# UNIVERSIDAD POLITÉCNICA SALESIANA

## FACULTAD DE INGENIERÍAS

## SEDE QUITO-CAMPUS SUR

### CARRERA DE INGENIERÍA DE SISTEMAS

**MENCIÓN ROBÓTICA E INTELIGENCIA ARTIFICIAL**

# PLAN DE PROPUESTA PARA LA IMPLANTACIÓN DE LA NORMA DE SEGURIDAD INFORMÁTICA ISO 27001:2005, PARA EL GRUPO SOCIAL FONDO ECUATORIANO POPULORUM PROGRESSIO (GSFEPP)

**TESIS PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS**

**OSCAR EDUARDO CAMPAÑA TENESACA**

**DIRECTOR: ING. JORGE LÓPEZ**

**Quito, Noviembre 2010**

# DECLARACIÓN

Yo Oscar Eduardo Campaña Tenesaca, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Universidad Politécnica Salesiana, según lo establecido por la ley de Propiedad Intelectual, por su reglamento y por la normatividad institucional vigente.

---

Oscar Eduardo Campaña Tenesaca

# CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Oscar Eduardo Campaña Tenesaca bajo mi dirección.

---

Ing. Jorge López

# AGRADECIMIENTOS

En primer lugar quiero agradecer a mis padres ya que debido a su incondicional ayuda pude concluir mis estudios universitarios y realizar este trabajo de tesis.

Además quiero agradecer a mi director de tesis el Ing. Jorge López por su ayuda mientras fue mi maestro y por su excelente dirección en este trabajo de tesis.

# ÍNDICE:

## ÍNDICE DE ILUSTRACIONES:

# CAPÍTULO I

# 1 DEFINICIÓN DEL NEGOCIO

## 1.1 ORIGEN Y GIRO DEL NEGOCIO

El Fondo Ecuatoriano Populorum Progressio es una fundación privada con finalidad social, sin fines de lucro[1] y ecuménica[2], auspiciada por la Conferencia Episcopal Ecuatoriana[3].

Nació de la intención común de un grupo de laicos[4], sacerdotes y obispos, liderado por Mons. Cándido Rada, que buscaba dar respuesta al llamado de Pablo VI[5] en la encíclica[6] Populorum Progressio de crear un "fondo común" para la "asistencia a los más desheredados" en la perspectiva de un "desarrollo solidario de la humanidad".

El primer estatuto del FEPP[7] fue aprobado el 22 de julio de 1970, por decreto supremo de gobierno. La evolución institucional se refleja en las versiones nuevas del estatuto: 1971, 1974 y 1980 hasta la última reforma aprobada el 29 de enero de 1992.

Con este reconocimiento oficial, la institución tiene plena capacidad jurídica para realizar lícitamente todos los actos y contratos permitidos por las leyes ecuatorianas y el derecho internacional.

Desde el año 2000 se define como Grupo Social FEPP, ya que se han constituido al interior de la institución nuevas personerías jurídicas, que mantienen principios, valores, metodologías[8] y destinatarios comunes.

---

[1]Refiérase al glosario de términos.
[2]El **ecumenismo** se refiere a toda iniciativa que apunte a una mayor unidad o cooperación entre las confesiones cristianas.
[3]Refiérase al glosario de términos.
[4]Refiérase al glosario de términos.
[5] Refiérase al glosario de términos.
[6] Refiérase al glosario de términos.
[7]**FEPP:** Fondo Ecuatoriano Populorum Progressio
[8] Refiérase al glosario de términos.

### 1.1.1 PLAN DE ACCIÓN ESTRATÉGICO:

Los aspectos en los cuales el Grupo Social FEPP basa estratégicamente su plan de acción son los siguientes:

- **Implementación de los puntos clave de la planificación estratégica del GSFEPP[9]**

  La planificación estratégica, elaborada para el período 2006/2010, se completó con la terminación de las planificaciones de todos los equipos regionales, empresas y cooperativa. De esta forma todos los equipos que componen el GSFEPP se han alineado con las líneas estratégicas que el conjunto señaló como prioritarias. Analizaremos los puntos clave de la mencionada planificación estratégica y los pasos que se han dado en su implementación.

- **Opción por el desarrollo local**

  Prácticamente en todos los equipos regionales del GSFEPP se ha asumido esta opción de trabajar con mucha más fuerza en el ámbito de lo local, promoviendo la interacción con otros actores locales: los gobiernos locales, las delegaciones de otras instancias gubernamentales, otras ONGs[10] y, fundamentalmente, las organizaciones populares que han sido históricamente nuestras principales aliadas en el trabajo de desarrollo.

  Desde la Dirección Ejecutiva se fortaleció esta línea, ya que en las Orientaciones para el Ser y Quehacer del FEPP en 2007 se abordó este tema con el título: “Las personas son el sujeto y el fin del desarrollo local”.

  Aunque aún falta tiempo para poder valorar la incidencia real de la opción tomada, no hay duda que esta orientación posiciona al

[9] Grupo Social Fondo Ecuatoriano Populorum Progressio
[10] Organización no gubernamental.

GSFEPP en un plano de mayor cooperación y coordinación con otras instituciones.

- **Fortalecimiento de las finanzas populares**

  Las finanzas populares se han convertido en una alternativa real para impulsar el desarrollo. Es un campo en que intervienen con fuerza una gran parte de los diversos equipos del GSFEPP.

  En 2007 se han consolidado las redes locales y, por propia iniciativa, éstas han iniciado el proceso para la constitución de la gran red nacional. Estas redes ven en el GSFEPP un aliado estratégico muy importante para apoyar su propio proceso.

  Se considera que esta iniciativa despierta gran esperanza, ya que supone un salto cualitativo para consolidar las finanzas populares y desarrollar su enorme potencial a favor del desarrollo.

- **Comercialización popular**

  Si las finanzas populares se han transformado en una realidad que está adquiriendo una dinámica propia, la comercialización es aún una de las asignaturas pendientes, el cuello de botella que ha supuesto una enorme limitación para las propuestas de desarrollo.

  Esto hizo que el GSFEPP decidiera priorizar esta línea dentro de sus proyectos de cambio en la planificación estratégica. La alternativa diseñada se basa en la constitución y buen funcionamiento de los centros de negocios y servicios campesinos. La estrategia de los CNC[11] supone superar la visión tradicional de los centros de acopio y comercialización que,

[11] Centro de negocios campesinos.

aunque en algunos casos han logrado ser exitosos, en otros no han alcanzado su plena sostenibilidad.

Los CNC pretenden intervenir en toda la cadena de valor de los productos desde la etapa de producción, pasando por la asistencia técnica, el procesamiento y alistamiento del producto para llegar a la comercialización.

En prácticamente todas las regionales se están implementando CNC y algunos de ellos han alcanzado un éxito importante. En los próximos años se desarrollará esta propuesta en todo su potencial.[12]

### 1.1.2 CAMPO DE ACCIÓN DEL GSFEPP

Desde hace muchos años el GSFEPP asumió como propuesta para acercarse a las familias beneficiarias de su acción la descentralización en oficinas regionales y empresas.

En la actualidad al menos una de las instancias del GSFEPP está presente con su acción en 23 de las 24 provincias del Ecuador, incluyendo las islas Galápagos, donde FUNDER está a punto de constituir una sede permanente.

Las regionales atienden 21 provincias, en 14 de las cuales se trabaja con mayor intensidad y presencia. Esta presencia se da en 86 cantones y 236 parroquias civiles.

La razón de ser del GSFEPP es apoyar los esfuerzos solidarios que de forma organizada realizan las familias campesinas y urbano marginales pobres del Ecuador para construirse una vida mejor.

[12]Fuente :Fuente: Luis María Gavilanes del Castillo, El FEPP: Llamada, pulso y Desafío, Julio 1995, ImpreFEPP, Quito-Ecuador.

La experiencia de trabajo institucional se ha desarrollado fundamentalmente en el sector rural, pero en los últimos años se ha dedicado atención también al sector urbano popular. Se da prioridad a lugares alejados, con altos índices de pobreza y sin mayor atención del estado u otras instituciones.

El apoyo se dirige preferentemente a las organizaciones de base y de segundo grado, sean éstas de hecho o jurídicas, procurando siempre su fortalecimiento y consolidación.

La colaboración se caracteriza por la apertura y amplitud de respuesta ofrecida a las organizaciones y familias sin excluir, limitar ni condicionar el apoyo por motivos de etnia, género, credo religioso, edad, opción ideológica o política. El GSFEPP tiene como una de sus opciones promover de forma activa el mejoramiento de las relaciones de equidad de género, étnica e inter generacional. Por ello pone especial atención a los grupos más vulnerables y desprotegidos: indígenas, afro descendientes montubios, mujeres, niños/as y jóvenes.

El calor humano, la alegría, el respeto, la identificación y el espíritu de servicio son las características que queremos que tenga nuestro trabajo con las familias beneficiarias.

En estos últimos años la acción conjunta del GSFEPP llega a un número aproximado de 100.000 familias, unas 550.000 personas.[13]

### 1.1.3 MISIÓN

El Fondo Ecuatoriano Populorum Progressio está al servicio de hombres y mujeres campesinos, indígenas, afro ecuatorianos,

[13]Fuente: Luis María Gavilanes del Castillo, El FEPP: Llamada, pulso y Desafío, Julio 1995, ImpreFEPP, Quito-Ecuador.

mestizos y pobladores urbano marginales organizados, como una instancia de apoyo a los esfuerzos que realizan para el logro de sus aspiraciones profundas en aspectos de organización, educación, acceso a fuentes de trabajo y medios de producción, transformación y comercialización, conservación del medio ambiente, equidad entre géneros y bienestar, contribuyendo a crear esperanza, justicia y paz.

Motivados por el Evangelio[14] y la doctrina social de la Iglesia[15], especialmente la encíclica Populorum Progressio[16], los miembros del FEPP asumimos la inspiración cristiana como motor de un desarrollo integral, sostenible y liberador; respaldamos nuestras propuestas con recursos técnicos, administrativos y financieros y nos comprometemos a buscar transformaciones en la sociedad a partir de los valores de la opción preferencial por los pobres, la no violencia, la transparencia y un espíritu de servicio ágil y alegre, fieles a la palabra y ejemplo de Mons. Cándido Rada, nuestro fundador.

Se cuenta con la solidaridad de personas e instituciones del Ecuador y del exterior que comparten nuestros objetivos e ideales. Nos esforzamos por alcanzar responsable y progresivamente nuevas formas de financiamiento y autofinanciamiento para la consecución de nuestros fines.

Se utiliza el diálogo como instrumento para la cooperación, la superación de las dificultades y el encuentro creativo de personas y pueblos, manteniendo cada uno nuestra propia identidad.

Trabajar con mujeres y hombres que nos enriquecen permanentemente con su confianza y el testimonio de una vida

[14] Refiérase al glosario de términos.
[15] Refiérase al glosario de términos.
[16] Refiérase al glosario de términos.

esencial y sacrificada, nos hace sentir la satisfacción de pertenecer a una fundación que hace del servicio su razón de ser.[17]

### 1.1.4 VISIÓN

El Fondo Ecuatoriano Populorum Progressio es un Grupo Social consolidado y sostenible, integrado por oficinas, empresas sociales y cooperativas descentralizadas, fuertemente unidas por principios y valores comunes y articulados entre sí, que generan productos y servicios eficientes y de calidad.

En una sociedad en constante evolución impulsa con ideas innovadoras, acompañamiento solidario y recursos humanos, económicos y técnicos, los esfuerzos de grupos populares, familias y personas necesitadas que desarrollan capacidades locales, creando economías de encadenamiento vinculadas a mercados reales.

Promueve el acceso a nuevas formas y medios de producción, la conservación y uso sostenible de los recursos naturales, la formación profesional, la generación de empleo, la transformación y comercialización de productos y los sistemas financieros locales, que producen cambios positivos en las condiciones de vida de la población, con equidad de género.

Genera ingresos, administra recursos tanto propios como de la cooperación nacional e internacional, mantiene relaciones de coordinación y colaboración con instituciones públicas y privadas y tiene seguridad respecto a la sostenibilidad de sus servicios.

Ha alcanzado la sostenibilidad de los servicios en base a su calidad, privilegiando los recursos locales.

[17]Fuente: Fuente: Luis María Gavilanes del Castillo, El FEPP: Llamada, pulso y Desafío, Julio 1995, ImpreFEPP, Quito-Ecuador..

Es una institución reconocida a nivel nacional e internacional por sus valores y el impacto alcanzado y el impacto alcanzado en las condiciones de vida de la población de escasos recursos.[18]

### 1.1.5 VALORES

Los valores en lo que creemos quienes hacemos el FEPP y que procuramos vivirlos refleja la orientación profundamente cristiana de la institución, que se inspira en la doctrina social de la iglesia católica, en especial en la encíclica Populorum Progressio de Papa Paulo VI. Estos son: Inspiración cristiana, No violencia, Austeridad[19], Honradez, Transparencia, Sencillez, Agilidad, Alegría, Solidaridad, Diálogo, Respeto, Creatividad.[20]

[18]Carlos Ernesto Ortega, Finanzas Populares y migración: tejiendo la red para el desarrollo local, Abril 2009, ImpreFEPP, Quito-Ecuador.
[19] Refiérase al glosario de términos.
[20]Fuente: Carlos Ernesto Ortega, Finanzas Populares y migración: tejiendo la red para el desarrollo local, Abril 2009, ImpreFEPP, Quito-Ecuador.

