2021

Manual del MSPI y Línea Base de Seguridad de Información

INSTITUCIÓN UNIVERSITARIA DE ENVIGADO

VERSIÓN EN REVISIÒN
FECHA: 12/12/2021

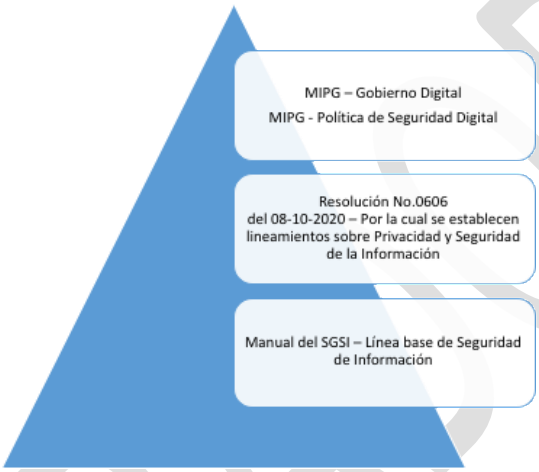
TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

1. Introducción

Este manual proporciona el marco de implementación del Modelo de Seguridad y Privacidad de la Información y la definición de la línea base que establece a un nivel más detallado las consideraciones a ser tenidas en cuenta en la implementación de las diferentes guías de operación.



Este marco de implementación se soporta en la norma ISO 27001:2013, el modelo MSPI (*Modelo de Seguridad y Privacidad de la Información*) del MinTIC (*Ministerio de tecnologías de información y comunicaciones*) y la norma ISO 27002.

Los procedimientos de control de documentos de la Institución y que hacen parte del Sistema de Gestión de Calidad de la IUE, se aplican a este Manual y a todos los documentos del MSPI.

2. Glosario

a) **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas, entre otros) que tenga valor para la organización. (Modelo de Seguridad y Privacidad de la Información,2016).

b) **Activo de información:** Cualquier elemento que contenga, genere, adquiera, gestione y/o procese información, que tiene valor para uno o más procesos de la organización y debe protegerse. (NTC-ISO/IEC 27001).

c) **Confidencialidad:** Propiedad de la información que hace que no esté disponible o sea conocida por personas, Institución es o procesos no autorizados. (NTC-ISO/IEC 27000: 2018).

d) **Custodio:** Es una parte designada de la Institución, un cargo, proceso, o grupo de trabajo encargado de hacer efectivos las restricciones y clasificaciones de acceso definidos por el propietario. (Guía para la Gestión y Clasificación de Activos de Información,2016).

e) **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).

f) **Ciberespacio**: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

g) **Disponibilidad:** Propiedad de la información que hace que este accesible y utilizable por solicitud de una Institución autorizada. (NTC-ISO/IEC 27000: 2018).

h) **Hardware:** Equipos de cómputo y de comunicaciones que por su criticidad son considerados activos de información, no sólo activos fijos. (Guía para la Gestión y Clasificación de Activos de Información,2016).

i) **Información:** Datos relacionados que tienen significado para la Institución. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la Institución y, en consecuencia, necesita una protección adecuada. (Guía para la Gestión y Clasificación de Activos de Información,2016).

j) **Información Pública:** Otorgada por el funcionario público en ejercicio de sus funciones o con su intervención. Así mismo, es público el documento otorgado por un particular en ejercicio de funciones públicas o con su intervención. (Ley 1562 de 2012).

k) **Información pública Clasificada:** Que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014).

l) **Información reservada:** Expresamente sometidos a reserva por la Constitución o la ley, y en especial: los protegidos por el secreto comercial o industrial, los relacionados con la defensa o seguridad nacionales, los amparados por el secreto profesional, los que involucren derechos a la privacidad e intimidad de las personas, incluidas en las hojas de vida, la historia laboral y los expedientes pensionales, los datos genéticos humanos y demás registros de personal que obren en los archivos de las instituciones públicas o privadas, así como la historia clínica, los relativos a las condiciones financieras de las operaciones de crédito público y tesorería que realice la nación. también se deben considerar como información reservada la información

asociada a: la seguridad pública, las relaciones internacionales, la prevención, investigación y persecución de los delitos y las faltas disciplinarias, mientras que no se haga ,efectiva la medida de aseguramiento o se formule pliego de cargos, el debido proceso y la igualdad de las partes en los procesos judiciales, la administración efectiva de la justicia, los derechos de la infancia y la adolescencia, la estabilidad macroeconómica y financiera del país, la salud pública, los documentos que contengan las opiniones o puntos de vista que formen parte del proceso deliberativo de los servidores públicos, y o consagrados en la Ley 1712 de 2014 en su artículo 19. (Ley 1712 de 2014).

