los contratistas la cancelación del contrato.

La Política de seguridad de la información para el uso de la computadora prohíbe el uso de sus recursos para:

- Enviar correo electrónico usando la identidad de otra persona (falsificación de correo electrónico).

- Tome cualquier acción que a sabiendas interfiera con el funcionamiento normal de la red, sus sistemas, periféricos y / o acceso a redes externas.
- Instalar cualquier sistema o software en la red sin aprobación previa.
- Instalar cualquier sistema de software o hardware que instalará conscientemente un virus, Caballo de Troya, gusano o cualquier otro mecanismo destructivo conocido o desconocido.
- Intento de suplantación de IP.
- Intentar la descarga, publicación o difusión no autorizada de materiales protegidos por derechos de autor.
- Intentar cualquier descarga no autorizada de software desde Internet.
- Acceder, crear, transmitir (enviar o recibir), imprimir o descargar material que sea discriminatoria, despectiva, difamatoria, obscena, sexualmente explícita, ofensiva o hostigadora basada en género, raza, religión, nacionalidad, origen, ascendencia, edad, discapacidad, condición médica, orientación sexual o cualquier otro estado protegido por las leyes.

3.3. Uso de email

El correo electrónico (email) es una forma altamente eficiente que hace parte de los medios de comunicación modernos. Utilizado adecuadamente, el correo electrónico proporciona a los diferentes grupos de interés un medio para comunicarse facilitando los tiempos y traslado físico. Sin embargo, esta conveniencia también suele experimentar una desventaja muy conocida y denominada como Abuso de Internet. Los Uso incorrecto de esta tecnología de correo electrónico puede poner en peligro la integridad de los y niveles de servicio. El acceso al correo electrónico es una herramienta que proporciona a los usuarios apoyo para la realización de los trabajos y su uso no debe poner en peligro el funcionamiento del sistema o la reputación y / o la integridad del Instituto nacional de Formación Técnica Profesional.

Las cuentas de correo electrónico se ponen a disposición de todo el personal del INFOTEP que requiere el servicio para el desempeño de funciones relacionadas con el trabajo. Se aplican las siguientes declaraciones:

- ✓ Todo el correo electrónico y los recursos del sistema asociados son propiedad del INFOTEP.
- ✓ El correo electrónico está sujeto a las mismas restricciones sobre su uso y la misma revisión como cualquier otro recurso proporcionado por el

INFOTEP para el uso de los funcionarios. Su uso y contenido pueden ser monitoreados.

- ✓ El uso del correo electrónico debe ser capaz de soportar el escrutinio público. Los usuarios deben cumplir con toda la legislación, regulaciones, políticas y estándares aplicables. Esta Incluye el cumplimiento de las disposiciones sobre derechos de autor y licencias con respecto a tanto los programas como los datos.

- ✓ Si bien el correo electrónico se proporciona como una herramienta de estratégica para el INFOTEP a los funcionarios deben darle un uso razonable, el uso incidental para propósitos personales es aceptable. Este uso no debe, sin embargo, perjudican la productividad de los empleados, perturbar el sistema y/o dañar la reputación del INFOTEP.

Los Funcionarios del INFOTEP no pueden:

- ✓ Utilizar el correo electrónico para la solicitud comercial o para llevar a cabo intereses empresariales propios o de otra organización.

- ✓ Utilizar correo electrónico para distribuir documentos falsos, cartas en cadena o anuncios y/o amenazas.

- ✓ Utilizar el correo electrónico para distribuir material pornográfico.

- ✓ Utilizar el correo electrónico para enviar programas ejecutables o juegos.
- ✓ Utilizar el correo electrónico para enviar material potencialmente ofensivo.
- ✓ Propagar virus a sabiendas o maliciosamente.

Los usuarios no deben enviar y/o responder a cadenas no institucionales. Además, los usuarios deben considerar el impacto al crear y usar grandes listas de distribución relacionadas con el trabajo.

El correo electrónico es un registro y, por lo tanto, la gestión del mismo debe estar alineada a la legislación, regulaciones, políticas y estándares.

El presunto uso inapropiado de la tecnología de correo electrónico será revisado por dirección desde la oficina de sistemas y comunicación, caso por caso, y puede conducir a acciones disciplinarias. Con respecto a los contratistas, llevar a la cancelación del acuerdo contractual.

3.4. Seguridad de internet / Intranet

La World Wide Web (WWW) es un sistema para intercambiar información sobre la Internet. Una Intranet es una red propietaria que es específica para instituciones como INFOTEP, así como para el estado colombiano.

En el nivel más básico, la Web se puede dividir en dos componentes principales; Los servidores web, que son aplicaciones que ponen la información a Internet (en esencia publicar información) y navegadores web (clientes), que son para acceder y mostrar la información almacenada en los servidores Web. La web es el host más atacado en la red de la mayoría de las instituciones. Como resultado, es esencial asegurar los servidores web y la infraestructura de red que los apoya.

Las amenazas de seguridad específicas a los servidores Web generalmente se encuentran en una de las siguientes categorías:

- ✓ Las actividades maliciosas pueden explotar errores de software en el servidor Web, sistema operativo subyacente o contenido activo para obtener acceso al servidor Web. Ejemplos de acceso no autorizado están ganando acceso a archivos o carpetas que no estaban destinados a ser accesibles al público o la ejecución de comandos privilegiados y / o la instalación de software en la Web servidor.
- ✓ Los ataques de denegación de servicio pueden ser dirigidos al servidor web denegando a los usuarios la capacidad de utilizar el servidor Web durante la duración del ataque.
- ✓ La información sensible en el servidor Web puede ser distribuida a personas no autorizadas.