## 1.2 ORGANIZACIÓN ESTRUCTURAL Y FUNCIONAL

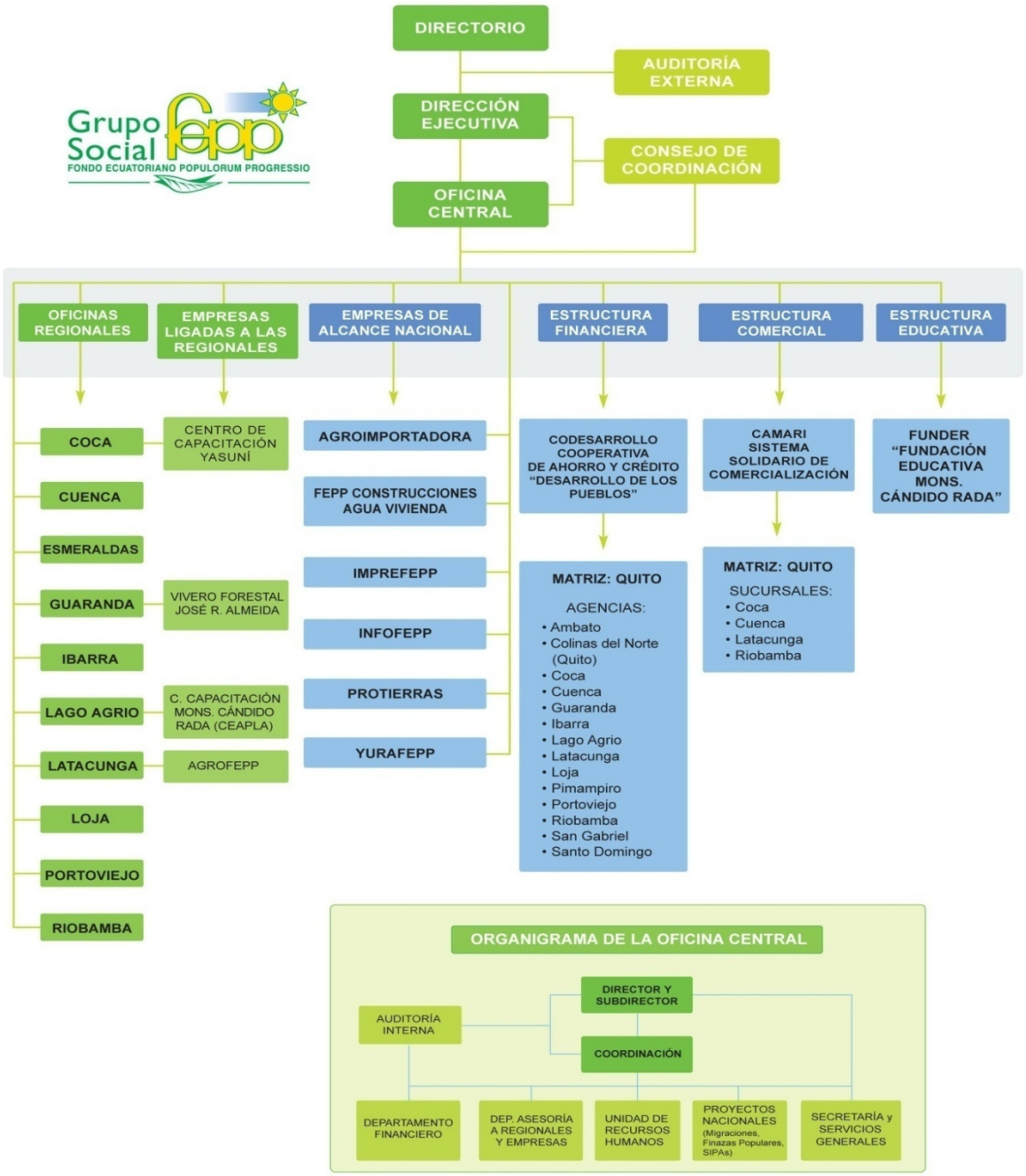


Ilustración 1.- Organigrama del Grupo Social Fondo Ecuatoriano Populorum Progressio[21]

[21] Fuente: Archivo departamento de diseño e impresión IMPREFEPP.

## 1.3 OBJETIVOS ESTRATÉGICOS DEL NEGOCIO

Basados en la Misión y Visión del Grupo Social FEPP, se han definido los siguientes objetivos estratégicos:

- Garantizar la confiabilidad[22], confidencialidad[23] e integridad[24] de la información que se genera en las diferentes entidades del GSFEPP.
- Mejorar los procesos internos en la gestión de la información con la finalidad de mejorar el servicio al público en general en la administración de los proyectos con finalidad social aquí manejados.
- Ser una Institución transparente, confiable, integra que goce de plena confianza en el ciudadano ecuatoriano y en especial de los más pobres.

## 1.4 DEFINICIÓN DEL PROBLEMA.

### 1.4.1 PLANTEAMIENTO DEL PROBLEMA

El Grupo Social FEPP, debido a su transcendental importancia en la sociedad ecuatoriana en especial en los sectores pobres, es la institución encargada de generar y financiar proyectos que ayuden al mejoramiento de la calidad de vida de los hombres y mujeres campesinos, indígenas, afro ecuatorianos, mestizos y pobladores urbano marginales organizados, de tal manera que la información que se genera en esta institución debe contar con un altísimo grado de protección ya que maneja información financiera de fondos públicos y aportes externos.

La estructura informática si bien es un medio por el cual ha permitido dotar de herramientas para el ágil desempeño de las labores dentro

[22] Refiérase al Glosario de Términos
[23] Refiérase al Glosario de Términos
[24] Refiérase al Glosario de Términos

de la institución, no cuenta con un nivel estructurado de protección de la información.

A continuación enumeramos en términos generales todos los problemas que en relación al tema tiene el Grupo Social FEPP:

- No se encuentran establecidas políticas de acceso y de uso de los computadores a los usuarios que manejan la información de las diferentes empresas y regionales que forman el Grupo Social FEPP.

- Todos los computadores del Grupo Social FEPP tienen habilitados los periféricos y puertos de salida, esto conlleva a un grave problema de seguridad ya que fácilmente se pueda dar fuga de información.

- No se cuenta con políticas de manejo de personal dentro del Grupo Social FEPP.

- La definición de políticas de uso de hardware y software está determinada por las implementadas en las políticas de grupo del directorio activo para el del Grupo Social FEPP, pero este se va implementando a medida que los usuarios lo permiten.

- El uso de los recursos informáticos, está determinado por las necesidades generadas, pero en la mayoría de los casos la demanda de servicios excede la disponibilidad de recursos generando cuellos de botella en los servidores y por consiguiente insatisfacción en los usuarios.

- El manual de políticas y de procedimientos, no es completo y no cuenta con una aprobación de parte de la Directiva de la organización.

- No existe una adecuada implementación de seguridades de acceso al centro de cómputo que garantice la seguridad de la

información y del hardware que se encuentra en este y que brinda los servicios a la institución lo que pone en riesgo la información del Grupo Social FEPP.

- El centro de cómputo no cuenta con instalaciones adecuadas para prevenir incidentes de incendios por lo que pone en riesgo todo el equipo informático del centro de cómputo.

- No existe una adecuada administración de incidentes de seguridad, lo cual pone en riesgo a la información generada en el Grupo Social FEPP.

- Las políticas de respaldos, no están bien estructurados, no existe información documentada y se las maneja de forma empírica, por lo que no garantizan una eficaz recuperación.

- El servicio de antivirus, no se encuentra debidamente normalizado debido a problemas en la contratación de actualizaciones en las licencias, esto conlleva a tener problemas serios de ataques a la red.

- Existe un inventario de hardware de los equipos del Grupo Social FEPP, por parte del departamento de informática, pero este no refleja los movimientos y localización del mencionado hardware en las instalaciones.

- El personal del centro de cómputo no es suficiente para brindar los servicios necesarios, no está definido exactamente las funciones que realiza y para determinadas actividades no cuenta con una especialización para el área requerida.

- Se encuentran presentados proyectos para la mejora en las comunicaciones y seguridades en la red, pero hace mucho tiempo no se los ejecuta porque no existe el suficiente financiamiento, sumado al constante cambio de autoridades que no permiten implementar los proyectos presentados.

- No existen controles de entrada eficientes, ni tampoco un adecuado diseño de seguridad física para las oficinas del Grupo Social FEPP.

- No existe un control efectivo que permita evitar la filtración de la información ya que no se cuenta con controles que garanticen la confidencialidad, integridad y disponibilidad de la información de la todas las empresas y regionales del Grupo Social FEPP.

Por todos estos y otros problemas que existen es de vital importancia que el Grupo Social FEPP cuente con un plan de gestión de la seguridad de la información, de tal manera que se considera la oportunidad de realizar una propuesta que permita implantar un Sistema de Gestión de Seguridad Informática (SGSI)[25] tomando como base la norma ISO[26] 27001:2005 de forma metódica y documentada, basada en objetivos de seguridad y una evaluación de los riesgos a los que está sometida.

De continuar observándose los problemas antes mencionados, la información del Grupo Social FEPP no podrá ser garantizada en términos de confidencialidad, integridad y disponibilidad.

## 1.5 FORMULACIÓN DEL PROBLEMA

¿Cómo se lograría mantener una administración adecuada de la información, bajo normas establecidas y que garanticen su protección en el Grupo Social Fondo Ecuatoriano Populorum Progressio?

[25] Refiérase al Capítulo II

[26] Organización Internacional de Normalización, organismo encargado de promover el desarrollo de normas internacionales, cuyo objetivo es buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones a nivel internacional.

## 1.6 SISTEMATIZACIÓN DEL PROBLEMA

¿Qué ámbitos de mayor prioridad del Grupo Social FEPP requiere una administración segura de la información?

¿Cómo organizar los procesos actuales para alcanzar un esquema en la seguridad de la información?

¿Qué herramientas son necesarias para el modelamiento del sistema de información?

¿Qué se necesita para implementar la Norma ISO27001:2005 en el Grupo Social FEPP?

## 1.7 DEFINICIÓN DEL PROYECTO

### 1.7.1 OBJETIVOS

#### 1.7.1.1 Objetivo General

Proponer la implantación de la norma de seguridad informática ISO 27001:2005 en el Grupo Social Fondo Ecuatoriano Populorum Progressio, para identificar y evaluar los riesgos que existe en la seguridad de la información, mediante la cual nos permita implantar contramedidas, procesos y procedimientos para un apropiado control y una mejora continua de la seguridad de la información dentro de la institución.

#### 1.7.1.2 Objetivos específicos

- Realizar el análisis teórico de la Norma ISO[27] 27001, para desarrollar la propuesta.
- Efectuar un estudio de la situación actual del Grupo Social FEPP para obtener un diagnóstico del estado de seguridad de la información.
- Desarrollar una propuesta documentada que le permita al Grupo Social FEPP mantener un control recomendable en cuanto a seguridad de la información.
- Determinar el costo beneficio en la implantación del SGSI[28], para que de esta manera las autoridades competentes tomen en cuenta esta propuesta.

## 1.8 JUSTIFICACIÓN

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes dentro del Grupo Social FEPP. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen institucional necesarios para lograr los objetivos del Grupo Social FEPP, además, cabe señalar que las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el "hacking"[29] o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente

[27] Organización Internacional de Normalización
[28] Sistema de Gestión de Seguridad de la Información
[29] Refiérase al glosario de términos.

desde dentro de la propia institución o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos, y en este contexto el Grupo Social FEPP debe estar preparado.

El SGSI[30] estará dirigido al cumplimiento de la legalidad, la adaptación dinámica y puntual de las condiciones variables del entorno, así como de la protección adecuada de la información para asegurar el máximo beneficio.

La norma en mención cubre varias áreas de conocimiento en el tratamiento de la información relacionada con su seguridad, en donde describe que actividades deben realizarse en relación a la gestión, diseño, implantación y evaluación de las mismas.

## 1.9 ALCANCE

Presentar el planteamiento del presente proyecto es la definición del Sistema de Gestión de la Seguridad de la Información en el Grupo Social FEPP, la cual permita mejorar la gestión, administración y seguridad de la sensible información de la institución, mediante la implantación de la norma ISO 27001:2005, con el fin de que, a futuro la mencionada institución pueda certificarse.

## 1.10 LIMITANTES

- No contar con un esquema de comunicación interna que informe la importancia de la seguridad de la información.
- Difícil adaptación del personal del Grupo Social FEPP a las nuevas políticas de seguridad.

[30] Sistema de Gestión de Seguridad de la Información

- Desinterés de la Dirección Gerencial en la aplicación y continuidad de la norma.

## 1.11 RESULTADOS ESPERADOS

- Establecer las bases para la gestión de la Seguridad de la Información en el Grupo Social FEPP.
- Compromiso de todos quienes conforman el Grupo Social FEPP para que el Sistema de Gestión de Seguridad de la Información tenga éxito.
- Debido a que no existe un sistema ciento por ciento seguros en cuanto a la seguridad de la información, es importante que el personal del Grupo Social FEPP esté consciente el riesgo que conlleva manejar la sensible información que esta dependencia maneja.
- Se espera que esta propuesta se ponga en práctica para el beneficio no solo de la institución sino en el servicio que presta al pueblo ecuatoriano.

# CAPÍTULO II

# 2 FUNDAMENTACIÓN

## 2.1 SEGURIDAD DE LA INFORMACIÓN

La Seguridad[31] de la Información[32] se refiere a la Confidencialidad[33,] Integridad[34] y Disponibilidad[35] de la información y datos, independientemente de la forma que los datos pueden tener: electrónicos, impresos, audio u otras formas.

Además, la seguridad de la información involucra la implementación de estrategias que cubran los procesos en donde la información es el activo primordial. Estas estrategias deben tener como punto primordial el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo, es decir, que ayuden a proteger y salvaguardar tanto información como los sistemas que la almacenan y administran.

Cabe mencionar que la seguridad es un proceso continuo de mejora por lo que las políticas y controles establecidos para la protección de la información deberán revisarse y adecuarse, de ser necesario, ante los nuevos riesgos que surjan, a fin de tomar las acciones que permitan reducirlos y en el mejor de los casos eliminarlos.

[31]Refiérase al Glosario de Términos
[32] Refiérase al Glosario de Términos
[33] Refiérase al Glosario de Términos
[34] Refiérase al Glosario de Términos
[35] Refiérase al Glosario de Términos

## 2.2 ¿QUÉ ES UN SGSI?

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System.

Se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

Los términos *Confidencialidad, Integridad y Disponibilidad* constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

- **Confidencialidad:** la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

- **Integridad:** mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

- **Disponibilidad:** acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, este proceso es el que constituye un SGSI[36].

[36]Sistema de Gestión de Seguridad de la Información

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.

## 2.3 ¿QUE INCLUYE UN SGSI?

- *Manual de seguridad:* documento que expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc., del SGSI.

- *Procedimientos:* documentos que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información.

- *Instrucciones, checklists y formularios:* documentos que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información.

- *Registros:* documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI; están asociados a documentos de los otros tres niveles como output que demuestra que se ha cumplido lo indicado en los mismos.

De manera específica la Norma ISO 27001:2005 (Estándar para la seguridad de la información, norma principal que especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI)) especifica los siguientes documentos:

**2.3.1. ALCANCE DEL SGSI.-** ámbito de la organización que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas (en aquellos casos en los que el ámbito de influencia del SGSI considere un subconjunto de la organización como delegaciones, divisiones, áreas, procesos, sistemas o tareas concretas).