m) **Integridad:** Es la propiedad de precisión y completitud. (NTC-ISO/IEC 27000: 2018).

n) **Personas:** Hace referencia a los cargos que, por su conocimiento, experiencia y criticidad para el proceso, son consideradas activos de información. (Adaptado de la Guía para la Gestión y Clasificación de Activos de Información,2016).

o) **Propietario:** Persona o Institución con la responsabilidad de rendir cuentas y la autoridad para gestionar un activo. (Guía para la Gestión y Clasificación de Activos de Información,2016).

p) **Política de seguridad de la información**: Establece a alto nivel los objetivos y metas relacionados con la seguridad de la información. (ISO/NTC 27001: 2013).

q) **Servicio:** Servicios de computación y comunicaciones, tales como Internet, páginas de consulta, directorios compartidos e Intranet, que sean prestados por un tercero. (Adaptado de la Guía para la Gestión y Clasificación de Activos de Información,2016).

r) **Seguridad de la Información:** Es el conjunto de medidas de detección, prevención y contención para las personas, los procesos, la tecnología y la infraestructura dentro de una organización, para proteger la confidencialidad, la disponibilidad e integridad de la información, con el objetivo de apoyar el cumplimiento de los objetivos de dicha organización. (Adaptado de la NTC-ISO/IEC 27001: 2013).

s) **Software:** Programas computacionales que son responsabilidad de la IUE y que cumplen con diversas funcionalidades de procesamiento de información como son: sistemas operativos, procesadores de texto, hojas de cálculo electrónico, sistemas de gestión de base de datos, servicios web y gestión documental, entre otros. El software puede ser comercial o desarrollado localmente. (Adaptado de la NTC-ISO/IEC 27001: 2013).

3. Normatividad

En el documento Matriz de Requisitos Legales y Otros Aplicables (DI-F-0009) se encuentra la información de las normas a ser consideradas en la elaboración de este Manual y la Gestión de Seguridad de la Información.

4. Objetivos

Permitir por medio de la implementación de estándares y mejores prácticas de seguridad de la información proteger la confidencialidad, integridad y disponibilidad de los activos de información asociados a los procesos de la Institución Universitaria de Envigado.

5. Alcance

El presente Manual aplica a todos los procesos de la Institución Universitaria de Envigado en el marco de una implementación incremental de los mismos, iniciando en el año 2021 con los procesos: Apoyo a Gestión Académica, Gestión Financiera y Gestión de Tecnología.

Fuente: IUE

5.1. Planear-Hacer-Verificar-Actuar

El ciclo PHVA es el procedimiento lógico y por etapas que permite el mejoramiento continuo del sistema de gestión de Seguridad de la Información a través del MSPI, y que le da solidez a todo el proceso. Las fases son 4 y se describen a continuación:

5.1.1.Fase PLANEAR - establecer el MSPI

a) La Institución ha definido su política de Seguridad de la Información en la Política de Seguridad Digital MIPG, la cual puede ser consultada en https://www.iue.edu.co/?transparencia=otros-documentos-de-planeacion#297-297-mipg-p2

b) Igualmente ha definido los lineamientos Lineamientos seguridad y privacidad de la información en la Resolución 0660 de 2020, la cual puede ser consultada en: https://www.iue.edu.co/?transparencia=normativa-de-la-entidad-o-autoridad#111-143-2020-resoluciones

c) Para la Institución, el MSPI está destinado a facilitar la gestión de riesgos asociados a los activos de información que soportan los procesos institucionales.

d) El Modelo se basa en un enfoque sistemático para la identificación de activos de información y riesgos. El marco de gestión de riesgos en el que los criterios para la evaluación de riesgos son descritos y la estructura de la valoración del riesgo son definidos en el Manual Gestión y Plan de Tratamiento de Riesgos de Seguridad de la Información.