- ✓ Información sensible que no se cifra cuando se transmite entre el servidor Web y el navegador pueden ser interceptados.
- ✓ La información en el servidor Web se puede cambiar con fines maliciosos.
- ✓ Las actividades malintencionadas pueden obtener acceso no autorizado a otros recursos en la red informática de la organización a través de un ataque exitoso en la Web servidor.
- ✓ El servidor puede ser utilizado como un punto de distribución para software de copias ilegales herramientas de ataque, o pornografía, tal vez haciendo responsable a la institución de daños y perjuicios.

El servicio de alojamiento contratado por INFOTEP es responsable del servidor Web. Algunos ejemplos de controles para protegerse de acceso no autorizado o modificación son:

- ✓ Instalar o habilitar sólo los servicios necesarios.
- ✓ Instalar contenido Web en una unidad de disco duro o partición lógica dedicada.
- ✓ Limitar las cargas a los directorios que no son legibles por el servidor Web.
- ✓ Definir un directorio único para todos los scripts externos o programas ejecutados como parte del contenido web.
- ✓ Desactivar el uso de enlaces duros o simbólicos.

- ✓ Definir una matriz de acceso de contenido Web completa que identifica qué carpetas y los archivos dentro del directorio de documentos del servidor Web están restringidos y que sean accesibles (y por quién).
- ✓ Utilizar sistemas de detección de intrusiones basados en host y/o integridad de archivos checkers para detectar intrusiones y verificar el contenido web.

El mantenimiento de un servidor Web seguro es responsabilidad de la empresa contratada por el INFOTEP “hosting” e implica las siguientes etapas:

- ✓ Configurar, proteger y analizar archivos de registro.
- ✓ Copias de seguridad de información crítica con frecuencia.
- ✓ Mantener una copia protegida y autorizada de la Web de la organización
- ✓ Contenido.
- ✓ Establecer y seguir procedimientos para recuperar de compromiso.
- ✓ Probar y aplicar parches de manera oportuna.
- ✓ Probar la seguridad periódicamente.

La empresa contratada para el hosting es responsable de la seguridad de Internet:

- ✓ Mantener actualizados los sistemas operativos y el software de aplicaciones. Debido a que los sistemas de software son tan complejos, es común que problemas que se descubren sólo después de que el software s

ha utilizado. Aunque la mayoría de los vendedores tratan de resolver las fallas de seguridad conocidas de manera oportuna, normalmente hay una brecha el problema es conocido públicamente, el tiempo que el vendedor requiere para preparar correcciones y la hora de instalar la actualización. Esta brecha proporciona la oportunidad a intrusos para montar un ataque dentro de las redes o computadoras. Para mantener este intervalo de tiempo tan corto como posible, es necesario estar al tanto de:

a) Anunciar los problemas relacionados con la seguridad que puedan aplicarse.

b) Tomar las medidas inmediatas para reducir la exposición a la vulnerabilidad, como la desactivación del software afectado.

c) Actualizaciones permanentes de proveedores.

✓ Restringir sólo los servicios de red esenciales y el sistema operativo en el host servidor.

✓ Asegurar que solo el conjunto de servicios requerido y aplicaciones sean instaladas en el servidor host. No instalar servicios innecesarios o desactivar los mismos desde el host.

✓ Configurar equipos para la copia de seguridad de archivos.

✓ Proteger las computadoras contra virus y amenazas programadas.

✓ Permitir sólo el acceso físico adecuado a las computadoras.

✓ Diseñar, implementar y monitorear un sistema de cortafuegos efectivo.

3.5. Gestión de Soporte técnico

Un servicio de ayuda o soporte técnico se caracteriza por la capacidad de respuesta, el conocimiento, la retroalimentación y mejora. La velocidad a la que se resuelven los problemas, el número de solicitudes el primer nivel de apoyo, el seguimiento con la comunidad de usuarios sobre el estado, la seguridad y el seguimiento del desempeño con el objetivo de mejorar son las características que separan una misión progresista y segura operación.

Las funciones del soporte Técnico deben incluir:

- ✓ Adhesión a todas las políticas y procedimientos publicados.
- ✓ Recomendación de nuevos y/o cambios en las políticas y procedimientos.
- ✓ Propiedad de todas atenciones hasta ser reasignadas o enrutadas a los contratistas.
- ✓ El rendimiento de todas las tareas de primera línea tales como restablecimientos de contraseña, restablecimientos de impresora, etc.
- ✓ Encaminamiento del sistema o consultas técnicas al líder del proceso de Sistemas y Comunicación.
- ✓ Informar y monitorear las solicitudes de atención.

- ✓ Notificación y escalada de todos los incidentes de actividad sospechosa o violaciones de la seguridad.

Se debe emplear un entorno de firewall para realizar las siguientes funciones:

- ✓ Paquetes de filtros y protocolos.
- ✓ Realizar la inspección de las conexiones.
- ✓ Realizar operaciones proxy o aplicaciones seleccionadas.
- ✓ Supervisar el tráfico permitido o negado por el cortafuego.
- ✓ Proporcionar autenticación a los usuarios utilizando una forma de autenticación que no se basan en contraseñas estáticas y reutilizables.

3.6. Restablecimiento de credenciales o contraseña

Los restablecimientos de contraseña son responsabilidad del área que administra el servicio. Las identidades de los solicitantes serán verificadas confirmado los datos del usuario y registrándolo mediante formato establecido por dicha área.