**2.3.2. POLÍTICA Y OBJETIVOS DE SEGURIDAD.-** documento de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información.

**2.3.3. PROCEDIMIENTOS Y MECANISMOS DE CONTROL QUE SOPORTAN AL SGSI.-** aquellos procedimientos que regulan el propio funcionamiento del SGSI.

**2.3.4. ENFOQUE DE EVALUACIÓN DE RIESGOS.-** descripción de la metodología a emplear (cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado), desarrollo de criterios de aceptación de riesgo y fijación de niveles de riesgo aceptables.

**2.3.5. INFORME DE EVALUACIÓN DE RIESGOS.-** estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización.

**2.3.6. PLAN DE TRATAMIENTO DE RIESGOS.-** documento que identifica las acciones de la dirección, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de seguridad de la información, en función de las conclusiones obtenidas de la evaluación de riesgos,

de los objetivos de control identificados, de los recursos disponibles, etc.

**2.3.7. PROCEDIMIENTOS DOCUMENTADOS.-** todos los necesarios para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados.

**2.3.8. REGISTROS.-** documentos que proporcionan evidencias de la conformidad con los requisitos y del funcionamiento eficaz del SGSI.

**2.3.9. DECLARACIÓN DE APLICABILIDAD.**- (SOA -*Statement of Applicability*, en sus siglas inglesas); documento que contiene los objetivos de control y los controles contemplados por el SGSI37, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.

## 2.4 CONTROL DE LA DOCUMENTACIÓN

Para los documentos generados se debe establecer, documentar, implantar y mantener un procedimiento que defina las acciones de gestión necesarias para:

- Aprobar documentos antes de su emisión.
- Revisar y actualizar documentos cuando sea necesario y renovar su validez.
- Garantizar que los cambios y el estado actual de revisión de los documentos están identificados.

37Sistema de Gestión de la Seguridad de la Información

- Garantizar que las versiones relevantes de documentos vigentes están disponibles en los lugares de empleo.
- Garantizar que los documentos se mantienen legibles y fácilmente identificables.
- Garantizar que los documentos permanecen disponibles para aquellas personas que los necesiten y que son transmitidos, almacenados y finalmente destruidos acorde con los procedimientos aplicables según su clasificación.
- Garantizar que los documentos procedentes del exterior estén identificados.
- Garantizar que la distribución de documentos está controlada.
- Prevenir la utilización de documentos obsoletos.
- Aplicar la identificación apropiada a documentos que son retenidos con algún propósito.

## 2.5 ¿CÓMO SE IMPLEMENTA UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN?

Para establecer y Gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA (Planificación, Hacer, Verificar y Actuar), tradicional en los sistemas de gestión de la calidad.

- Plan (Planificar): establecer el SGSI
- Do (Hacer): implementar y utilizar el SGSI
- Check (Verificar): monitorizar y revisar el SGSI
- Act (Actuar): Mantener y Mejorar el SGSI


Ilustración 2.- Ciclo PDCA[38]

### 2.5.1 PLAN.- ESTABLECER EL SGSI

#### 2.5.1.1 Definir el alcance del SGSI

En términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión.

#### 2.5.1.2 Definir una Política de Seguridad que:

- Incluya el marco general y los objetivos de seguridad de la información de la organización.

[38]Fuente : Sistema de Gestión de la Seguridad : http://internetvendeblog.com/2010/02/sistema-de-gestion-de-la-seguridad-de-la-informacion-sgsi/

- Considere requerimientos legales o contractuales relativos a la seguridad de la información.
- Esté alineada con el contexto estratégico de gestión de riesgos de la organización en el que se establecerá y mantendrá el SGSI.
- Establezca los criterios con los que se va a evaluar el riesgo.
- Esté aprobada por la dirección.

**2.5.1.3 Definir una metodología de evaluación del riesgo apropiada para el SGSI** y los requerimientos del negocio, además de establecer los criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable.

Lo primordial de esta metodología es que los resultados obtenidos sean comparables y repetibles (existen numerosas metodologías estandarizadas para la evaluación de riesgos, aunque es perfectamente aceptable definir una propia).

**2.5.1.4 Identificar riesgos:**

- Identificar los activos que están dentro del alcance del SGSI y a sus responsables directos, denominados propietarios.
- Identificar las amenazas en relación a los activos.
- Identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas.

- Identificar los impactos en la confidencialidad, integridad y disponibilidad de los activos.

#### 2.5.1.5 Analizar y evaluar los riesgos

Evaluar el impacto en el negocio de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información.

Evaluar de forma realista la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados.

Identificar y evaluar las distintas opciones de tratamiento de los riesgos para:

- Aplicar controles adecuados.
- Aceptar el riesgo, siempre y cuando se siga cumpliendo con las políticas y criterios establecidos para la aceptación de los riesgos.
- Evitar el riesgo, por ejemplo mediante el cese de las actividades que lo originan.
- Transferir el riesgo a terceros, por ejemplo a compañías aseguradoras.

#### 2.5.1.6. Seleccionar los objetivos de control

El estándar especifica en su “Anexo A” el listado completo de los controles, agrupándolos en once rubros. Para cada uno de ellos define el objetivo y lo describe brevemente.

Cabe aclarar que el anexo A proporciona una buena base de referencia, no siendo exhaustivo, por lo tanto se pueden seleccionar más aún. Es decir, estos 133 controles (hoy) son los mínimos que se deberán aplicar, o justificar su no aplicación, pero esto no da por completa la aplicación de la norma si dentro del proceso de análisis de riesgos aparecen aspectos que quedan sin cubrir por algún tipo de control.

Por lo tanto, si a través de la evaluación de riesgos se determina que es necesaria la creación de nuevos controles, la implantación del SGSI impondrá la inclusión de los mismos, sino seguramente el ciclo no estará cerrado y presentará huecos claramente identificables.

**2.5.1.7. Definir una declaración de aplicabilidad** que incluya:

- Los objetivos de control y controles seleccionados y los motivos para su elección.
- Los objetivos de control y controles que actualmente ya están implantados.
- Los objetivos de control y controles del Anexo A[39] excluidos y los motivos para su exclusión; este es un mecanismo que permite, además, detectar posibles omisiones involuntarias.

### 2.5.2 DO: IMPLEMENTAR Y UTILIZAR EL SGSI

- Definir un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.

[39] Refiérase a los Anexos “Anexo A ISO 27001:2005”

- Implantar el plan de tratamiento de riesgos, con el fin de alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades.

- Implementar los controles anteriormente seleccionados que lleven a los objetivos de control.

- Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles.

- Procurar programas de formación y concienciación en relación a la seguridad de la información a todo el personal.

- Gestionar las operaciones del SGSI.

- Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información.

- Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.

### 2.5.3 CHECK: MONITORIZAR Y REVISAR EL SGSI

La organización deberá ejecutar procedimientos de monitorización y revisión para:

- Detectar a tiempo los errores en los resultados generados por el procesamiento de la información.

- Identificar brechas e incidentes de seguridad.

- Ayudar a la dirección a determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad de la información se desarrollan en relación a lo previsto.

- Detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores.

- Determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.

- Revisar regularmente la efectividad del SGSI, atendiendo al cumplimiento de la política y objetivos del SGSI, los resultados de auditorías de seguridad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas.

- Medir la efectividad de los controles para verificar que se cumple con los requisitos de seguridad.

- Revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que hayan podido producirse en la organización, la tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior requerimientos legales, obligaciones contractuales, etc.

- Realizar periódicamente auditorías internas del SGSI en intervalos planificados.

- Revisar el SGSI por parte de la dirección periódicamente para garantizar que el alcance definido sigue siendo el adecuado y que las mejoras en el proceso del SGSI son evidentes.

- Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.

- Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI.

### 2.5.4 ACT: MANTENER Y MEJORAR EL SGSI

La organización deberá regularmente:

- Implantar en el SGSI las mejoras identificadas.
- Realizar las acciones preventivas y correctivas adecuadas y a las lecciones aprendidas de las experiencias propias y de otras organizaciones.
- Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.
- Asegurarse que las mejoras introducidas alcanzan los objetivos previstos.

## 2.6 HISTORIA DE LA ISO[40]27000

*ISO/IEC 27000* es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

Desde 1901, y como primera entidad de normalización a nivel mundial, BSI (British Standards Institution) es responsable de la publicación de importantes normas como:

- 1979 Publicación BS 5750 - ahora ISO 9001

[40]ISO (International Organization for Standardization)

- 1992 Publicación BS 7750 - ahora ISO 14001
- 1996 Publicación BS 8800 - ahora OHSAS 18001

La norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa -británica o no- un conjunto de buenas prácticas para la gestión de la seguridad de su información.

La primera parte de la norma (BS 7799-1) es una guía de buenas prácticas, para la que no se establece un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que establece los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000.

En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión.

En 2005, con más de 1700 empresas certificadas en BS7799-2, este esquema se publicó por ISO como estándar ISO 27001, al tiempo que se revisó y actualizó ISO17799. Esta última norma se renombra como ISO 27002:2005 el 1 de Julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión.

En Marzo de 2006, posteriormente a la publicación de la ISO27001:2005, BSI publicó la BS7799-3:2006, centrada en la gestión del riesgo de los sistemas de información.

### 2.6.1 LA SERIE 27000

A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares. Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044.

- **ISO 27000:** En fase de desarrollo; Contendrá términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión. Esta norma está previsto que sea gratuita, a diferencia de las demás de la serie, que tendrán un coste.

- **ISO 27001:** Publicada el 15 de Octubre de 2005. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones. Sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005 (nueva numeración de ISO 17799:2005 desde el 1 de Julio de 2007), para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.

  La implantación de ISO/IEC 27001 en una organización es un proyecto que suele tener una duración entre 6 y 12 meses, dependiendo del grado de madurez en seguridad de la

información y el alcance, entendiendo por alcance el ámbito de la organización que va a estar sometido al Sistema de Gestión de la Seguridad de la Información ( en adelante SGSI) elegido. En general, es recomendable la ayuda de consultores externos.

Aquellas organizaciones que hayan adecuado previamente de forma rigurosa sus sistemas de información y sus procesos de trabajo a las exigencias de las normativas legales de protección de datos (p.ej., en España la conocida LOPD y sus normas de desarrollo, siendo el más importante el Real Decreto 1720/2007, de 21 de diciembre de desarrollo de la Ley Orgánica de Protección de Datos) o que hayan realizado un acercamiento progresivo a la seguridad de la información mediante la aplicación de las buenas prácticas de ISO/IEC 27002, partirán de una posición más ventajosa a la hora de implantar ISO/IEC 27001.

La certificación de un SGSI es un proceso mediante el cual una entidad de certificación externa, independiente y acreditada audita el sistema, determinando su conformidad con ISO/IEC 27001, su grado de implantación real y su eficacia y, en caso positivo, emite el correspondiente certificado.

Antes de la publicación del estándar ISO 27001, las organizaciones interesadas eran certificadas según el estándar británico BS 7799-2.

El Anexo C de la norma ISO 27001 muestra las correspondencias del Sistema de Gestión de la Seguridad de la Información (SGSI) con el Sistema de Gestión de la Calidad según ISO 9001:2000 y con el Sistema de Gestión Medio Ambiental según ISO 14001:2004 (ver ISO 14000), hasta el punto de poder llegar a certificar una organización en varias normas y con base en un sistema de gestión común.

El equipo de proyecto de implantación debe estar formado por representantes de todas las áreas de la organización que se vean afectadas por el SGSI, liderado por la dirección y asesorado por consultores externos especializados en seguridad informática, derecho de las nuevas tecnologías, protección de datos y sistemas de gestión de seguridad de la información (que hayan realizado un curso de implantador de SGSI).

- **ISO 27002:** Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO27001 contiene un anexo que resume los controles de ISO 27002:2005.

- **ISO 27003:** En fase de desarrollo. Consistirá en una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.

- **ISO 27004**: Especifica las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase “Do” (Implementar y Utilizar) del ciclo PDCA[41].

[41]Plan, Do, Check,Act (Planear, Hacer, Verificar y Actuar)

- **ISO 27005:** Publicada el 4 de Junio de 2008. Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. El conocimiento de los conceptos, modelos, procesos y términos descritos en la norma ISO/IEC 27001 e ISO/IEC 27002 es importante para un completo entendimiento de la norma ISO/IEC[42] 27005:2008, que es aplicable a todo tipo de organizaciones (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro) que tienen la intención de gestionar los riesgos que puedan comprometer la organización de la seguridad de la información.

- **ISO 27006:** Publicada el 13 de Febrero de 2007. Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSIs) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001 y los SGSIs. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma.

- **ISO 27007:** En fase de desarrollo; su fecha prevista de publicación es Mayo de 2010. Consistirá en una guía de auditoría de un SGSI.

[42]Internacional Electrotechnical Commission (Comisión Electrotécnica Internacional)

- **ISO 27011:** En fase de desarrollo; su fecha prevista de publicación es finales de 2008. Consistirá en una guía de gestión de seguridad de la información específica para telecomunicaciones, elaborada conjuntamente con la ITU (Unión Internacional de Telecomunicaciones).

- **ISO 27031:** En fase de desarrollo; su fecha prevista de publicación es Mayo de 2010. Consistirá en una guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones.

- **ISO 27032:** En fase de desarrollo; su fecha prevista de publicación es Febrero de 2009. Consistirá en una guía relativa a la cyber seguridad.

- **ISO 27033:** En fase de desarrollo; su fecha prevista de publicación es entre 2010 y 2011. Es una norma consistente en 7 partes: gestión de seguridad de redes, arquitectura de seguridad de redes, escenarios de redes de referencia, aseguramiento de las comunicaciones entre redes mediante gateways, acceso remoto, aseguramiento de comunicaciones en redes mediante VPNs y diseño e implementación de seguridad en redes. Provendrá de la revisión, ampliación y remuneración de ISO 18028.

- **ISO 27034:** Fecha de publicación Febrero de 2009. Contiene una guía de seguridad en aplicaciones.