e) El análisis sistemático de riesgos se realiza por procesos.

f) Las opciones para el tratamiento del riesgo se identifican y evalúan de conformidad con el proceso establecido en el Manual Gestión y Plan de Tratamiento de Riesgos de Seguridad de la Información.

g) Los objetivos de control y controles son seleccionados a partir del Anexo A de la norma ISO 27001: 2013 NTC y la norma ISO 27002, para cumplir con los criterios y requisitos del marco de gestión de riesgos, teniendo en cuenta los criterios de aceptación de riesgo y los requisitos jurídicos, regulatorios y contractuales actuales.

h) El Comité de Gestión debe aprobar la implementación del MSPI y los cambios a este manual, también aprueba los riesgos residuales.

5.1.2. Fase HACER – implementar y operar el MSPI

Fase del ciclo donde se lleva a cabo las medidas que se han planificado en la fase anterior, siguiendo los siguientes lineamientos:

a) El plan de tratamiento de riesgos de la Institución refleja las decisiones adoptadas en la fase PLANEAR, e identifica las medidas de gestión, las responsabilidades y las prioridades para la gestión de los riesgos de Seguridad de Información identificados.

b) Los recursos y financiación adecuados, como se describe en el plan de tratamiento de riesgos, están asignados para su implementación.

c) Los controles seleccionados están implementados para ajustarse a los objetivos de control identificados.

d) La IUE, ha definido como medir la efectividad de sus controles y ha especificado como utilizar estas medidas, para mejorar la efectividad del control, así como generar resultados comparables y reproducibles, lo cual se encuentra establecido en los indicadores del MSPI.

e) Se han implementado programas de entrenamiento y cultura como es requerido en el plan de tratamiento del riesgo.

f) Se desarrollan en forma incremental las guías de operación requeridas en la implementación del MSPI.

g) La IUE ha implementado actividades de monitoreo y control en el marco de la gestión del SGC y la gestión de riesgos institucional.

5.1.3. Fase VERIFICAR – monitorear y revisar el MSPI

Fase del ciclo donde se examinan las acciones y procedimientos para comprobar si se están consiguiendo los resultados esperados, de acuerdo a los siguientes lineamientos:

a) Los controles implementados para ajustarse a los objetivos de control están en operación para detectar eventos de seguridad, incidentes y brechas de seguridad, habilitar a la dirección para evaluar si las actividades de seguridad están siendo ejecutadas de acuerdo con los criterios establecidos, y tomar las acciones para resolver alguna brecha de seguridad de forma, que refleje las prioridades de la Institución.

b) La IUE, revisa en forma regular la efectividad del MSPI, de acuerdo con las políticas, el Manual Gestión y Plan de Tratamiento de Riesgos de Seguridad de la Información y guías de operación, buscando mejorar en forma continua la efectividad del MSPI a través del análisis de los resultados de auditoría y el monitoreo de eventos y/o actividades, todo en el contexto de los objetivos y el plan de tratamiento de riesgos, al menos una vez al año.

c) La IUE mide la efectividad de los controles, a través de los indicadores propuestos para ésto, y verificar que los requerimientos de seguridad han sido alcanzados.

d) A intervalos planeados, lo mismo que cuando hallan cambios significativos, la IUE revisa su evaluación de riesgos y plan de tratamiento de los mismos, incluyendo niveles de riesgo residual y riesgo aceptable (tomando en cuenta cambios en la efectividad de los controles), que son afectados por los cambios, o lleva a cabo evaluaciones de riesgo adicionales en relación con las nuevas tecnologías, y sistemas o cualquier otro cambio que afecte la información o activos de información de la Institución .

e) La IUE lleva a cabo regularmente auditorías internas al MSPI, de acuerdo con el Procedimiento de auditoría interna y el Programa de Auditoría Interna.

f) El plan de tratamiento de riesgo es actualizado para tomar en cuenta los hallazgos de las actividades de evaluación y monitoreo.