Es responsabilidad del solicitante, al solicitar una contraseña para confirmar su identidad. Esto puede lograrse mediante:

- ✓ Proporcionar su nombre e identificación.

- ✓ Responder a una pregunta y una respuesta únicas presentadas al registrarse, tales como: Lugar de nacimiento, apellido de soltera de la madre, etc.).
- ✓ Número de teléfono

Las responsabilidades de los servicios contratados por el INFOTEP ante entidades externas son:

- ✓ Confirme la identidad del solicitante.
- ✓ Informar toda la actividad sospechosa al administrador de seguridad inmediatamente. Discrepancias en las respuestas, incapacidad para proporcionar la ID de usuario, solicitudes frecuentes de cambios en el mismo ID de usuario.
- ✓ Restablecer la contraseña.
- ✓ Registro de detalles de la llamada.
- ✓ Confirmar el restablecimiento de la contraseña al usuario registrado en el ID de usuario por correo electrónico.
- ✓ Informar la actividad mensualmente al INFOTEP.

3.6. Seguridad física y medioambiental.

El INFOTEP por medio del área de Sistemas y Comunicación, tiene la responsabilidad de la documentación, ejecución, seguimiento y pruebas de un

plan de seguridad física para computadoras y equipos de comunicación. Este plan de seguridad física evaluaría los riesgos de posibles pérdidas debido a:

- ✓ Destrucción física o el robo de activos físicos,
- ✓ Pérdida o destrucción de información y archivos de programas,
- ✓ Robo de información.
- ✓ Robo de activos indirectos.
- ✓ Demora o prevención del procesamiento informático.

Se incluirían en el plan medidas para reducir la posibilidad de una pérdida y debe atender:

- ✓ Los cambios en el medio ambiente para reducir la exposición.
- ✓ Medidas para reducir el efecto de una amenaza.
- ✓ Procedimientos de control mejorados.
- ✓ Detección precoz.
- ✓ Planes de contingencia.

A continuación, figuran las directrices de los puntos de acción para establecer, aplicar y Mantener un programa de seguridad física en el INFOTEP:

- ✓ Realizar un análisis de riesgo.
- ✓ Determinar las probabilidades locales de desastres naturales.
- ✓ Proteger las utilidades de apoyo.

- ✓ Garantizar la fiabilidad informática.
- ✓ Proporcionar protección física.
- ✓ Implementar la seguridad procesal.
- ✓ Plan para contingencias,
- ✓ Desarrollar conciencia de seguridad, y
- ✓ Validar el programa.

3.7. Backup de la Información.

Se deben tomar copias de seguridad de información institucional y software esencial regularmente. Se deben proporcionar instalaciones de respaldo adecuadas para garantizar que la información y el software puedan recuperarse después de un desastre o evento. Los sistemas de respaldo deberan someterse a asegurarse de que cumplen con los requisitos de los planes de continuidad. El seguimiento y los controles deben ser considerados:

- ✓ Un nivel mínimo de información de respaldo, junto con información, registros completos de las copias de respaldo y la restauración documentada de los procedimientos, deben almacenarse en una ubicación remota a una distancia para evitar un daño causado por desastre en la sede física del INFOTEP. Al menos tres ciclos de respaldo de información deben conservarse.

- ✓ La información de respaldo debe tener un nivel adecuado de protección del medio ambiente compatible con las normas aplicadas dentro del INFOTEP.
- ✓ Los medios de respaldo deben ser probados regularmente, donde sea factible, para asegurar que puedan ser confiados para uso de emergencia cuando sea necesario.
- ✓ Los procedimientos de restauración deben ser verificados y probados regularmente para verificar si son eficaces y que pueden ser completados en el tiempo asignados dentro de los procedimientos operativos de recuperación.
- ✓ El período de retención de información esencial de la empresa y también los requisitos para que las copias archivadas permanezcan permanentemente.

3.8. Control de acceso.

Se requieren controles de acceso lógicos y físicos para asegurar la información y los bienes físicos.

Se deben implementar las siguientes directrices para controlar el acceso lógico dentro del INFOTEP:

- ✓ Documentar y adherirse a procedimientos para otorgar, modificar y revocar Acceso.
- ✓ Instalar mecanismos de detección para intentos de acceso no autorizados.

- ✓ Tiempo de espera de una sesión después de 15 minutos de inactividad.
- ✓ Revocar el acceso después de un período de inactividad de 60 días.

Las directrices de control de acceso físico para el INFOTEP incluyen:

- ✓ Todos los equipos de telecomunicaciones e informáticos que se encuentren asegurados, y en ambiente cerrado.
- ✓ Los códigos de acceso para entornos seguros deben ser cambiados al menos cada 60 días o en el caso de un funcionario que salga de la institución que previamente tenía acceso.
- ✓ Contabilizar todas las claves emitidas para las instalaciones que utilizan este método.
- ✓ Reemplazar el mecanismo de bloqueo cuando falta una llave.
- ✓ Cuando el sistema lo permita, registrar todos los accesos y retener.
- ✓ Asegurar todos los periféricos tales como aire acondicionado, generadores, etc.

3.9. Redes.

Las conexiones no seguras a los servicios de red pueden afectar a toda la Institución. Los usuarios sólo deben tener acceso directo a los servicios que han sido específicamente autorizados. Este control es particularmente importante para las conexiones de red y a aplicaciones sensibles o críticas.

Los procedimientos relativos a la utilización de redes y servicios de red deberán abarcar:

- ✓ Las redes y servicios de red a los que se puede acceder.
- ✓ Procedimientos de autorización para determinar a quién se le permite acceder, qué redes y que servicios dentro de la red.
- ✓ Controles de gestión y procedimientos para proteger el acceso a conexiones y servicios de red.