- **ISO 27799:** Publicada el 12 de Junio de 2008. Es un estándar de gestión de seguridad de la información en el sector sanitario aplicando ISO 17799 (actual ISO 27002). Esta norma, al contrario que las anteriores, no la desarrolla el subcomité JTC1/SC27, sino el comité técnico TC 215. ISO 27799:2008 define directrices para apoyar la interpretación y aplicación en la

salud informática de la norma ISO / IEC 27002 y es un complemento de esa norma. ISO 27799:2008 especifica un conjunto detallado de controles y directrices de buenas prácticas para la gestión de la salud y la seguridad de la información por organizaciones sanitarias y otros custodios de la información sanitaria en base a garantizar un mínimo nivel necesario de seguridad apropiado para la organización y circunstancias que van a mantener la confidencialidad, integridad y disponibilidad de información personal de salud. ISO 27799:2008 se aplica a la información en salud en todos sus aspectos y en cualquiera de sus formas, toma la información (palabras y números, grabaciones sonoras, dibujos, vídeos y imágenes médicas), sea cual fuere el medio utilizado para almacenar (de impresión o de escritura en papel o electrónicos de almacenamiento ) y sea cual fuere el medio utilizado para transmitirlo (a mano, por fax, por redes informáticas o por correo), ya que la información siempre debe estar adecuadamente protegida.

# CAPÍTULO III

# 3 DIAGNÓSTICO DE LA SITUACIÓN ACTUAL DEL GRUPO SOCIAL FONDO ECUATORIANO POPULORUM PROGRESSIO

## 3.1 DEFINIR ALCANCE DEL SGSI

Uno de los pasos más importantes a la hora de implementar un SGSI es definir adecuadamente el alcance. ¿Qué ámbito debe cubrir? Este suele ser un tema complicado de decidir, principalmente porque un alcance global, que cubra toda la organización, no suele ser ni la opción más eficiente ni la más eficaz. Hay que pensar que la implantación de un SGSI[43] es un proyecto de gran calado, con repercusiones transversales a todo el alcance que definamos, y cuyas raíces deberían llegar hasta la cultura de la organización. Por tanto, la mejor opción siempre será diseñar un SGSI para un alcance más reducido, optimizando recursos y resultados, y que cuando la filosofía de gestión de la seguridad haya calado y los controles implementados se puedan extender progresivamente hacia toda la organización.

El manejo de la información es similar en todas las empresas del Grupo Social FEPP, se diferencian en el campo o líneas de acción en las que se desenvuelven. Para el caso del Grupo Social FEPP, es indispensable que se defina un alcance global ya que el manejo de la seguridad de la información es de vital importancia en todas las empresas que la conforman por ello es importante realizar un diagnóstico de la situación actual del Grupo Social FEPP, utilizando como base el Anexo A de la Norma 27001:2005.

[43] SGSI Sistema de Gestión de Seguridad de la Información

## 3.2 CMMI

Capability Maturity Model Integration (CCMI) es un modelo de aseguramiento de calidad que contribuye a:

- Integrar las funciones de la organización.
- Mejorar los procesos de la organización a través de mejores prácticas basadas en casos de éxitos identificando objetivos y prioridades de la organización.

### 3.2.1 REPRESENTACIONES

La representación usada en CMMI ofrece una guía para efectuar las actividades de mejora de los procesos y es utilizada en el método de evaluación.

Se cuenta con dos procesos de representación:

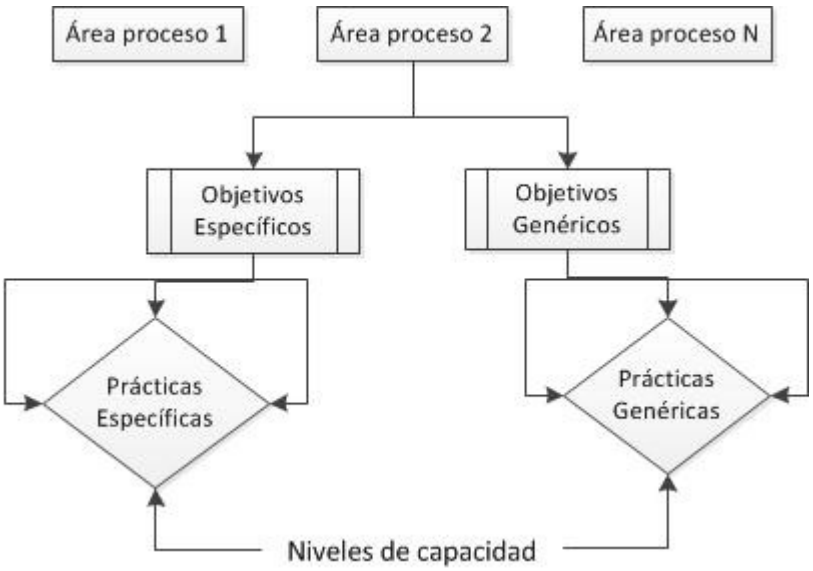


Ilustración 3.- Representación Continua[44]

[44] Fuente: Investigador.

- La representación continúa que trata de mejorar un proceso específico o un conjunto de ellos por lo tanto una organización puede ser certificada para un área de proceso en cierto nivel de capacidad.

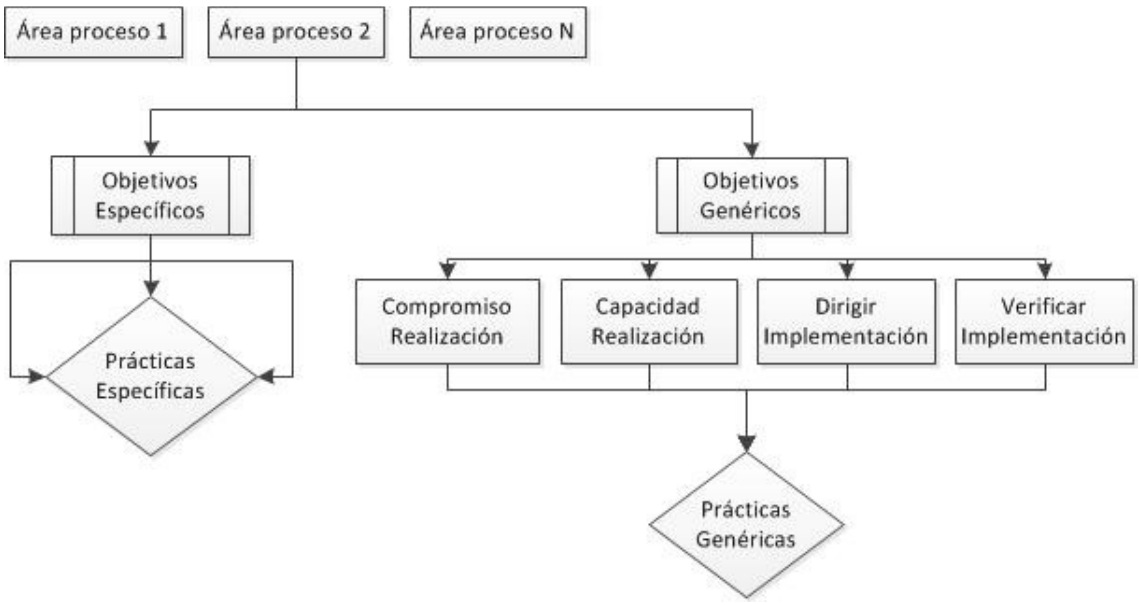


Ilustración 4.- Representación Escalonada.[45]

- La representación escalonada o por etapas que define la mejor de la organización completa según los procesos definidos mediante un método estructurado y sistemático de mejoramiento de procesos. Al alcanzar un nivel, la organización se asegura de contar con una infraestructura robusta en términos de procesos para optar alcanzar el siguiente nivel. Por lo tanto es una organización la que puede ser certificada bajo un nivel, en este caso llamado nivel de madurez.

En la siguiente tabla se muestran los niveles para estos dos tipos de representaciones:

[45] Fuente: Investigador

| | REPRESENTACIÓN CONTINUA | REPRESENTACIÓN ESCALONADA |
|---|---|---|
| | **NIVEL DE CAPACIDAD** | **NIVEL DE MADUREZ** |
| **NIVEL 0** | **INCOMPLETO:**<br><br>Un proceso es denominado "incompleto" cuando uno o más objetivos específicos del área de proceso no son satisfechos. | **NO APLICA** |
| **NIVEL 1** | **REALIZADO:**<br><br>Un proceso[46] es denominado "proceso realizado" cuando satisface todos los objetivos específicos del área de proceso. Soporta y permite el trabajo necesario para producir. | **REALIZADO:**<br><br>La mayoría de los procesos son caóticos. La organización usualmente no provee un ambiente estable para soportar los procesos. Los éxitos en estas organizaciones se deben a la competencia y esfuerzos de la gente dentro de la organización y no al uso de procesos probados. A pesar de este caos, organizaciones pertenecientes al nivel de madurez 1con frecuencia producen productos y servicios que funcionan; sin embargo, ellos frecuentemente exceden sus presupuestos y no cumplen sus planes. Estas organizaciones son caracterizadas por la tendencia a no cumplir con |

[46] Refiérase al Glosario de Términos.

| | | |
|---|---|---|
| | | sus compromisos, al abandono de procesos durante tiempos de crisis, y a la incapacidad para repetir sus éxitos, está caracterizado además por la realización de trabajo redundante[47] , por personas que no comparten sus métodos de trabajo a lo largo de la organización y cuando una persona clave en un área de negocio específica dentro de la organización se marcha, su conocimiento se va con ella y se pierde para la organización. Es claro que en este nivel es donde ninguna organización quiere estar y donde por lo general la mayoría que no tiene sus procesos definidos se encuentra. |

[47] Refiérase al Glosario de Términos.

| | | |
|---|---|---|
| **NIVEL 2** | **MANEJADO:**<br><br>Un proceso es denominado como “proceso manejado” cuando tiene la infraestructura base para apoyar el proceso. El proceso es planeado y ejecutado en concordancia con la política, emplea gente calificada los cuales tienen recursos adecuados para producir salidas controladas; involucra partes interesadas; es monitoreado, controlado y revisado; es evaluado. | **MANEJADO:**<br><br>Se ordena el caos. Las organizaciones se enfocan en tareas cotidianas referentes a la administración. Cada proyecto de la organización cuenta con una serie de procesos para llevarlo a cabo, los cuales son planeados y ejecutados de acuerdo con políticas establecidas; los proyectos utilizan gente capacitada los cuales disponen de recursos para obtener las salidas controladas; se involucra a las partes interesadas; son monitoreados, controlados y revisados; y son evaluados según la descripción del proceso. La disciplina del proceso ayuda a asegurar que existen prácticas y los proyectos son realizados y manejados de acuerdo a los planes documentados. El estado de los artefactos y la entrega de los servicios siguen planes definidos. Acuerdos son establecidos entre partes interesadas y son revisados cuando sea necesario. Los artefactos y servicios son apropiadamente controlados. Estos además satisfacen sus descripciones especificadas, estándares y procedimientos. |

| | | |
|---|---|---|
| **NIVEL 3** | **DEFINIDO:**<br><br>Un proceso denominado “proceso definido” es adaptado desde el conjunto de procesos estándares de la organización de acuerdo a las guías de adaptación de la organización, y aporta artefactos, medidas y otra información de mejora a los activos organizacionales. | **DEFINIDO:**<br><br>Los procesos son caracterizados y entendidos de buena forma, y son descritos en estándares, procedimientos, herramientas y métodos. El conjunto de procesos y estándares de la organización, los cuales son la base para el nivel de madurez 3, es establecido y mejorado continuamente. Estos procesos estándares son usados para estableces consistencia a través de la organización. Los proyectos establecen sus procesos adaptando el conjunto de procesos estándares de la organización de acuerdo a guías a adaptación.<br><br>Los estándares, descripción de procesos y procedimientos para un proyecto, son adaptados desde un conjunto de procesos estándares de la organización a un particular proyecto o unidad organizacional y así son más consistentes. Un proceso definido claramente plantea el propósito, entradas, criterios de entrada, actividades, roles, medidas, pasos de verificación, salidas y criterios de salida. Los procesos son manejados más proactivamente entendiendo las interrelaciones de las actividades y medidas detalladas del proceso, sus artefactos y sus servicios. |

| | | |
|---|---|---|
| **NIVEL 4** | **MANEJADO CUANTITATIVAMENTE**[48]<br><br>Un proceso denominado "proceso manejado cuantitativamente" es controlado usando técnicas estadísticas y otras técnicas cuantitativas. Objetivos cuantitativos para la calidad y realización del proceso son establecidos y usados como criterios para manejar el proceso. | **MANEJADO CUANTITATIVAMENTE**<br><br>La organización y proyectos establecen objetivos cuantitativos para medir la calidad y realización de los procesos y los usa como criterios en el manejo de ellos. Los objetivos cuantitativos son definidos en base a las necesidades de clientes, usuarios finales, organización y actores de los procesos. La calidad y la realización de procesos son entendidos en términos estadísticos y son manejados durante todo el ciclo de vida del proceso. Para subprocesos seleccionados, se recolectan y analizan estadísticamente medidas sobre la realización de procesos. Estas métricas son incorporadas en el repositorio de métricas de la organización para apoyar la toma de decisiones. Causas especiales de variación de procesos son identificadas y cuando sea necesario, las fuentes de estas causas son corregidas para evitar futuras ocurrencias. |
| | | |

[48] Refiérase al Glosario de Términos.

| | | |
|---|---|---|
| **NIVEL 5** | **OPTIMIZACIÓN**<br><br>Un proceso denominado "optimización" es mejorado basado en el entendimiento de causas comunes de variación del proceso. Un proceso en optimización se focaliza en la mejora continua del proceso realizado a través de mejoras incrementales y usando innovación tecnológica. | **OPTIMIZACIÓN**<br><br>Una organización mejora continuamente sus procesos basándose en el conocimiento de las causas comunes de variación inherente en los procesos, se focaliza sobre la mejora continua de los procesos a través de mejoras continuas, incrementales y tecnológicas, Los objetivos de mejora cuantitativa de procesos para la organización son establecidos, continuamente revisados para reflejar cambios en los objetivos del negocio y usados como criterio en la mejora de procesos son medidos y evaluados contra los objetivos de mejora cuantitativa del proceso. |

Luego de haber podido analizar los dos modelos que podemos utilizar y debido a que se tomará en cuenta a todas las empresas y regionales del Grupo Social Fondo Ecuatoriano Populorum Progressio dentro de lo que establece el alcance del SGSI, se trabajará con el modelo de representación escalonada.