5.1.4. Fase ACTUAR – mantener y mejorar el MSPI

Esta es la última fase del ciclo, donde se deben implementar medidas de mejora, para elevar la eficacia de todas las acciones en materia de Seguridad de la Información, teniendo en cuenta los siguientes lineamientos:

a. En caso de que oportunidades de mejora para el MSPI sean identificadas durante la fase VERIFICAR, son implementadas siempre y cuando cumplan con los criterios de relevancia del Plan de Tratamiento de Riesgos.

5.2. Marco para la gestión de riesgos

El enfoque de la organización para la gestión del riesgo, que ha sido específicamente aprobado y autorizado, está contenido en el *Manual Gestión y Plan de Tratamiento de Riesgos de Seguridad de la Información* el cual es aplicado a todos sus procesos.

5.3. Evaluación de riesgos

El método de la IUE para la evaluación de riesgos es la *Manual Gestión y Plan de Tratamiento de Riesgos de Seguridad de la Información* y la matriz de riesgos, derivada de esta metodología que es apropiada para el alcance del MSPI de la Institución, los objetivos institucionales, disposiciones reglamentarias, legales y contractuales.

5.4. Enfoque sistemático para la evaluación de riesgos

La Institución tiene un enfoque documentado en la *Manual Gestión y Plan de Tratamiento de Riesgos de Seguridad de la Información,* que contempla la evaluación y tratamiento riesgos con un enfoque sistemático.

5.5. Declaración de aplicabilidad

Los objetivos de control y los controles de la norma ISO 27001:2013 a ser consideradas en la IUE, se seleccionan de acuerdo con los objetivos de gestión de riesgos y las necesidades institucionales, esta información se documenta en la Declaración de Aplicabilidad.

5.6. Línea Base de Seguridad de la Información

A continuación, se presenta la línea base en diferentes dominios de control, los cuales son definidos en forma incremental y de acuerdo a las necesidades institucionales:

5.6.1. Línea Base de Seguridad para dispositivos Móviles

a) La Oficina Informática dentro del plan de sensibilización en Seguridad de la Información, debe asegurar que los usuarios conocen y utilizan las herramientas para realizar las copias de seguridad en los dispositivos móviles como por ejemplo OneDrive de Microsoft.

b) La oficina de informática y la oficina de comunicaciones dentro del plan de sensibilización en Seguridad de la Información, debe asegurar que los usuarios conocen y practican las recomendaciones para el cuidado y seguridad física de los dispositivos móviles.

c) El responsable de la administración de la consola de antivirus definirá las recomendaciones para la protección y configuraciones, para la instalación de antivirus de los dispositivos móviles.

d) Para los dispositivos móviles que contengan información confidencial o critica para la Institución y de acuerdo con análisis de riesgos realizado sobre los mismos, se deberá contemplar la opción de cifrado en reposo.

e) El área de soporte de la oficina de informática de la IUE debe dentro del plan de sensibilización informar las posibilidades de configurar la opción de borrado remoto de información en los dispositivos móviles, con el fin de eliminar los datos y restaurar los valores de fábrica de manera remota, para evitar divulgación no autorizada de información en caso de pérdida o hurto del dispositivo.

5.6.2. Línea Base de Seguridad de Trabajo en Casa

LA IUE dentro de las actividades de sensibilización y capacitación al personal, deben desarrollar un capítulo específico sobre la protección de equipos de cómputo en casa, el cual deber ser de carácter general y que sustentará a futuro un escenario posible de Teletrabajo o Trabajo en Casa.

Estas actividades deben incluir:

a) Como contar con la protección física adecuada contra hurto, daño o pérdida del equipo y/o de la información, divulgación no autorizada de información, acceso remoto no autorizado a los sistemas de información de la Institución o un mal uso de estos.

b) Como resguardar adecuadamente los equipos e información requeridos, así como los mecanismos de seguridad para garantizar la integridad, disponibilidad y confidencialidad de la información.

c) Porque es importante los mecanismos de seguridad como la protección de antivirus, requisitos de barreras de firewall y demás soluciones requeridas para salvaguardar adecuadamente la información de la Institución.

d) Se define con antelación entre la Institución y las partes interesadas, el trabajo a realizar, la información y los sistemas a los que requiere acceder, así como el horario al cual podrá acceder, el cual debe estar documentado y aprobado previamente por la Oficina Informática.