La ruta del terminal de usuario al servicio informático debe ser controlada. Las redes están diseñadas para permitir el máximo alcance para un intercambio de recursos y flexibilidad de enrutamiento. Estas características permiten mitigar el acceso no autorizado a aplicaciones. Incorporar controles que restrinjan la ruta entre un terminal de usuario y los servicios informáticos a los que su usuario está autorizado a acceder. La creación de un camino forzado puede reducir tales riesgos.

Se deben implementar los siguientes métodos para limitar la ruta a un servicio:

- ✓ Asignar líneas o números de teléfono dedicados,
- ✓ Conexión automática de puertos a sistemas de aplicación especificados o pasarelas de seguridad.
- ✓ Limitar opciones de menú y submenú para usuarios individuales.

- ✓ Prevenir la itinerancia ilimitada de la red.
- ✓ Hacer cumplir el uso de sistemas de aplicación especificados y/o seguridad Gateways para usuarios de redes externas.
- ✓ Controlar activamente las comunicaciones de origen a destino vía pasarelas de seguridad. Firewalls.
- ✓ Restringir el acceso a la red estableciendo dominios lógicos separados por redes privadas virtuales, para los diferentes grupos de usuarios dentro del INFOTEP.

Las conexiones externas proporcionan un potencial de acceso no autorizado a Información. Por lo tanto, el acceso de usuarios remotos debe ser objeto de autenticación. Hay diferentes tipos de autenticación, algunos de estos proporcionan un mayor nivel de protección que otros. Métodos basados en el uso de técnicas criptográficas pueden proporcionar autenticación. Es importante determinar a partir de una evaluación de riesgos el Protección requerida. Esto es necesario para la selección apropiada de un método de autentificación. La autenticación de los usuarios remotos debe lograrse utilizando uno de las siguientes técnicas:

- Una técnica basada en criptografía,
- Fichas de hardware.
- Un protocolo de respuesta / respuesta.

- Líneas privadas dedicadas o una verificación de dirección de usuario de red.
- Procedimientos de devolución de llamada

Las redes se están extendiendo cada vez más y pueden requerir la Interconexión o intercambio de instalaciones de procesamiento de información y escalamiento de las mismas. Estas ampliaciones aumentarán el riesgo de acceso no autorizado a sistemas de información que utiliza el INFOTEP. En tales circunstancias, se deben introducir controles en las redes para segregar a los grupos de servicios de información, usuarios y sistemas de información.

La seguridad de las grandes redes debe controlarse dividiéndolas en dominios de red lógicos separados. Dominios de una red interna y dominios de red externas, cada uno protegido por un perímetro de seguridad definido. Este perímetro debe implementarse instalando una pasarela segura entre las dos redes a interconectarse para controlar el acceso y el flujo de información entre los dos dominios. Esta puerta de enlace debe configurarse para filtrar el tráfico entre estos dominios y bloquear el acceso no autorizado de acuerdo con el procedimiento de control de acceso del INFOTEP. Los criterios de segregación de redes deben basarse en los procedimientos de control de acceso y tener en cuenta el impacto relativo del costo y del rendimiento de los incorporados dentro del enrutamiento de red adecuado.

Estos controles deben implementarse a través de pasarelas de red que filtran el tráfico por medio de tablas o reglas predefinidas. Las restricciones aplicadas deben ser sobre los procedimientos y requisitos de acceso de las aplicaciones las cuales deben mantenerse actualizarse. Las aplicaciones para restricciones que deben aplicarse son:

- Correo electrónico.
- Transferencia de archivos unidireccional, en ambos sentidos de transferencia de archivos.
- Acceso interactivo.
- Acceso a la red vinculado a la hora del día o la fecha.

Las redes compartidas deben tener controles de enrutamiento para asegurar que las conexiones de la computadora y los flujos de información no infrinjan los procedimientos de control de acceso de aplicaciones. Este control es esencial para las redes compartidas con terceros.

Los controles de enrutamiento deben basarse en una dirección de origen y de destino positiva. La traducción de direcciones de red también es muy útil. Los mecanismos para aislar las redes y evitar que las rutas se propaguen desde la red. Ellos pueden ser Implementados en software o hardware. Los implementadores deben ser conscientes a la fuerza de los mecanismos

desplegados. Los servicios de red pueden tener características de seguridad únicas o complejas.

3.10. Instalaciones externas.

El tratamiento de las comunicaciones por medio de contratistas puede introducir posibles exposiciones a la seguridad, como la posibilidad de compromiso, daño o pérdida de datos.

Antes de utilizar instalaciones externas, se deben identificar los riesgos y controles acordados con el contratista e incorporados en el contrato. Especial en los temas que deben ser abordados incluyen:

- ✓ Identificación de aplicaciones sensibles o críticas mejor retenidas internamente.
- ✓ Obtener la aprobación de los propietarios de aplicaciones.
- ✓ Implicaciones para planes de continuidad de negocio.
- ✓ Normas de seguridad a especificar y el proceso para medir la conformidad.
- ✓ Asignación de responsabilidades y procedimientos específicos para supervisar todas las actividades de seguridad pertinentes.
- ✓ Responsabilidades y procedimientos para reportar y manejar incidentes de seguridad

3.11. Continuidad del negocio.

Las instalaciones y sistemas de tecnología de la información son vulnerables a Interrupciones, algunas de las cuales son de corto plazo (medidas en minutos y horas) y otras duran un día o más. La intención de Planificación de Continuidad de Negocios es estar alerta y listo para sostener los procesos de una organización durante y después de una perturbación imprevista de los servicios causada por los desastres o fallas de seguridad.