## 3.3 ANÁLISIS DE BRECHAS

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| ***A.5*** POLÍTICA DE SEGURIDAD. | ***A.5.1*** Política de la seguridad de la información.<br><br>*Objetivo:* Proporcionar dirección gerencial. | ***A.5.1.1*** Documentar política de seguridad de información. | No se cuenta con un Documento aprobado por el Grupo Social FEPP en cuanto a políticas de seguridad de la información se refiere. |
| | | ***A.5.1.2*** Revisión de la política de seguridad de la información. | No se realiza dicha actividad ya que no se cuenta con políticas de seguridad. |
| ***A.6*** ORGANIZACIÓN | ***A.6.1*** Organización | ***A.6.1.1*** Compromiso de la gerencia con la seguridad | No existe un compromiso formal por parte de |

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| DE LA SEGURIDAD DE LA INFORMACIÓN. | interna.<br><br>*Objetivo:* Manejar la seguridad de la información dentro de la organización. | de la información. | Presidencia del Grupo Social FEPP en cuanto a políticas de seguridad de la información. |
| | | ***A.6.1.2*** Coordinación de la seguridad de la información. | No existe coordinación con los diferentes representantes de la organización. |
| | | ***A.6.1.3*** Asignación de responsabilidades de la seguridad de la información. | No existe asignación formal de responsabilidades de la seguridad de la información. |
| | | ***A.6.1.4*** Proceso de autorización para los medios de procesamiento | No se ha definido procesos de autorización gerencial para los medios de procesamiento de la |

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| | | de información. | información. |
| | | ***A.6.1.5*** Acuerdos de confidencialidad[49]. | No existen acuerdos de confidencialidad, salvo el acuerdo que se especifica en el contrato de trabajo en el departamento de recursos humanos cuando una persona ingresa a la Institución. |
| | | ***A.6.1.6*** Contacto con autoridades. | El Contacto con autoridades es escaso. |
| | | ***A.6.1.7*** Contacto con grupos de interés especial. | El Grupo Social FEPP no mantiene contacto con grupos o foros de seguridad especializados. |

[49]Refiérase al Glosario de Términos

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| | | ***A.6.1.8*** Revisión independiente de la seguridad de la información. | No se realiza ninguna revisión debido a que no se cuenta con políticas formalmente establecidas. |
| | ***A.6.2*** Partes externas<br>*Objetivo:* Entidades externas. | ***A.6.2.1*** Identificación de riesgos relacionados con entidades externas. | Se tienen identificados los riesgos de manera intuitiva. |
| | | ***A.6.2.2*** Tratamiento de la seguridad cuando se trabaja con clientes. | En el Grupo Social FEPP el acceso a la información por parte de los clientes se trata de manera segura y de forma intuitiva ya que no se cuenta con requerimientos de seguridad identificados. |
| | | ***A.6.2.3*** Tratamiento de la seguridad en contratos con | No existe un tratamiento seguro para manejo, acceso |

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| | | terceras personas. | y procesamiento de la información por parte de terceras personas. |
| ***A.7*** GESTIÓN DE ACTIVOS | ***A.7.1*** Responsabilidad por los activos.<br><br>*Objetivo:* Alcanzar y mantener la protección apropiada de los activos de la organización. | ***A.7.1.1*** Inventarios de activos[50]. | Se cuenta con un inventario de activos de hardware[51], pero este documento se lo debe actualizar debido a que hay nuevas adquisiciones de equipos.<br><br>No se tiene un inventario de software[52]. |
| | | ***A.7.1.2*** Propiedad de los activos[53]. | La propiedad de todos los activos corresponde al Grupo Social FEPP. |

[50]Refiérase al Glosario de Términos
[51]Refiérase al Glosario de Términos
[52]Refiérase al Glosario de Términos
[53]Refiérase al Glosario de Términos

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| | | ***A.7.1.3*** Uso aceptable de los activos. | No se encuentra documentado el uso aceptable de activos. |
| | ***A.7.2*** Clasificación de la información.<br><br>*Objetivo:* Asegurar que la información reciba un nivel apropiado de protección. | ***A.7.2.1*** Lineamientos de clasificación. | La información si es clasificada en términos de valor, confidencialidad y grado crítico. |
| | | ***A.7.2.2*** Etiquetado y manejo de la información. | El etiquetado y el manejo de la información no se encuentran estandarizados en el Grupo Social FEPP. |
| ***A.8*** SEGURIDAD DE LOS | ***A.8.1*** Antes del empleo.<br><br>*Objetivo:* Asegurar que los | ***A.8.1.1*** Roles y responsabilidades. | Se encuentran definidos pero no documentados los roles y responsabilidades de los |

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| RECURSOS HUMANOS. | empleados, contratistas y terceros entiendan sus responsabilidades, y sean adecuados para los roles para los cuales se les considera: y reducir el riesgo de robo, fraude o mal uso de los medios. | | empleados para el manejo de la información. |
| | | ***A.8.1.2*** Selección. | Se la realiza de acuerdo a la necesidad y al perfil buscado, según el procedimiento documentado que existe en RRHH. |
| | | ***A.8.1.3*** Términos y condiciones de empleo. | Se realizan contratos por servicios profesionales, ocasionales y por nombramiento y en cada uno |

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| | | | de estos se especifica los términos y condiciones del empleo.<br><br>Por ningún motivo se realiza contratos verbales. |
| | | ***A.8.2.1*** Gestión de responsabilidad | No se cumple en el Grupo Social FEPP. |
| | | ***A.8.2.2*** Capacitación y educación en seguridad de la información. | Se carece de capacitaciones en seguridad de la información. |
| | | ***A.8.2.3*** Proceso disciplinario. | Se cuenta con un proceso disciplinario documentado. |
| | ***A.8.3*** Terminación o cambio de empleo.<br><br>*Objetivo:* Asegurar que los | ***A.8.3.1*** Responsabilidades de terminación. | Se encuentran definidas las responsabilidades para la terminación o cambio de |

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| | empleados, contratistas y usuarios de terceras partes se retiran de una organización o cambian el empleo de una manera ordenada. | | empleo. |
| | | ***A.8.3.2*** Devolución de activos[54]. | Si un empleado se retira de la institución, por norma general tiene que entregar todos los activos a la Unidad de Activos Fijos, caso contrario se procede a descontar de la liquidación correspondiente. |
| | | ***A.8.3.3*** Eliminación de derechos de acceso[55]. | No se encuentra definido claramente. |

[54]Refiérase al Glosario de Términos

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| ***A.9*** *S*EGURIDAD FISICA Y AMBIENTAL. | ***A.9.1*** Áreas seguras.<br><br>*Objetivo:* Prevenir el acceso físico no autorizado, daño e interferencia a las instalaciones e información de la organización. | ***A.9.1.1*** Perímetro de seguridad física. | Todas las aéreas que conforman el Grupo Social FEPP si se encuentran definidos perímetros de seguridad física.<br><br>En informática no existe un perímetro de seguridad eficiente. |
| | | ***A.9.1.2*** Controles de entrada físicos. | No existen controles de entrada eficientes. |
| | | ***A.9.1.3*** Seguridad de oficinas, habitaciones y medios. | No existe un diseño de seguridad física apropiado en las oficinas del Grupo Social FEPP. |

[55]Refiérase al Glosario de Términos

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| | | ***A.9.1.4*** Protección contra amenazas externas y ambientales. | Se cuenta con un plan de protección física contra amenazas[56]. |
| | | ***A.9.1.5*** Trabajo en área seguras. | No existen ningún tipo de lineamientos para trabajar en áreas seguras. |
| | | ***A.9.1.6*** Áreas de acceso público, entrega y carga. | Existe control en los puntos de acceso protegiendo de esta manera puntos de acceso no autorizados. |
| | ***A.9.2*** Seguridad de los equipos.<br><br>*Objetivo:* Prevenir pérdidas, daños, robo o comprometer | ***A.9.2.1*** Ubicación y protección del equipo. | Los equipos no se encuentran protegidos y su ubicación no son de lo más eficientes. |

[56] Refiérase al Glosario de Términos

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| | los activos e interrupción de las actividades de la organización. | | |
| | | ***A.9.2.2*** Servicios públicos | Todos los equipos en el Grupo Social FEPP cuentan con ups[57] y reguladores de voltaje de esta manera se protege de fallas causadas por servicios públicos. |
| | | ***A.9.2.3*** Seguridad en el cableado. | En cuanto al cableado se considera protegido ya que se cuenta con un cableado estructurado y una conexión a tierra protegiendo los servicios de información. |

[57]Refiérase al Glosario de Términos

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| | | ***A.9.2.4*** Mantenimiento de equipo. | No se realiza mantenimiento preventivo de equipos en el Grupo Social FEPP. |
| | | ***A.9.2.5*** Seguridad del equipo fuera del local. | No se ha establecido un procedimiento para la manipulación del equipo fuera del Grupo Social FEPP. |
| | | ***A.9.2.6*** Eliminación seguro o re-uso del equipo. | No se realiza ningún chequeo que asegure que se haya removido o sobre escrito data confidencial del equipo. |
| | | ***A.9.2.7*** Traslado de propiedad. | No se realiza control alguno sobre software llevado fuera de la institución así como tampoco de la información |

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| | | | transportada a través de medios electrónicos.<br><br>De los equipos se llena un documento de autorización de salida de equipos. |
| ***A.10*** GESTIÓN DE COMUNICACIONES Y OPERACIONES. | ***A.10.1*** Procedimientos y responsabilidades de operación.<br><br>*Objetivo:* Asegurar la operación correcta y segura de los recursos de tratamiento de la información. | ***A.10.1.1*** Procedimientos de operación de documentos. | No existen procedimientos de operación de documentos. |
| | | ***A.10.1.2*** Gestión de | No existe control de cambios en los medios y sistemas de |

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| | | cambio | procesamiento de la información. |
| | | ***A.10.1.3*** Segregación de deberes. | Se encuentra segregadas las responsabilidades y deberes de cada uno de las personas dentro de la institución, pero no se encuentran plasmadas en un documento. |
| | | ***A.10.1.4*** Separación de los medios de desarrollo y operacionales. | No se encuentran separadas. |
| | ***A.10.2*** Gestión de entrega de servicio de tercera parte. | ***A.10.2.1*** Entrega del servicio. | No se encuentra establecido en el contrato ningún control de seguridad para con terceros. |
| | | ***A.10.2.2*** Monitoreo y | No se realiza monitoreo de |

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| | | revisión de los servicios de terceros. | los servicios provistos por terceros. |
| | | ***A.10.2.3*** Manejar los cambios en los servicios de terceros. | No se realiza ya que no se cuenta con políticas ni procedimientos de seguridad existentes. |
| | ***A.10.3*** Planificación y aceptación del sistema.<br><br>*Objetivo:* Minimizar el riesgo de fallas de los sistemas. | ***A.10.3.1*** Gestión de capacidad. | No se realiza monitoreo de los recursos que aseguren un buen desempeño del sistema requerido. |
| | | ***A.10.3.2*** Aceptación del sistema. | No se realiza ya que no se cuenta con criterios de aceptación establecidos para sistemas nuevos ni tampoco |

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| | | | para actualizaciones. |
| | ***A.10.4*** Protección contra código malicioso y movible.<br><br>*Objetivo:* Proteger la integridad del software y de la información. | ***A.10.4.1*** Controles contra software malicioso. | No se cuenta con controles documentados que ayuden a proteger la integridad de la información contra software malicioso. |
| | | ***A.10.4.2*** Controles contra códigos móviles. | No aplica ya que no se cuenta con códigos móviles. |
| | ***A.10.5*** Copia de seguridad.<br><br>*Objetivo:* Mantener la integridad y disponibilidad de la información y los recursos de procesamiento de la información. | ***A.10.5.1*** Back-up o respaldo de la información. | Se realizan respaldos de la información pero no es un proceso documentado. |

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| | ***A.10.6*** Gestión de seguridad de la red.<br><br>*Objetivo:* Asegurar la protección de la información en las redes y la protección de su infraestructura de soporte. | ***A.10.6.1*** Controles de red. | No se cuenta con un adecuado manejo y control de la red debido a que no se cuenta con procedimientos formales. |
| | | ***A.10.6.2*** Seguridad de los servicios de red. | No se encuentran plenamente identificados los dispositivos de seguridad así como tampoco niveles de servicio que puedan ser incluidos en contratos de servicios de red. |
| | ***A.10.7*** Manejo de medios | ***A.10.7.1*** Gestión de los | No existen procedimientos |

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| | de información.<br><br>*Objetivo:* Prevenir la divulgación, modificación, eliminación o destrucción no autorizada de los activos, e interrupción de las actividades del negocio. | medios removibles. | para la gestión de medios removibles en el Grupo Social FEPP. |
| | | ***A.10.7.2*** Eliminación de medios. | No se cuenta con procedimientos para la eliminación de medios en el Grupo Social FEPP. |
| | | ***A.10.7.3*** Procedimientos de manejo de la información. | No se cuenta con procedimientos documentados para el manejo y almacenaje de la |

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| | | | información en el Grupo Social FEPP. |
| | | ***A.10.7.4*** Seguridad de documentación del sistema. | No se encuentra debidamente protegida la documentación de un acceso no autorizado. |
| | ***A.10.8*** Intercambio de información.<br><br>*Objetivo:* Mantener la seguridad de la información y el software dentro de una organización y con cualquier entidad externa. | ***A.10.8.1*** Procedimientos y políticas de información y software. | No se encuentra establecida ninguna política ni procedimiento que proteja el intercambio de la información a través del uso de medios de comunicación. |
| | | ***A.10.8.2*** Acuerdos de intercambio. | No se han establecido acuerdos para el intercambio de la información tanto |

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| | | | interno como externo. |
| | | ***A.10.8.3*** Medios físicos en tránsito. | No se cuenta con procedimientos para el transporte de la información más allá de los límites físicos del Grupo Social FEPP. |
| | | ***A.10.8.4*** Mensajes electrónicos. | No se protege adecuadamente los mensajes electrónicos. |
| | | ***A.10.8.5*** Sistemas de información comercial. | No aplica. |
| | ***A.10.9*** Servicio de comercio electrónico.<br><br>*Objetivo:* Asegurar la | ***A.10.9.1*** Comercio electrónico. | No aplica. |

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| | seguridad de servicios de comercio electrónico y su utilización segura. | | |
| | | ***A.10.9.2*** Transacciones en línea. | No aplica. |
| | | ***A.10.9.3*** Información disponible públicamente. | No se tiene establecidas políticas ni procedimientos de seguridad documentadas, que eviten la modificación no autorizada de la información. |
| | ***A.10.10*** Seguimiento.<br><br>*Objetivo:* Detectar las actividades de procesamiento de la | ***A.10.10.1*** Registro de auditoría. | No se realiza actividades de auditoría para la seguridad de la información en el Grupo Social FEPP. |