5.6.3. Línea Base de Seguridad de Control de Acceso

a) La IUE, establece e implementa procedimientos formales para controlar la asignación de derechos de acceso a usuarios. Dichos procedimientos cobijan todas las etapas del ciclo de vida del usuario, desde su registro inicial hasta el bloqueo o la eliminación del registro a quienes no necesiten más acceso. Se brinda atención especial, donde sea apropiado, a la necesidad del control de asignaciones de accesos privilegiados que permitan superar los controles básicos de los sistemas.

b) La IUE, propone limitar el acceso a información y a sus instalaciones de procesamiento de información con fines de protección de datos personales, seguridad de la información y continuidad del negocio (Confidencialidad, Integridad y Disponibilidad).

c) Los lineamientos de gestión de usuarios se deben aplicar para los sistemas que se basen en contraseñas, identificación y autenticación de los usuarios.

d) Toda creación de nuevas cuentas sobre los sistemas de información debe ejecutarse siguiendo criterios (perfiles y atributos de acceso) del mapa de accesos y roles establecidos por la Institución, para cada cargo vs aplicación o plataforma.

e) Es responsabilidad del jefe inmediato, reportar a través de la Mesa de Servicios cualquier novedad a la Coordinación de Recursos Humanos, para la creación, modificación, desactivación, bloqueo y/o retiro de usuario de la aplicación, desde que se vincula personal nuevo, durante su permanencia en la organización y hasta su retiro laboral.

f) Una vez Gestión Humana notifique el retiro de un colaborador, la Oficina Informática debe gestionar la inactivación de inmediato de las claves de acceso al Directorio Activo, correo electrónico y todas aquellas aplicaciones a las que tiene acceso, basados en el mapa de accesos y roles.

g) La clave de acceso a cada aplicativo debe ser entregada de manera segura y es de uso personal e intransferible del usuario. Por lo tanto, se presume que toda la acción realizada bajo la cuenta asociada a un usuario fue ejecutada por el responsable de la cuenta.

h) Es responsabilidad de cada usuario, la salvaguarda de las contraseñas que le fueron entregadas o las establecidas por el mismo.

i) Cualquier cambio o modificación al mapa de accesos y roles, debe ser autorizado por el jefe inmediato y/o el responsable de la aplicación o plataforma involucrada.

j) Las contraseñas deben cambiarse al primer inicio de sesión.

k) Después de un número determinado de intentos no exitosos de ingreso de la contraseña a cualquier aplicación o plataforma, el usuario será bloqueado de manera inmediata.

l) La Oficina Informática, junto con el líder funcional o líder de cada área, debe realizar validaciones anuales del mapa de accesos y roles, a fin de cerciorarse que los usuarios acceden solamente a los recursos autorizados para la realización de sus tareas, velando siempre por el mínimo privilegio.

m) Cada usuario tiene que autenticarse antes de acceder a un recurso de tecnología sobre el cual está autorizado, por medio de un usuario y una contraseña.

n) El propietario de la aplicación y de la información, debe identificar y documentar explícitamente la sensibilidad o confidencialidad de ésta.

o) Los propietarios de los activos de información deben autorizar los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles establecidos y las necesidades de uso.

p) No está permitido para ningún usuario acceder a la información y a las aplicaciones de un sistema de información, para el cual no haya sido autorizado.

q) Las cuentas de acceso privilegiado deben estar nombradas y sus contraseñas deben estar en custodia.

r) El acceso a programas utilitarios de sistemas debe estar controlado mediante el mapa de roles.

s) Las contraseñas deben cambiarse al primer inicio de sesión y periódicamente cada 30 días.

t) Después de un número determinado de intentos no exitosos de ingreso de la contraseña, el usuario será bloqueado de manera inmediata y deberá solicitar el desbloqueo al área de TI.

u) Cualquier cambio en las funciones de los usuarios, deben ser notificados por el jefe de la Oficina Informática

v) El profesional universitario de informática y el técnico operativo deben revisar los derechos de acceso de los usuarios a intervalos de seis meses.

w) Los grupos de servicios de información, usuarios y sistemas de información deben ser segregados en redes.

x) Se deben restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.