La continuidad del negocio debe comenzar identificando eventos que pueden causar interrupciones a procesos del INFOTEP, fallas de equipos, inundaciones e incendios entre otros. Esto debería ser seguida de una evaluación del riesgo para determinar el impacto de esas interrupciones (Tanto en términos de magnitud como de tiempo de recuperación). Ambas actividades deben llevarse a cabo con la plena participación de los propietarios de los recursos empresariales y los procesos. Esta evaluación considera todos los procesos de negocio, y no está limitado a las instalaciones de procesamiento de la información.

Debe elaborarse un plan estratégico basado en una evaluación de riesgos apropiada para el enfoque general de la continuidad del negocio.

En el caso de una interrupción que se extienda más allá de un período de tiempo determinado. El largo del período de tiempo puede variar con el sistema o

la instalación involucrados. El procedimiento para la ejecución de tal capacidad será documentado en una contingencia formal o plan, ser revisado anualmente y actualizado según sea necesario.

Los procedimientos deben tener en cuenta las copias de seguridad diarias diferenciales y las copias de seguridad que se llevarán a cabo y enviará a una instalación fuera del sitio designada. Además, los planes deben asignar responsabilidades específicas al personal o cargos designados para facilitar la recuperación y/o la continuidad de las funciones esenciales de TI.

La gestión de la continuidad del negocio debería incluir controles para identificar los riesgos, limitar las consecuencias de los incidentes dañinos y garantizar la reanudación de operaciones esenciales.

3.12. Plan de recuperación ante desastres.

Un Plan de Recuperación de Desastres está destinado a mantener los procesos críticos ante el evento por la pérdida de cualquiera de las siguientes áreas durante un período prolongado de tiempo:

- ✓ Computadoras de escritorio y sistemas portátiles.
- ✓ Servidores.
- ✓ Sitios Web.

- ✓ Redes de área local.
- ✓ Redes de área amplia.
- ✓ Sistemas distribuidos.
- ✓ Sistemas mainframe.

Se deben formar equipos para abordar cada una de las áreas indicadas, así como personal de conocimientos claves dentro de áreas en particular. Toda la información de contacto debe estar disponible para la administración de TI, el personal de TI y la dirección del INFOTEP, esta información debe incluir:

- ✓ Número de teléfono de trabajo.
- ✓ Número de buscapersonas.
- ✓ Número de teléfono de la casa.
- ✓ Número de teléfono celular.
- ✓ Dirección de correo electrónico del trabajo.
- ✓ Dirección de correo electrónico de inicio.
- ✓ Dirección del domicilio.

Las comunicaciones a la dependencia de sistemas son responsabilidad de los líderes de proceso. Respecto a las comunicaciones externas, es sumamente importante que existe un único punto de divulgación para garantizar la exactitud y las actualizaciones. Los siguientes roles e individuos deben ser determinados y documentados:

- ✓ Hacia arriba, dentro de la organización del organismo afectado.
- ✓ Fuera hacia las agencias afectadas.
- ✓ Fuera al público.

Las copias del Plan deben ser:

- ✓ Almacenado fuera del sitio en un lugar seguro.
- ✓ Almacenados en la residencia personal de los conductores del equipo.
- ✓ Almacenados en la residencia personal de todos los gerentes y líderes de proceso.
- ✓ Almacenados en un sitio web seguro

3.13. Estrategia de Recuperación del negocio.

Una Estrategia de Recuperación de empresas proporciona el plan organizativo documentado para restaurar la funcionalidad empresarial completa de la forma más rápida y rentable posible. La estrategia de recuperación se inicia tan pronto como se considerada capaz de reanudar operaciones normales después de un desastre.

La Estrategia de Recuperación debe incluir la planificación anticipada y los preparativos para recuperarse de circunstancias externas. La estrategia de recuperación debe ser creada, implementada, probada y mantenida para asegurar la restauración de los servicios del INFOTEP en caso de interrupción.

Un "peor escenario" debe ser la base para desarrollar el plan, donde el peor de los casos el escenario es la destrucción de la instalación principal o primaria, teniendo en cuanta que el plan se basa en esta premisa, las situaciones menos críticas se pueden manejar usando subconjuntos del plan, con modificaciones menores (si es necesario). Recuperación o la mitigación de un escenario no debe considerarse una proposición de todo o nada.

Los objetivos específicos de la estrategia de recuperación deben incluir:

- ✓ Objetivos completos de recuperación de la funcionalidad del servicio, en etapas, por retraso, duración y grado.
- ✓ Detalles de los procesos ya existentes para recuperarse de un incidente.
- ✓ En qué período de tiempo se espera que el proceso existente restablezca el servicio.
- ✓ Requisitos para pasar de los procesos existentes a procesos suficientes.
- ✓ Plazo para obtener recursos adicionales.

La Estrategia de Recuperación del INFOTEP debe incluir información detallada, paso a paso, instrucciones para cómo reemplazar / restaurar lo siguiente, en la secuencia apropiada:

- ✓ Aplicaciones / Procesos
- ✓ Funcionalidad / Capacidad
- ✓ Equipo / Infraestructura

- ✓ Personal / Habilidades
- ✓ Duración / retraso de ejecución
- ✓ Conectividad / Red
- ✓ Fuentes de datos
- ✓ Instalaciones / Servicios / Locales físicos
- ✓ Transporte
- ✓ Documentación / Material de referencia

3.14. Gestión del centro de datos.

Relacionado específicamente con la seguridad de la información y la gestión de centros de ritmo de cambio, la realidad de la World Wide Web y el creciente número de los portales internos y externos exigen un monitoreo constante con estrategias defensivas.