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| | información no autorizadas. | | |
| | | ***A.10.10.2*** Uso del sistema de monitoreo. | No se ha establecido procedimientos para monitoreo del uso de medios de procesamiento de la información. |
| | | ***A.10.10.3*** Protección de la información del registro. | No se protege la información del registro contra accesos no autorizados. |
| | | ***A.10.10.4*** Registros del administrador y operador. | No se registra las actividades del administrador ni operador del sistema. |
| | | ***A.10.10.5*** Registro de fallas. | No se realiza un registro de fallas. |
| | | ***A.10.10.6*** Sincronización | No existe sincronización de relojes con una fuente de |

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| | | de relojes. | tiempo exacta. |
| ***A.11*** CONTROL DE ACCESOS. | ***A.11.1*** Requisitos del negocio para el control de accesos.<br><br>*Objetivo:* Controlar los accesos de la información. | ***A.11.1.1*** Política del control de acceso. | No se ha establecido políticas de control de acceso documentadas para ninguna de los departamentos de el Grupo Social FEPP. |
| | ***A.11.2*** Gestión de acceso de usuarios.<br><br>*Objetivo:* Asegurar el acceso del usuario autorizado y prevenir el acceso no autorizado a los sistemas de información. | ***A.11.2.1*** Inscripción del usuario. | No existe un procedimiento de inscripción de otorgamiento de accesos a los sistemas de información. |

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| | | ***A.11.2.2*** Gestión de privilegios. | No se realiza el control del uso de privilegios ya que no existe un proceso formal que ayude en esta tarea. |
| | | ***A.11.2.3*** Gestión de la clave del usuario. | No se tiene un proceso formal en gestiones de claves para usuarios. |
| | | ***A.11.2.4*** Revisión de los derechos de acceso del usuario. | No se realiza ninguna revisión de derechos de acceso del usuario. |
| | ***A.11.3*** Responsabilidad de usuarios.<br><br>*Objetivo:* Prevenir el acceso de usuarios no autorizados, y | ***A.11.3.1*** Uso de clave | No se tiene buenas prácticas de uso de claves por parte de los usuarios. |

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| | comprometer o robar la información y los recursos del procesamiento de la información. | | |
| | | ***A.11.3.2*** Equipo de usuario desatendido. | El usuario no se asegura de dar una adecuada protección al equipo. |
| | | ***A.11.3.3*** Política de pantalla y escritorio limpio. | No se han adoptado políticas. |
| | ***A.11.4*** Control de acceso a la red[58].<br><br>*Objetivo:* Prevenir el acceso no autorizado a los | ***A.11.4.1*** Política sobre el uso de servicios de red. | No se tiene políticas definidas de uso de red. |

[58] Refiérase al Glosario de Términos

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| | servicios de red. | | |
| | | ***A.11.4.2*** Autenticación[59] del usuario para conexiones externas. | No se tiene ningún método establecido de autenticación para usuarios remotos. |
| | | ***A.11.4.3*** Identificación del equipo en red. | Se identifica el equipo en red pero todavía no es un estándar para todos los equipos del Grupo Social FEPP. |
| | | ***A.11.4.4*** Protección del puerto de diagnóstico remoto. | No existe protección de puertos. |
| | | ***A.11.4.5*** Segregación en redes. | No existe segregación de redes. |

[59] Refiérase al Glosario de Términos

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| | | ***A.11.4.6*** Control de conexión de redes | El control de conexión de redes es consecuencia de la norma 11.1 no se tiene políticas de control de acceso. |
| | ***A.11.5*** Control de acceso al sistema operativo.<br><br>*Objetivo:* Prevenir el acceso no autorizado a los sistemas operativos. | ***A.11.5.1*** Procedimientos de registro en el Terminal. | No existe procedimiento de registros seguros. |
| | | ***A.11.5.2*** Identificación y autenticación del usuario. | No se ha establecido una técnica de autenticación adecuada para verificar la identidad de usuario. |
| | | ***A.11.5.3*** Sistema de gestión de claves. | No existe un adecuado manejo de claves. |

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| | | ***A.11.5.4*** Uso de utilidades del sistema. | No existe control sobre el uso de programas de utilidad. |
| | | ***A.11.5.5*** Sesión inactiva[60]. | Los usuarios no aplican sesiones inactivas. |
| | | ***A.11.5.6*** Limitación de tiempo de conexión. | No se hace restricción sobre los tiempos de conexión a las aplicaciones. |
| | ***A.11.6*** Control de acceso a las aplicaciones e información.<br><br>*Objetivo:* Prevenir el acceso no autorizado a la información contenida en los sistemas de aplicación. | ***A.11.6.1*** Restricción al acceso a la información. | No existen políticas de control de acceso definidas. |

[60] Refiérase al Glosario de Términos

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| | | ***A.11.6.2*** Aislamiento del sistema sensible. | No se cuenta con sistemas sensibles en el Grupo Social FEPP. |
| | ***A.11.7*** Computación móvil y trabajo a distancia.<br><br>*Objetivo:* Asegurar la seguridad de la información cuando se utilizan recursos de computación móvil y de trabajo a distancia. | ***A.11.7.1*** Computación móvil y comunicaciones. | No se aplica en el Grupo Social FEPP. |
| | | ***A.11.7.2*** Tele-trabajo. | No se aplica en el Grupo Social FEPP |
| ***A.12*** ADQUISICIÓN, DESARROLLO | ***A.12.1*** Requerimientos de seguridad de los sistemas. | ***A.12.1.1*** Análisis y especificación de los requerimientos de | No existen enunciados que ayuden a mejorar los requerimientos de controles |

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN. | *Objetivo:* Asegurar que la seguridad sea una parte integral de los sistemas de información. | seguridad. | de seguridad en los sistemas existen. |
| | ***A.12.2*** Procesamiento correcto en las aplicaciones.<br><br>*Objetivo:* Evitar errores, pérdida, modificación no-autorizada o mal uso de la información en las aplicaciones. | ***A.12.2.1*** Validación de data de insumo. | No se realiza. |
| | | ***A.12.2.2*** Control de procesamiento interno. | No se realiza controles de chequeos de validación en |

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| | | | las aplicaciones. |
| | | ***A.12.2.3*** Integridad del mensaje. | No se han identificado los controles apropiados para identificar los requerimientos para proteger la integridad del mensaje en las aplicaciones. |
| | ***A.12.3*** Controles criptográficos.<br><br>*Objetivo:* Proteger la confidencialidad, autenticidad o integridad de la información a través de medios criptográficos. | ***A.12.3.1*** Política sobre el uso de controles criptográficos[61]. | No se cuenta con políticas para el uso de controles criptográficos. |

[61] Refiérase al Glosario de Términos

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| | | ***A.12.3.2*** Gestión clave. | No se tiene una gestión clave para el uso de técnicas de criptografía. |
| | ***A.12.4*** Seguridad de los archivos del sistema.<br><br>*Objetivo:* Garantizar la seguridad de los archivos del sistema. | ***A.12.4.1*** Control de software operacional. | No se cuenta con procedimientos de control en la instalación de software. |
| | | ***A.12.4.2*** Protección de la data de prueba del sistema. | No se cuenta con protección alguna. |
| | | ***A.12.4.3*** Control de acceso al código fuente del programa. | Las restricciones al código fuente son mínimas. |

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| | ***A.12.5*** Seguridad de los procesos de desarrollo y soporte.<br><br>*Objetivo:* Mantener la seguridad del software e información del sistema de aplicación. | ***A.12.5.1*** Procedimientos de control de cambio. | No se cuenta con procedimientos formales para el control de cambios. |
| | | ***A.12.5.2*** Revisión técnica de las aplicaciones después de cambios en el sistema operativo. | No se realiza una revisión profunda de las aplicaciones después del cambio de sistema operativo. |
| | | ***A.12.5.3*** Restricciones sobre los cambios en los paquetes de software. | No se realiza un control estricto sobre cambios en los paquetes de software. |

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| | | ***A.12.5.4*** Filtración de información. | No existe un control efectivo que permita evitar la filtración de la información. |
| | ***A.12.6*** Gestión de vulnerabilidad técnica.<br><br>*Objetivo:* Reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas publicadas. | ***A.12.6.1*** Control de vulnerabilidades técnicas. | No se obtiene información oportuna sobre las vulnerabilidades técnicas de sistemas de información. |
| ***A.13*** GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA | ***A.13.1*** Reporte de eventos y debilidades de seguridad de la información . | ***A.13.1.1*** Reporte de eventos en la seguridad de la información. | No se reportan eventos de seguridad apropiadamente. |

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| INFORMACIÓN. | *Objetivo:* Asegurar que la información de los eventos y debilidades en la seguridad de la información asociados con los sistemas de información sea comunicada de una manera que permita tomar una acción correctiva oportuna. | | |
| | | ***A.13.1.2*** Reporte de debilidades en la seguridad. | No se reportan por parte de los usuarios debilidades en la seguridad de los sistemas o servicios. |
| | | ***A.13.2.1*** Responsabilidades y procedimientos. | No se han establecido responsabilidades ni procedimientos ante |

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| | | | incidentes de seguridad. |
| | | ***A.13.2.2*** Aprendizaje de los incidentes en la seguridad de la información. | No existe mecanismo alguno que permita identificar costos de incidentes en la seguridad de información. |
| | | ***A.13.2.3*** Recolección de evidencia. | Se realiza seguimiento de control y recolección de evidencias tras un incidente en la seguridad de la información. |
| ***A.14*** GESTIÓN DE LA CONTINUIDAD COMERCIAL. | ***A.14.1*** Aspectos de la seguridad de la información de la gestión de la continuidad comercial.<br><br>*Objetivo:* Contrarrestar las interrupciones de las | ***A.14.1.1*** Incluir seguridad de la información en el proceso de gestión de continuidad comercial. | No aplica. |

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| | actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallas o desastres importantes o desastres en los sistemas de información y asegurar su reanudación oportuna. | | |
| | | ***A.14.1.2*** Continuidad comercial y evaluación del riesgo. | No aplica. |
| | | ***A.14.1.3*** Desarrollar e implementar planes de continuidad incluyendo seguridad de la información. | No aplica. |

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| | | ***A.14.1.4*** Marco referencial para la planeación de la continuidad comercial. | No aplica. |
| | | ***A.14.1.5*** Prueba, mantenimiento y re-evaluación de planes de continuidad comerciales. | No aplica. |
| ***A.15*** CUMPLIMIENTO. | ***A.15.1*** Cumplimiento con requerimientos legales.<br><br>*Objetivo:* Evitar violaciones de cualquier ley, obligación reguladora o contractual y de cualquier requerimiento de seguridad. | ***A.15.1.1*** Identificación de legislación aplicable. | No se han definido requerimientos estatutarios reguladores y contractuales para cada sistema de información. |
| | | ***A.15.1.2*** Derechos de propiedad intelectual | Se encuentra en etapa de trámite. |

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| | | (IPR). | |
| | | ***A.15.1.3*** Protección los registros organizacionales. | Se protege los registros organizacionales contra perdida destrucción y falsificación de la información. |
| | | ***A.15.1.4*** Protección de data y privacidad de información personal. | Existe privacidad de información personal. |
| | | ***A.15.1.5*** Prevención de mal uso de medios de procesamiento de información. | No se realiza prevención a los usuarios de utilizar medios de procesamiento para propósitos no autorizados. |
| | | ***A.15.1.6*** Regulación de controles criptográficos. | No se realiza controles. |

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| | ***A.15.2*** Cumplimiento con las políticas y estándares de seguridad, y el cumplimiento técnico.<br><br>*Objetivo:* Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional. | ***A.15.2.1*** Cumplimiento con las políticas y estándares de seguridad. | No se cumple ya que no se cuenta con políticas y estándares de seguridad. |
| | | ***A.15.2.2*** Chequeo de cumplimiento técnico. | No se realiza chequeo técnico. |
| | ***A.15.3*** Consideraciones de auditoría de los sistemas de información.<br><br>*Objetivo:* Maximizar la efectividad y minimizar las | ***A.15.3.1*** Controles de auditoría de sistemas de información. | No se planea ni ejecuta actividades de auditoría de sistemas de información. |

| DOMINIO | SUB-DOMINIO | ISO | GSFEPP |
|---|---|---|---|
| | interferencias en el proceso de auditoría del sistema de la información. | | |
| | | ***A.15.3.2*** Protección de las herramientas de auditoría de los sistemas de información. | No se protege porque no se cuenta con herramientas de auditoría. |

# 3.4 DIAGNÓSTICO DE LA EMPRESA DE INFORMÁTICA[62] (INFOFEPP)

## 3.4.1 DESCRIPCIÓN GENERAL DE LOS SISTEMAS DE INFORMACIÓN ACTUALES

El Grupo Social Fondo ecuatoriano Populorum Progressio cuenta con un sistema que gestiona y almacena la información financiera que genera la realización de ejercicio contable principalmente desarrollado con los proyectos financiados principalmente con entidades extranjeras, que solicitan como requisito un SGSI[63].

## 3.4.2 DESCRIPCIÓN ACTUAL DE FUNCIONES DE LA UNIDAD INFORMÁTICA

Las funciones que brindan el Departamento de Informática en el Grupo Social FEPP son:

- Administrar las bases de datos.
- Administrar las redes LAN[64].
- Administrar la red de Comunicación.
- Administrar el Portal Web[65] institucional.
- Mantenimiento del hardware.
- Mantenimiento del software.

[62]Refiérase al Glosario de Términos
[63]Sistema de Gestión de Seguridad de la Información.
[64] Local Area Net (Red de área local).
[65] Refiérase al Glosario de Términos

- Soporte técnico y atención al usuario en general.

- Mantener y Administrar el Sistema Administrativo Contable Integrado FEPP.

### 3.4.3 ESTRUCTURA FÍSICA DEL ÁREA

El departamento cuenta con un área administrativa de uso de los empleados, un área de reparación de equipos y un área de servidores.
Los sistemas y servicios ofrecidos a los empleados, están sustentados por el servicio que brindan los servidores, los cuales se describen a continuación:

- Servidor[66] de dominio (Hp Proliant G4).
- Servidor de Base de Datos (Hp Proliant G4).
- Servidor Web (Hp Proliant G4).
- Servidor Proxy internet (PC emula servidor).
- Servidor de Correo (PC emula servidor).
- Servidor Antivirus (Hp Proliant G4).

#### 3.4.3.1 Soporte, Mantenimiento de Hardware[67] y Software[68]

Esta área se encarga de realizar mantenimiento de todo el Hardware existente en el Grupo Social FEPP. Revisión del Software ya sea actualización de Sistemas Operativos que tenga la institución, instalación de utilitarios y antivirus.