5.6.4. Línea Base de Seguridad sobre el uso de Controles Criptográficos

a) Se debe realizar una valoración de riesgos e impactos, para facilitar la selección de controles y los niveles de protección requeridos sobre la información en tránsito e información almacenada.

b) Si en la evaluación de riesgos se define la necesidad de un sitio seguro, este debe contar un certificado digital vigente y generado por un organismo certificador autorizado y registrado ante la ONAC, con mínimo un (1) año de vigencia a partir de su adquisición.

c) Si en la evaluación de riesgos se define la necesidad de utilizar mecanismos de cifrado y protección de la información en tránsito y almacenada, se deben utilizar algoritmos estándar vigentes y seguros, reconocidos por la industria de Ciberseguridad.

5.6.5. Línea Base de Seguridad de Gestión de Llaves Criptográficas

a) Las responsabilidades y condiciones de la generación, certificación, uso, cambio o recuperación de firmas electrónicas o llaves criptográficas en los procesos o actividades de la IUE deben ser documentadas según las necesidades de cada dependencia.

b) Las novedades de colaboradores (ejemplo: vacaciones, cambio de responsabilidades o retiro de la Institución) que gobiernen o gestionen certificados o llaves criptográficas de la

Institución, requiere la entrega formal de elementos custodiados y la generación de nuevas llaves o certificados en caso de ser requerido.

c) Los controles de gestión, custodia y protección de certificados y llaves criptográficas de la Institución deben ser auditados mínimo una vez al año.

5.6.6. Línea Base de Seguridad de Copias de Respaldo

a) El líder de cada aplicación en conjunto con el desarrollador de la aplicación deberá establecer el método de copia de respaldo que más se ajuste a su necesidad, teniendo en cuenta los siguientes factores: Cuáles datos se deben incluir, tipos de respaldos, Cantidad de copias a realizar, modalidad de copia, dónde guardarlas, quiénes los generan, cuándo hacerlo y soporte físico a utilizar para el respaldo.

b) La herramienta utilizada para realizar el backup de servidores en su totalidad es Veeam Backup.

c) Se establece un backup diario, en los horarios 6pm y 8am en aplicativo, y semanal, cada viernes a las 12m en cinta la cual se archiva.

d) Las cintas magnéticas o cualquier otro instrumento que resguarde la información institucional, deberá ser custodiada en sitios y mecanismos que garanticen la seguridad de la misma.

e) La información de los archivos contenidos en las copias de seguridad debe ser única y exclusivamente de uso institucional y no personal.

f) Los líderes de proceso son los únicos autorizados para solicitar la recuperación de información ante una pérdida total, parcial o para realizar pruebas controladas y se debe realizar dicha solicitud a través de la mesa de servicios.

g) Es responsabilidad del administrador de copias, informar la disponibilidad de los respaldos, realizar el trámite para obtener los medios magnéticos, ejecutar el procedimiento de recuperación e informar los resultados.

h) La IUE, debe asegurar que la información respaldada esté disponible y guarde la completitud y exactitud, por lo que es necesario realizar pruebas a los Backups realizados, de forma controlada y a intervalos planificados.

i) El único medio de respaldo de la información para los colaboradores es OneDrive, el cual será configurado por la Oficina de Informática.

5.6.7.Línea Base de Seguridad de Transferencia de Información

a) Los líderes de área en conjunto con la Oficina Informática definen los mecanismos y herramientas que permiten que el intercambio de la información se realice de forma segura, deberá contemplar el uso de cifrado en casos que se consideren pertinentes como el envío de información confidencial por medio de correo electrónico o usar canales seguros como un FTPS/SFTP, VPN y demás medios que permitan que la información conserve su confidencialidad e integridad. Además de lo anterior, deben acordar en ambas partes los responsables de la ejecución de esta actividad (remitente – destinatario).

b) La Oficina Informática junto con el Líder de área, deben realizar un análisis de los riesgos relacionados con el intercambio de la información, asegurando se contemplen los eventos que puedan afectar la ejecución de las actividades y lograr solventarlas de manera efectiva. Los riesgos relacionados con el intercambio seguro de la información deben estar incluidos en la matriz de riesgos del proceso y aplicarle todo el ciclo de riesgos.

c) La transferencia de información a otras Instituciones, como el ministerio de educación y demás, se realiza de acuerdo con los protocolos y necesidades de estas instituciones. Es deber de la IUE seguir los lineamientos de estas.