Procedimientos de funcionamiento

- ✓ Los procedimientos operativos identificados por los procedimientos de seguridad deben documentarse y mantenido los procedimientos operativos deben tratarse como documentos formales y cambios autorizados por la administración.
- ✓ Los procedimientos deben especificar las instrucciones para la ejecución detallada Incluyendo los siguientes:

a) Procesamiento y manejo de información.

b) Requisitos de programación, incluyendo interdependencias con otros sistemas.

c) Instrucciones para manejar errores u otras condiciones excepcionales, que podrían resultar durante la ejecución del trabajo, incluidas las restricciones sobre el uso de utilidades.

d) Los contactos de apoyo y de propietario en caso de dificultades técnicas.

e) Instrucciones especiales de manejo de salida, tales como el uso de papelería especial.

f) La gestión de la producción confidencial, incluidos los procedimientos de eliminación de la producción de los trabajos fallidos.

g) Procedimientos de reinicio y recuperación del sistema para su uso en caso de fracaso.

Procedimientos documentados también deben ser preparados para la limpieza del sistema, actividades relacionadas con el procesamiento de la información y las instalaciones de comunicación, tales como los procedimientos de puesta en marcha y cierre de la computadora, respaldo, mantenimiento, manejo de sala de computadoras y manejo de correo entre otros.

3.15. Operación para el control de Cambios.

Los cambios en las instalaciones y sistemas de procesamiento de deben ser revisados. El control inadecuado de los cambios en las instalaciones de procesamiento es una causa común de fallas en el sistema o en la seguridad. La gestión formal debe establecer responsabilidades y procedimientos para garantizar un control de todos los cambios en equipos, software o procedimientos.

Los programas operativos deberían someterse a un estricto control de los cambios. Los procedimientos operativos y de control del cambio de la, se deben implementar los siguientes controles:

- ✓ Identificación y registro de cambios significativos.
- ✓ Evaluación del impacto potencial de tales cambios.
- ✓ Procedimiento formal de aprobación de los cambios propuestos.
- ✓ Comunicación de los detalles del cambio a todas las personas pertinentes.
- ✓ Procedimientos que identifican responsabilidades para abortar y recuperar los cambios fallidos.

3.16. Planificación y Aceptación de Sistemas.

Para minimizar el riesgo de falla del sistema:

- ✓ Se requiere una planificación y preparación anticipadas para asegurar la disponibilidad de capacidad y recursos adecuados.

- ✓ Deberían hacerse proyecciones de los requisitos de capacidad futura, para el riesgo de sobrecarga del sistema.
- ✓ Las necesidades operacionales de los nuevos sistemas establecidos, documentados y probados antes de su aceptación y uso.

3.17. Aceptación de Sistemas.

Los criterios de aceptación de nuevos sistemas de información, actualizaciones y nuevas versiones deben establecerse y las pruebas adecuadas del sistema realizadas antes de la aceptación. Los líderes de procesos deben asegurar que los requisitos y criterios para la aceptación de nuevos sistemas, que estén claramente definidos, acordados y probados.

Deben considerarse los siguientes controles:

- ✓ Los requisitos de rendimiento y capacidad informática.
- ✓ Procedimientos de recuperación de errores y planes de contingencia.
- ✓ Preparación y prueba de procedimientos operativos de rutina a normas.
- ✓ Conjunto acordado de controles de seguridad en su lugar.
- ✓ Procedimientos manuales efectivos.

- ✓ Acuerdos de continuidad de negocio según sea necesario.
- ✓ Pruebas de que la instalación del nuevo sistema no afectará negativamente los sistemas existentes, particularmente en los tiempos de procesamiento máximo.
- ✓ Evidencia de que se ha considerado el efecto del nuevo sistema dentro de la Institución.
- ✓ Capacitación en el funcionamiento o uso de nuevos sistemas.

Para los nuevos desarrollos, la el apoyo y seguimiento en todas las etapas del proceso son fundamentales para garantizar la eficiencia del diseño del sistema propuesto. Deben llevarse a cabo pruebas apropiadas para confirmar que todos los criterios de aceptación están plenamente satisfechos.

3.18. Operaciones y Registro de Fallas.

El personal operativo debe mantener un registro de sus actividades. Los registros apropiados deben incluir:

- ✓ Los tiempos de inicio y final del sistema.
- ✓ Los errores del sistema y las medidas correctivas adoptadas.

- ✓ La confirmación del manejo correcto de los archivos de datos y la salida de la computadora.
- ✓ El nombre de la persona que hace la entrada del registro.

Se deben reportar fallas y tomar medidas correctivas. Fallos reportados por los usuarios, Problemas de procesamiento de información o de sistemas de comunicaciones. Debe haber reglas claras para manejar los fallos reportados incluso:

- ✓ Revisión de registros de fallas para asegurar que las fallas han sido resueltas satisfactoriamente.
- ✓ Revisión de las medidas correctivas para asegurar que los controles no se han comprometido y que las medidas adoptadas están plenamente autorizadas.