[66] Refiérase al Glosario de Términos
[67] Refiérase al Glosario de Términos
[68] Refiérase al Glosario de Términos

Mantener el antivirus[69] corporativo con las últimas actualizaciones. Realizar un inventario informático anual de Hardware y Software.

### 3.4.4 DIAGNÓSTICO DE LA RED

#### 3.4.4.1 Administración de la Red

Los Administradores de la red LAN deberán mantener una red operativa, eficiente, segura, constantemente monitoreada y con una planeación adecuada y propiamente documentada.

Sus objetivos son:

- Mejorar la continuidad en la operación de la red con mecanismos adecuados de control y monitoreo, de resolución de problemas y de suministro de recursos.
- Hacer uso eficiente de la red y utilizar mejor los recursos, como por ejemplo, el ancho de banda.
- Reducir costos por medio del control de gastos y de mejores mecanismos de cobro.
- Hacer la red más segura, protegiéndola contra el acceso no autorizado, haciendo imposible que personas ajenas puedan entender la información que circula en ella.
- Controlar cambios y actualizaciones en la red de modo que ocasionen las menos interrupciones posibles, en el servicio a los usuarios.

[69] Refiérase al Glosario de Términos

El edificio del Grupo Social FEPP cuenta con una red LAN Ethernet[70] con cableado estructurado de datos de categoría 6 para los pisos del edificio. Para los switchs de frontera el edificio cuenta con switchs D-link para los pisos 1, 2, 3, 4.

El direccionamiento actual es de una red clases C, contando con una red general 192.168.3.0 para la red de datos. No cuenta con una estructura de VLANs[71]. La topología de la red es de tipo estrella, los protocolos utilizados son TCP/IP, las direcciones IP son dinámicas.

Todos los usuarios tienen acceso Internet a través de un proxy[72] y siempre controlando el acceso a páginas no recomendadas. Los Servidores tampoco tienen acceso a Internet por seguridad.

Existe un solo antivirus licenciado para la utilización en todas las máquinas. En lo que se refiere a instalaciones el edificio cuenta conexiones seguras tanto de red como eléctricas.

[70] Refiérase al Glosario de Términos.
[71] Refiérase al Glosario de Términos
[72] Refiérase al Glosario de Términos

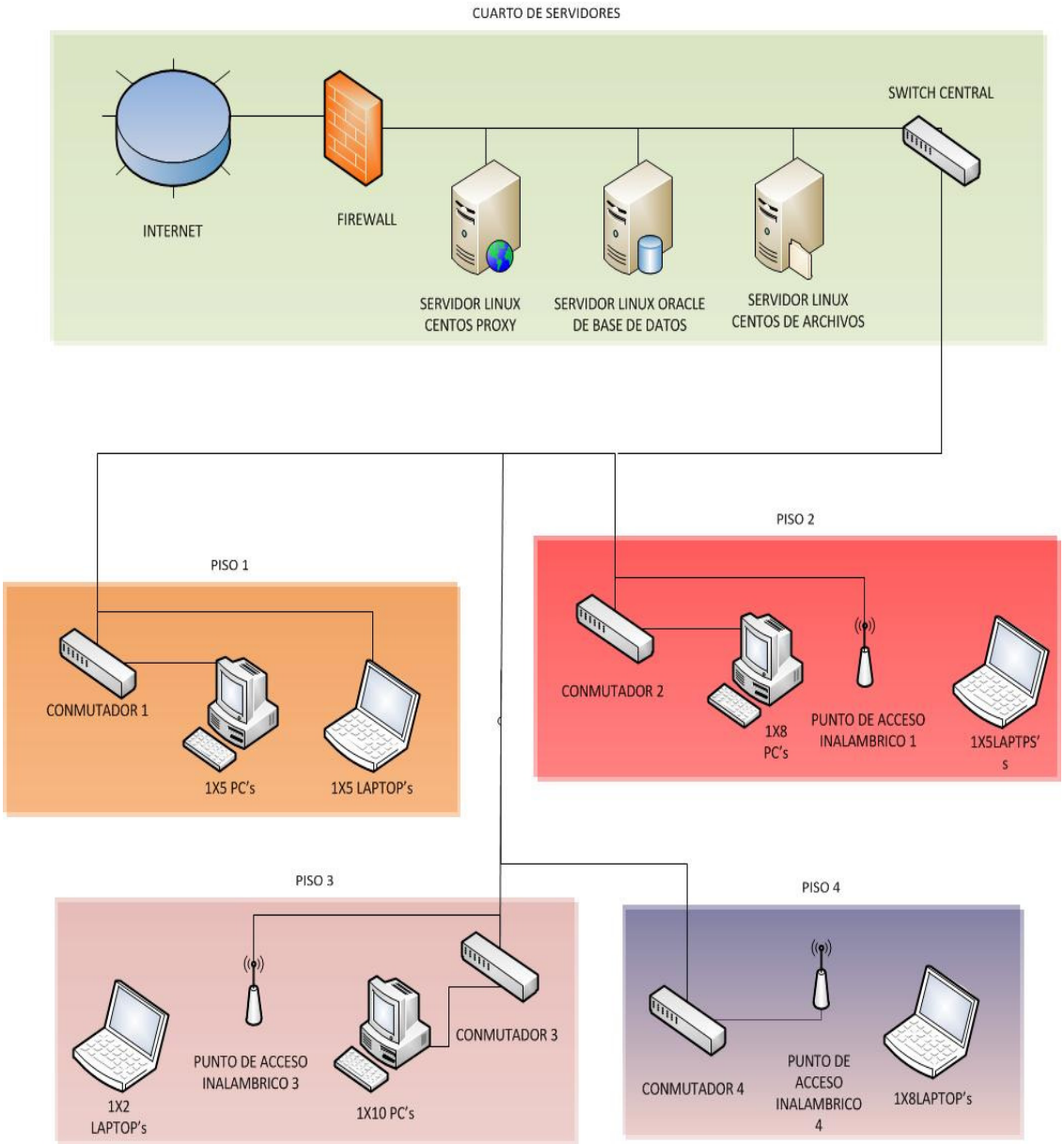


Ilustración 3.-Diagrama de Red del GSFEPP[73].

### 3.4.5 SEGURIDAD EN LA RED DE DATOS

Actualmente no se cuenta con políticas de manejo de puertos y permisos para el acceso a la información.

[73]Fuente: Investigador.

El área de servidores no cuenta con un cuarto frio además de no contar con todas las seguridades de acceso.

Lamentablemente ningún proceso, ya sea de instalación o procedimiento de recuperación se encuentra documentado todo es realizado en base a conocimientos y experiencia de quienes administran la red, así como tampoco existen un plan de contingencias que pueda prevenir cualquier tipo de riesgos.

### 3.4.6 ADMINISTRACIÓN DE BASES DE DATOS[74].

El Administrador de Base de Datos es el encargado de crear y configurar los servidores donde reposan las bases de datos del sistema, instalando clientes y estableciendo la conectividad al servidor. El respaldo de la Base de Datos se lo realiza una vez por semana estos respaldos no son verificados si funcionan o no y tampoco se tiene la política de almacenarlos en distintos lugares para respaldo.

Las contraseñas de los usuarios son asignadas la primera vez y después son cambiadas por el usuario en el primer inicio de sesión, así también solo se les da privilegios como usuario mas no de administrador.

Se cuenta con Oracle 11g en versión freeware[75] para Linux y cuya administración se hace a través de otro motor de base de datos como Oracle 10g para Windows.

[74] Refiérase al Glosario de términos.
[75] Refiérase al Glosario de términos.

## 3.5 RIESGOS[76], AMENAZAS[77] Y VULNERABILIDADES[78] DE LA SITUACIÓN ACTUAL DEL GRUPO SOCIAL FEPP

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| ***A.5.1.1*** Documentar política de seguridad de información. | No se cuenta con un Documento aprobado por el Grupo social FEPP en cuanto a políticas de seguridad de la información se refiere. | No contar con un documento que contenga lineamientos, escritos puede ocasionar que no se proceda de forma correcta en salvaguardar la información. | Impropio proceder en el manejo de la información. |
| ***A.5.1.2*** Revisión de la política de seguridad de la información. | No se realiza dicha actividad ya que no se cuenta con políticas de seguridad. | No se asegura la continua idoneidad, eficiencia y efectividad sino se realiza una | Se es vulnerable a fuga de información. |

[76]Refiérase al glosario de términos.
[77]Refiérase al glosario de términos.
[78]Refiérase al glosario de términos.