5.6.8. Línea Base de Seguridad de Desarrollo Seguro

a) La IUE ha implementado controles para que todas las actividades relacionadas con el desarrollo y mantenimiento de sistemas de información, aunque sea desarrollado por terceros, consideren la administración de los riesgos de seguridad.

b) El proveedor de desarrollo contratado deberá contar con una política para el desarrollo seguro.

c) El proveedor de desarrollo contratado deberá garantizar que se tienen ambientes de desarrollo, pruebas y producción separados.

d) Los datos utilizados para las pruebas deben ser seleccionados y éstas deben ser eliminadas luego de concluir el set de pruebas.

e) Las aplicaciones deben permitirse integrar a otros sistemas y deben ser escalables.

f) El custodio de los códigos fuentes, debe llevar un registro actualizado de todos los programas fuentes en uso, indicando nombre del programa, programador, Analista responsable que autorizó, versión, fecha de última modificación y estado (en modificación, en producción).

g) Se debe restringir el acceso a los códigos fuente de los programas. Solamente los ingenieros desarrolladores designados tendrán acceso.

h) Las aplicaciones deben cumplir con un esquema de roles y responsabilidades.

i) Se deben generar validaciones de entrada de datos para prevenir entrada errónea de datos.

j) No está permitido el quemado de datos (Nombre, correo, entre otros) en el código.

k) Las bases de datos deben cumplir con los principios básicos de relacionamiento de bases de datos.

l) Las pruebas realizadas a las aplicaciones deben ser ejecutadas técnicamente por el personal de ingeniería y funcionalmente por los usuarios solicitantes.

5.6.9. Línea Base de Seguridad para las relaciones con Proveedores

a) Los proveedores que tengan acceso a la información de la IUE deben firmar el acuerdo de confidencialidad definido para ello.

b) Para la contratación de servicios o componentes de la infraestructura de TI, se debe exigir a los proveedores la presentación de los planes de contingencia, con el fin de asegurar la disponibilidad de la información o el procesamiento de ésta.

c) Los proveedores deben reportar incidentes y compartir lo evidenciado con la Institución, a fin de dar respuesta al incidente.

d) Durante la ejecución del contrato, es función del área o colaborador que contrata, monitorear y hacer seguimiento a los controles pactados para asegurar la confidencialidad, integridad y disponibilidad de la información, frente a los riesgos previamente identificados.

e) Como parte de la supervisión a la ejecución del contrato, se deben contemplar procesos de auditoría a proveedores, cuyo objetivo sea validar el cumplimiento de los requisitos de Seguridad de la Información estipulados desde la fase de planeación de la contratación. Dichos resultados deben quedar consignados en los informes presentados por el supervisor del contrato.

f) Toda gestión que represente una modificación, mantenimiento o revisión al servicio de tecnología de la información, comunicaciones o equipos de suministros, debe ser evaluado y autorizado por el jefe de la Oficina Informática.

5.6.10. Línea Base para la Instalación de Software en Sistemas Operativos

a) Todo software instalado y utilizado en los equipos de propiedad de la IUE, debe cumplir con los principios y legislación nacional vigente sobre derechos de autor, y en todo caso está

sujeto al respeto de los derechos o voluntad expresada por el autor en documentos físicos o digitales de licenciamiento.

b) Toda instalación de software en los equipos de cómputo debe ser realizada a partir de fuentes obtenidas legalmente con la autorización de su autor expresada según el modo y vigencia de licenciamiento. Todo programa de software recibido, adquirido o desarrollado con recursos de la Institución debe ser utilizado según los términos de su licencia.

c) La IUE, debe mantener como mínimo un repositorio e inventario centralizado, así como un sistema de respaldo y copias de seguridad que garantice el conocimiento, disponibilidad, integridad y gestión eficiente de los activos de software.

d) La IUE, fomenta el uso de Software Libre, este tipo de software respeta la libertad del usuario, facilita la transferencia de conocimiento y se fundamenta en la solidaridad y la democratización del acceso al conocimiento.