3.19. Gestión de medios removibles.

Dentro del procedimiento operativos apropiados para proteger los documentos, medios informáticos (cintas, discos, cassettes, etc.), datos de entrada / salida y documentación ante daños, robo y acceso no autorizado. El seguimiento debe seguirse bajo los siguientes procedimientos:

- ✓ Si ya no es necesario, el contenido anterior de cualquier medio reutilizable debe ser removido o borrado.
- ✓ Debe exigirse autorización para todos los medios eliminados del INFOTEP un registro de todas esas remociones mantenidas.
- ✓ Todos los medios deben almacenarse en un ambiente seguro y si es el caso con las especificaciones de los fabricantes.
- ✓ Todos los procedimientos y niveles de autorización deben estar claramente documentados.

3.20. Eliminación de medios.

Para la eliminación segura de los medios y con la finalidad de minimizar este riesgo. Se deben considerar los siguientes controles:

- ✓ Los medios que contengan información sensible deberán eliminarse de manera segura por medio de incineración, trituración o vaciado de Información para evitar su uso o acceso.
- ✓ La siguiente lista identifica los elementos que pueden requerir una eliminación segura:

a) Documentos en papel.

b) Grabaciones de voz u otras grabaciones,

c) Informes de producción.

d) Cintas de impresora de uso único.

e) Cintas magnéticas.

f) Discos o casetes desmontables.

g) Soportes de almacenamiento ópticos (todos los formularios e incluyendo todos los fabricantes.

h) Medios de distribución de software.

i) Listados de programas.

j) Información de prueba.

k) Documentación del sistema.

La eliminación de artículos sensibles debe ser registrada donde sea posible para mantener una pista de auditoría. La eliminación de ciertos equipos debe ajustarse a los requisitos u otra legislación pertinente vigente.

3.21. Intercambio de Información y de Software.

Los intercambios de información y software entre instituciones deberían ser controlados y deben cumplir con cualquier legislación pertinente.

Los intercambios deben realizarse sobre la base de acuerdos, procedimientos y se deben establecer normas para proteger la información y los medios en tránsito. En las implicaciones comerciales y de seguridad asociadas con el intercambio electrónico de datos, el comercio electrónico, el correo electrónico y los requisitos para los controles deben ser considerados.

Los acuerdos sobre condiciones de seguridad deben incluir:

- ✓ Las responsabilidades de controlar y notificar la transmisión, expedición y recibo.
- ✓ Procedimientos para notificar al remitente, transmisión, despacho y recepción.
- ✓ Normas técnicas mínimas para el embalaje y la transmisión,
- ✓ Normas de identificación de mensajería.
- ✓ Responsabilidades en caso de pérdida de información.
- ✓ La propiedad de información y software y las responsabilidades de dicha información.

- ✓ Protección, cumplimiento de derechos de autor de software y consideraciones similares.
- ✓ Las normas técnicas para el registro y lectura de información de software.
- ✓ Cualquier control especial que pueda ser requerido para proteger artículos sensibles tales como criptografía.

La información puede ser vulnerable al acceso, uso indebido o corrupción no autorizados, durante el transporte físico, por ejemplo, cuando se envían medios a través del servicio postal o el mensajero. Por lo tanto, los medios que se transportan deben protegerse del acceso no autorizado, mal uso o corrupción.

3.22. Sobre los sistemas Públicamente disponibles.

La Información sobre un sistema disponible públicamente, deben de cumplir con las leyes, reglamentos. Debe ser un proceso formal de autorización antes de que la información se haga pública. Debe ser protegida para modificación no autorizada.

Software, datos y otra información que requiera un alto nivel de integridad, disponibles en un sistema público, deberían ser protegidos por mecanismos digitales como firmas, especialmente aquellos que permiten la retroalimentación y

la introducción directa de información, deben ser cuidadosamente controlados de manera que:

- ✓ La información se obtiene de conformidad con cualquier legislación.
- ✓ La entrada de información registrada ante el sistema de publicación será procesada de manera completa, precisa y oportuna.
- ✓ La información sensible será protegida durante el proceso de recolección y
- ✓ Cuando se almacena, el acceso al sistema de publicación no permite el acceso no deseado a redes que no hacen parte del segmento de red.

3.22. Sobre los sistemas de monitoreo y acceso público.

Los sistemas deben ser monitoreados para detectar desviaciones de los procedimientos de control de acceso y registrar los eventos del sistema para proporcionar evidencia en caso de incidentes de seguridad. La supervisión del sistema permite comprobar la eficacia de los controles adoptados.

Los registros de auditoría que registran excepciones y otros eventos relevantes para la seguridad deben ser producidos y conservados durante un período definido por el INFOTEP y dentro de lo establecido por la ley para ayudar en futuras investigaciones y monitorización del control. Los registros de auditoría también deben incluir:

- ✓ ID de usuario,
- ✓ Las fechas y horas para el inicio de sesión y la desconexión,
- ✓ Identidad terminal o ubicación si es posible,
- ✓ Registros de intentos de acceso al sistema que hayan tenido éxito y rechazados, y
- ✓ Registros de datos exitosos y rechazados y otro acceso a recursos intentos

Los procedimientos para monitorear el uso de las instalaciones de procesamiento y el resultado de las actividades de monitoreo revisadas regularmente. Tal procedimientos necesarios para garantizar que los usuarios sólo realizan actividades han sido explícitamente autorizados. El nivel de monitoreo requerido para las instalaciones deben determinarse mediante una evaluación del riesgo. Áreas que deben ser incluidos son:

- ✓ Acceso autorizado, incluyendo detalles tales como:
- ✓ El ID de usuario,
- ✓ la fecha y hora de los eventos clave,
- ✓ Los tipos de eventos,
- ✓ Los archivos a los que se accede, y

- ✓ El programa / utilidades utilizadas.
- ✓ Todas las operaciones privilegiadas, tales como:
- ✓ Uso de la cuenta de supervisor,
- ✓ Puesta en marcha y parada del sistema.
- ✓ Conexión / desacoplamiento del dispositivo de E / S.
- ✓ Intentos de acceso no autorizados, tales como:

a) Intentos fallidos,

b) Infracciones de procedimientos de acceso y notificaciones para pasarelas de red y firewalls.

c) Alertas de los sistemas propietarios de detección de intrusiones.

d) Alertas del sistema o fallas tales como consola de alertas o mensajes, excepciones de registro del sistema, y alarmas de gestión de red

3.23. Control de cambios.

La aplicación de los cambios debe ser estrictamente controlada por el uso de cambiar procedimientos de control para minimizar el riesgo de corrupción del sistema. Estos controles de cambios formalizados deben ser forzados. Deben

garantizar que los procedimientos de control no se ven comprometidos, que los programadores tienen acceso a sólo aquellas unidades requeridas para su trabajo y que se obtienen aprobaciones formales.

El cambio del software de aplicación puede afectar el entorno operativo. Cuando se deberían integrar los procedimientos prácticos, de aplicación y de cambio operacional. Estos procesos deben incluir:

- ✓ Mantener un registro de los niveles acordados de autorización.
- ✓ Asegurar que los cambios sean presentados por personal autorizado.
- ✓ Revisar los controles y procedimientos para asegurar que no se verán comprometidos por los cambios presentados.
- ✓ Identificar todo el software, las bases de datos y el hardware que requieran cambio.
- ✓ Obtener la aprobación formal antes de que comience el trabajo.
- ✓ Asegurar que los cambios se realicen para minimizar cualquier posible interrupción.
- ✓ Garantizar que la documentación del sistema esté actualizada.
- ✓ Mantener el control de versiones en todas las actualizaciones.

- ✓ Mantener una pista de auditoría de todas las solicitudes de cambio.
- ✓ Garantizar que la documentación operacional y los procedimientos del nuevo entorno.
- ✓ Asegurar que los cambios se implementen sin interrupción de negocios.

3.24. Controles de Software Malicioso.

Los Controles de detección y prevención para proteger contra software malicioso se deben implementar para la toma de concienciación del usuario. Contra el software malicioso debe basarse en la conciencia de seguridad, el acceso adecuado al sistema y los controles de gestión del cambio. Los Procedimientos que deben ser implementados:

- ✓ El cumplimiento de las licencias de software y la prohibición del uso de Software no autorizado.
- ✓ Protección contra los riesgos asociados con la obtención de archivos y software a través de redes externas o en cualquier otro medio, indicando qué deben adoptarse medidas de protección,
- ✓ Instalación y actualización periódica del software de detección y reparación de escanear computadoras y medios como un control preventivo o en una rutina base.

- ✓ Revisiones regulares del software y del contenido de información de los sistemas: la presencia de cualquier archivo o ingreso no autorizado deben ser formalmente investigados.
- ✓ Verificación de archivos en medios electrónicos de origen incierto o no autorizado, o archivos recibidos sobre redes no confiables.
- ✓ Verificación de cualquier archivo adjunto de correo electrónico y Software malicioso antes de su uso.
- ✓ Asignación de responsabilidades para tratar la protección antivirus en sistemas, entrenamiento en su uso, reportes y recuperación de ataques de virus.
- ✓ Planes apropiados para recuperarse de ataques de virus, incluidos todos los datos necesarios y las disposiciones de respaldo y recuperación de software,
- ✓ Verificación de toda la información relacionada con el software malicioso.

3.25. Protección de la Información.

Los registros del INFOTEP deben protegerse ante la posible pérdida, destrucción y falsificación. Algunos registros pueden necesitar ser retenidos de

manera segura para cumplir con los requisitos legales, así como para apoyar las actividades esenciales.

El sistema de almacenamiento y manipulación debe garantizar una clara identificación de su período de retención reglamentario. Debe permitir destrucción de registros después de ese período si no son necesarios por el INFOTEP.

Para cumplir con estas obligaciones, se deben tomar las siguientes medidas:

- ✓ Establecerse directrices sobre la retención, almacenamiento, manipulación y eliminación de registros e información.
- ✓ Establecerse un calendario de retención que identifique los tipos de registro el período de tiempo durante el cual deben ser retenidos.
- ✓ Mantenerse un inventario de fuentes de información clave.
- ✓ Implementarse controles apropiados para proteger los registros e información de pérdida, destrucción y falsificación.

4. Divulgación del manual de seguridad y privacidad de la información

El manual de seguridad y privacidad de la información se divulga a los miembros de la Entidad y a sus grupos de interés utilizando documentos electrónicos y portal web.

5. Vigencia del manual de seguridad y privacidad de la información

El presente manual de seguridad y privacidad de la información entra en vigencia a partir su aprobación por parte del rector del Instituto Nacional de Formación Técnica Profesional INFOTEP.

Dado en San Juan del Cesar, a los once (11) días del mes de enero de 2021

LUIS ALFONSO PEREZ GUERRA
RECTOR

Referencia Bibliográfica

MINTIC. (2010). ***Modelo de Seguridad y Privacidad de la Información.*** Recuperado el 09 de agosto de 2016 del sitio web: http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_Seguridad.pdf

MINTIC. (2010). ***Guía 5: Política general MSPI v1.*** Recuperado el 09 de agosto de 2016 del sitio web: http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_Seguridad.pdf