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| | | revisión de políticas de seguridad de la información. | |
| ***A.6.1.1*** Compromiso de la gerencia con la seguridad de la información. | No existe un compromiso formal por parte de Dirección del Grupo Social FEPP en cuanto a políticas de seguridad de la información. | El no contar con un compromiso formal puede conllevar a que no exista una adecuada gestión de control y seguridad de la información por parte del personal del Grupo Social FEPP. | Se es vulnerable a fuga de información. |
| ***A.6.1.2*** Coordinación de la seguridad de la información. | No existe coordinación con los diferentes representantes de la organización. | El no coordinar con las diferentes áreas ocasionaría que el personal cometa errores en cuanto a la seguridad de la información. | Pérdida, destrucción de la información. |
| ***A.6.1.3*** Asignación de responsabilidades de la | No existe asignación formal de responsabilidades de la seguridad de | Si no se asigna formalmente responsabilidades en la | Pérdida, mal uso de la |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| seguridad de la información. | la información. | seguridad de la información puede provocar varios percances en el desarrollo de actividades de las diferentes áreas del Grupo Social FEPP. | información. |
| ***A.6.1.4*** Proceso de autorización para los medios de procesamiento de información. | No se ha definido procesos de autorización gerencial para los medios de procesamiento de la información. | El no contar con procesos de autorización repercute directamente en no tener un buen desenvolvimiento de los procesos en los medios involucrados de procesamiento de la información. | No se garantiza la protección de la información. |
| ***A.6.1.5*** Acuerdos de confidencialidad. | No existen acuerdos de confidencialidad, salvo el acuerdo que se especifica en el contrato de trabajo en el departamento de | El no contar con acuerdos de confidencialidad claramente definidos conlleva a que exista fuga de información. | Fuga de información. |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| | recursos humanos cuando una persona ingresa a la Institución. | | |
| ***A.6.1.6*** Contacto con autoridades. | El Contacto con autoridades es escaso. | Al no existir un permanente contacto con las autoridades y no tener registro de ellas puede ocasionar que los acuerdos a los que se haya llegado no se den por completo o peor aún se omitan. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.6.1.7*** Contacto con grupos de interés especial. | El Grupo Social FEPP no mantiene contacto con grupos o foros de seguridad especializados. | El no mantener contacto con algún grupo de interés o foros, puede tener como consecuencia el no estar totalmente al día en cuanto a nuevas tecnologías o nuevas | Nueva forma de vulnerar y conseguir quebrantar la seguridad. |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| | | amenazas. | |
| ***A.6.1.8*** Revisión independiente de la seguridad de la información. | No se realiza ninguna revisión debido a que no se cuenta con políticas formalmente establecidas. | No contar con políticas formalmente establecidas puede ocasionar el no proceder de forma correcta en salvaguardar la información. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.6.2.1*** Identificación de riesgos relacionados con entidades externas. | Se tienen identificados los riesgos de manera intuitiva. | Si los riesgos están identificados de manera intuitiva, se corre el riesgo de que no se encuentren contemplados todos, lo que ocasionaría la falla o interrupción de todos los demás procesos e incluso la pérdida de información. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.6.2.2*** Tratamiento de la | En el Grupo Social FEPP el acceso a | El no tratar adecuadamente la | Manipulación inadecuada de la |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| seguridad cuando se trabaja con clientes. | la información por parte de los clientes no se trata de manera segura y de forma intuitiva ya que no se cuenta con requerimientos de seguridad identificados. | seguridad al momento de trabajar con clientes, es posible que se produzca fallas de confidencialidad, integridad y disponibilidad de la información. | información. |
| ***A.6.2.3*** Tratamiento de la seguridad en contratos con terceras personas. | No existe un tratamiento seguro para manejo, acceso y procesamiento de la información por parte de terceras personas. | Al no contar con acuerdos de confidencialidad en contratos a terceros implica que puede existir fuga de información, ya que estas personas podrían hacer uso de información que solo le compete a la Institución. | Vulnerabilidad en la seguridad de la información. |
| ***A.7.1.1*** Inventarios de activos. | Se cuenta con un inventario de activos de hardware, pero este | Al no contar con un inventario de activos no se puede | No garantizar la integridad y disponibilidad de la información. |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| | documento se lo debe actualizar debido a que hay nuevas adquisiciones de equipos.<br><br>No se tiene un inventario de software. | asegurar la protección total de la información lo que además ocasionaría perdida de la misma. | |
| ***A.7.1.2*** Propiedad de los activos. | La propiedad de todos los activos corresponde al Grupo Social FEPP. | Se debe tener control y registro de todos y cada uno de los activos ya que se podría incurrir en uso indebido de dichos activos. | Fuga de información. |
| ***A.7.1.3*** Uso aceptable de los activos. | No se encuentra documentado el uso aceptable de activos. | El no hacer un buen uso de los activos puede provocar que estos se encuentren subutilizados en cuanto a los equipos y en lo que respecta a la información, puede ocasionar que quienes hacen | No garantizar disponibilidad de la información. |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| | | uso de la información no lo haga de manera adecuada. | |
| ***A.7.2.1*** Lineamientos de clasificación. | La información si es clasificada en términos de valor, confidencialidad y grado crítico. | Si no se tuviera la información clasificada se puede correr el riesgo de no asegurar que la información recibe el nivel de protección adecuado. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.7.2.2*** Etiquetado y manejo de la información. | El etiquetado y el manejo de la información no se encuentran estandarizados en el Grupo Social FEPP. | El no tener un estándar para etiquetar la información implica que esta se pueda extraviar, confundir o que esta no reciba el nivel de protección adecuado. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| | | | |
| ***A.8.1.1*** Roles y responsabilidades. | Se encuentran definidos pero no documentados los roles y responsabilidades de los empleados para el manejo de la información. | El que un funcionario no tenga totalmente claro cuáles son sus funciones o roles dentro de la Organización puede acarrear el riesgo de robo, fraude o uso inadecuado de las instalaciones. | No garantiza la confidencialidad de la información. |
| ***A.8.1.2*** Selección. | Se la realiza de acuerdo a la necesidad y al perfil buscado, según el procedimiento documentado que existe en RRHH. | Al no realizar una verificación de datos por parte de Recursos Humanos puede ocasionar que algunas personas presenten información ilegitima. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| ***A.8.1.3*** Términos y condiciones de empleo. | Se realizan contratos por servicios profesionales, ocasionales y por nombramiento y en cada uno de estos se especifica los términos y condiciones del empleo.<br><br>Por ningún motivo se realiza contratos verbales. | No Existe riesgo ya que la institución cumple con este requisito. | N/A |
| ***A.8.2.1*** Gestión de responsabilidad. | No se cumple en el Grupo Social FEPP. | No contar con un documento que contenga lineamientos, escritos puede ocasionar que no se proceda de forma correcta en salvaguardar la información. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.8.2.2*** Capacitación y | Se carece de capacitaciones en | El no contar con | No garantizar la integridad y |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| educación en seguridad de la información. | seguridad de la información. | capacitaciones se corre el riesgo de que la seguridad en la información no sea manejada correctamente por el personal del Grupo Social FEPP. | disponibilidad de la información. |
| ***A.8.2.3*** Proceso disciplinario. | Se cuenta con un proceso disciplinario documentado. | No existe riesgo ya que el Grupo Social FEPP cumple con este requerimiento. | N/A |
| ***A.8.3.1*** Responsabilidades de terminación. | Se encuentran definidas las responsabilidades para la terminación o cambio de empleo. | El definir responsabilidades para la terminación o cambio de empleo ocasiona que pueda existir perdida de equipos o de la información. | Perdida de la información. |
| ***A.8.3.2*** Devolución de | Si un empleado se retira de la institución, por norma general tiene | No existe riesgo ya que el Grupo Social FEPP cumple | N/A |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| activos. | que entregar todos los activos a la Unidad de Activos Fijos, caso contrario se procede a descontar de la liquidación correspondiente. | con este requisito. | |
| ***A.8.3.3*** Eliminación de derechos de acceso. | No se encuentra definido claramente. | El tener acceso a la información después de que un empleado ha terminado con su contrato, implica graves riesgos en la seguridad de la información, ya que se puede producir un mal uso de esta. | Pérdida y manipulación de la información. |
| ***A.9.1.1*** Perímetro de seguridad física. | Todas las áreas que conforman el Grupo Social FEPP si se encuentran definidos perímetros de seguridad física.<br><br>En informática no existe un perímetro | El no contar con un perímetro de seguridad puede provocar el acceso no autorizado de terceras personas por ende poner en riesgo la seguridad | No garantizar la confidencialidad, integridad y disponibilidad de la información. |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| | de seguridad eficiente. | de la información. | |
| ***A.9.1.2*** Controles de entrada físicos. | No existen controles de entrada eficientes. | El no tener un control de entrada eficiente puede provocar que se filtren personas, equipos, etc. que provoquen riesgos en la seguridad. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.9.1.3*** Seguridad de oficinas, habitaciones y medios. | No existe un diseño de seguridad física apropiado en las oficinas del Grupo Social FEPP. | Si no existe un diseño de seguridad apropiado provoca que se ponga en riesgo la seguridad tanto de los funcionarios como de la información. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.9.1.4*** Protección contra amenazas externas y | Se cuenta con un plan de protección física contra amenazas. | No existe riesgo ya que el Grupo Social FEPP cumple | N/A |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| ambientales. | | con este requerimiento. | |
| ***A.9.1.5*** Trabajo en área seguras. | No existen ningún tipo de lineamientos para trabajar en áreas seguras. | El no trabajar en áreas seguras puede acarrear un peligro inminente para todas las personas quienes laboran en las diferentes áreas de la Institución. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.9.1.6*** Áreas de acceso público, entrega y carga. | Existe control en los puntos de acceso protegiendo de esta manera puntos de acceso no autorizados. | En este tipo de accesos no existe riesgos ya que el Grupo Social FEPP cumple con este requerimiento. | N/A |
| ***A.9.2.1*** Ubicación y protección del equipo. | Los equipos no se encuentran protegidos y su ubicación no son de lo más eficientes. | El no contar con equipos protegidos en una buena ubicación puede llevar a la pérdida de los mismos, ya sea | Perdida de información. |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| | | por robo o por fallas. | |
| ***A.9.2.2*** Servicios públicos. | Todos los equipos en el Grupo Social FEPP cuentan con ups y reguladores de voltaje de esta manera se protege de fallas causadas por servicios públicos. | No existe riesgo ya que los equipos del Grupo Social FEPP cumplen con este requisito. | N/A |
| ***A.9.2.3*** Seguridad en el cableado. | En cuanto al cableado se considera protegido ya que se cuenta con un cableado estructurado y una conexión a tierra protegiendo los servicios de información. | Si no se contara con un cableado estructurado esto podría originar problemas de transmisión de datos, y el hecho de que siga creciendo los usuarios podría ocasionar un colapso de toda la red. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.9.2.4*** Mantenimiento de equipo. | No se realiza mantenimiento preventivo de equipos en el Grupo | El no contar con un plan de mantenimiento preventivo de equipos puede ocasionar el | No garantizar la integridad y disponibilidad de la información. |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| | Social FEPP. | deterioro de estos equipos por ende provocar perdida de información. | |
| ***A.9.2.5*** Seguridad del equipo fuera del local. | No se ha establecido un procedimiento para la manipulación del equipo fuera del Grupo Social FEPP. | Si no se establece un procedimiento para la manipulación del equipo puede provocar que se pierdan dichos equipos o que exista un uso indebido del mismo. | No garantizar la confidencialidad de la información. |
| ***A.9.2.6*** Eliminación seguro o re-uso del equipo. | No se realiza ningún chequeo que asegure que se haya removido o sobre escrito data confidencial del equipo. | El no contar con una política de eliminación segura o rehusó del equipo puede provocar que el nuevo usuario acceda a información confidencial. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| | | | |
| ***A.9.2.7*** Traslado de propiedad. | No se realiza control alguno sobre software sacado fuera de la institución así como tampoco de la información transportada a través de medios electrónicos.<br><br>De los equipos se llena un documento de autorización de salida de equipos. | El riesgo que se tiene es que exista un grave peligro de fuga de información, así como también si no se registran los equipos que salen de la institución. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.10.1.1*** Procedimientos de operación de documentos. | No existen procedimientos de operación de documentos. | Si no se cuenta con procedimientos de operación documentados puede ocasionar, que no se tenga claro quiénes son los responsables y cuáles son las funciones que debe cumplir, | No garantizar la confidencialidad, integridad y disponibilidad de la información. |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| | | así como también puede llevar a que algunas personas se conviertan en imprescindibles para la Institución. | |
| ***A.10.1.2*** Gestión de cambio. | No existe control de cambios en los medios y sistemas de procesamiento de la información. | El no contar con un control de cambios puede ocasionar que los sistemas no funcionen adecuadamente al momento de implementarlos. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.10.1.3*** Segregación de deberes. | Se encuentra segregadas las responsabilidades y deberes de cada uno de las personas dentro de la institución, pero no se encuentran plasmadas en un documento. | El no contar con un documento oficial que avale dichas segregaciones conlleva a que en determinado momento se puedan intercambiar deberes y responsabilidades dentro de la institución. | Manejo inadecuado de la información. |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| ***A.10.1.4*** Separación de los medios de desarrollo y operacionales. | No se encuentran separadas. | El no contar con distintos ambientes tanto de desarrollo y de operaciones, corre el riego de que los usuarios accidentalmente manipulen la información del medio operacional. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.10.2.1*** Entrega del servicio. | No se encuentra establecido en el contrato ningún control de seguridad para con terceros. | El no contar con cláusulas claras en cuanto a la entrega del servicio prestado por terceros puede llevar a que estos no cumplan con un servicio eficiente y de calidad. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.10.2.2*** Monitoreo y revisión de los servicios | No se realiza monitoreo de los servicios provistos por terceros. | El no llevar un registro de monitoreo puede acarrear el | No garantizar la confidencialidad, integridad y disponibilidad de la |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| de terceros. | | inconveniente de que no se de cumplimiento a las cláusulas manifestada en los contratos. | información. |
| ***A.10.2.3*** Manejar los cambios en los servicios de terceros. | No se realiza ya que no se cuenta con políticas ni procedimientos de seguridad existentes. | Se debe tener mucho cuidado en cuanto al cambio en los servicios, ya que se puede poner en peligro los servicios de los que depende el Grupo Social FEPP. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.10.3.1*** Gestión de capacidad. | No se realiza monitoreo de los recursos que aseguren un buen desempeño del sistema requerido. | El riesgo que ocasiona es que exista un inadecuado uso de los recursos ocasionando que en algunos casos se subutilice al sistema. | No garantizar la disponibilidad de la información. |
| ***A.10.3.2*** Aceptación del sistema. | No se realiza ya que no se cuenta con criterios de aceptación | El riesgo de no contar con criterios de aceptación es que | No garantizar la confidencialidad, integridad y disponibilidad de la |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| | establecidos para sistemas nuevos ni tampoco para actualizaciones. | se ponga en producción sistemas que no cumplan con todos los requerimientos para los que fue diseñado. | información. |
| ***A.10.4.1*** Controles contra software malicioso. | No se cuenta con controles documentados que ayuden a proteger la integridad de la información contra software malicioso. | Si no se cuenta con controles de software maliciosos se pone en peligro la información ya que se vuelven vulnerables estos sistemas a ataques tanto interna como externamente. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.10.4.2*** Controles contra códigos móviles. | No aplica ya que no se cuenta con códigos móviles. | No existe riesgo. | N/A |
| ***A.10.5.1*** Back-up o respaldo de la información. | Se realizan respaldos de la información pero no es un proceso documentado. | El no llevar un registro de monitoreo puede acarrear el inconveniente de que no se de cumplimiento a las cláusulas | No garantizar la integridad y disponibilidad de la información. |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| | | manifestada en los contratos. | |
| ***A.10.6.1*** Controles de red. | No se cuenta con un adecuado manejo y control de la red debido a que no se cuenta con procedimientos formales. | El no tener un control adecuado de manejo de la red conlleva a que exista acceso no autorizados a la información tanto personal como institucional, poniendo en peligro la seguridad de la información. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.10.6.2*** Seguridad de los servicios de red. | No se encuentran plenamente identificados los dispositivos de seguridad así como tampoco niveles de servicio que puedan ser incluidos en contratos de servicios de red. | El no contar con seguridad de los servicios de red provoca que la red sea vulnerable a ataques a través de estos, y poner en peligro la seguridad de la información. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.10.7.1*** Gestión de los | No existen procedimientos para la | Si no existen procedimientos | No garantizar la confidencialidad, |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| medios removibles. | gestión de medios removibles en el Grupo Social FEPP. | para la gestión de medios removibles, provoca que exista fuga de información, además de provocar uso inadecuado de estos medios. | integridad y disponibilidad de la información |
| ***A.10.7.2*** Eliminación de medios | No se cuenta con procedimientos para la eliminación de medios en el Grupo Social FEPP. | El no tener procedimientos claros que detallen como eliminar aquellos medios que ya no son utilizados puede provocar confusiones ya que se puede eliminar aquellos que aun pueden prestar servicio por más tiempo. | No garantizar la disponibilidad de la información. |
| ***A.10.7.3*** Procedimientos de manejo de la información. | No se cuenta con procedimientos documentados para el manejo y almacenaje de la información en el | El no contar con lineamientos claros puede conducir a que la información esté propensa a | No garantizar la confidencialidad, integridad y disponibilidad de la información. |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| | Grupo Social FEPP. | no ser manejada de forma adecuada o peor aun esta sea divulgada sin autorización alguna. | |
| ***A.10.7.4*** Seguridad de documentación del sistema. | No se encuentra debidamente protegida la documentación de un acceso no autorizado. | Si la documentación no se encuentra debidamente protegida del acceso no autorizado, puede provocar que se manipule indebidamente la información. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.10.8.1*** Procedimientos y políticas de información y software. | No se encuentra establecida ninguna política ni procedimiento que proteja el intercambio de la información a través del uso de medios de comunicación. | Si no se establecen políticas para el intercambio de información puede ocurrir que exista pérdida o manipulación de la información. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.10.8.2*** Acuerdos de | No se han establecido acuerdos para | Si no se cuenta con acuerdos | No garantizar la confidencialidad, |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| intercambio. | el intercambio de la información tanto interno como externo. | que permitan realizar un adecuado intercambio de información puede conducir a que la información no cumpla su objetivo principal de acuerdo al tipo de acuerdo que se haya realizado. | integridad y disponibilidad de la información. |
| ***A.10.8.3*** Medios físicos en tránsito. | No se cuenta con procedimientos para el transporte de la información más allá de los límites físicos del Grupo Social FEPP. | El no contar con procedimientos para el transporte de la información el peligro es que exista manipulación o pérdida de estos medios. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.10.8.4*** Mensajes electrónicos. | No se protege adecuadamente los mensajes electrónicos. | El no tener lineamientos que detallen la protección que se debe realizar al momento de | No garantizar la confidencialidad, integridad de la información. |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| | | proteger los mensajes electrónicos puede llevar a que estos se pierdan o que a través de estos se filtren software de código malicioso. | |
| ***A.10.8.5*** Sistemas de información comercial. | No aplica | No existe riesgo. | N/A |
| ***A.10.9.1*** Comercio electrónico. | No aplica | No existe riesgo. | N/A |
| ***A.10.9.2*** Transacciones en línea. | No aplica | No existe riesgo. | N/A |
| ***A.10.9.3*** Información disponible públicamente. | No se tiene establecidas políticas ni procedimientos de seguridad documentadas, que eviten la modificación no autorizada de la | Si no se cuenta con políticas debidamente establecidas, se pone en riesgo la integridad de la información. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| | información. | | |
| ***A.10.10.1*** Registro de auditoría. | No se realiza actividades de auditoría para la seguridad de la información en el Grupo Social FEPP. | El no contar con auditorías puede acarrear una serie de convenientes como por ejemplo el que se esté trabajando con procedimientos inadecuados e inseguros en lo que respecta a la seguridad de la información. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.10.10.2*** Uso del sistema de monitoreo. | No se ha establecido procedimientos para monitoreo del uso de medios de procesamiento de la información. | Al no documentar los monitoreos realizados acarrea algunos inconvenientes como por ejemplo el que se presente algún problema que a su vez acarree más problemas por no haberlos solucionado a tiempo. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| ***A.10.10.3*** Protección de la información del registro. | No se protege la información del registro contra accesos no autorizados. | El no proteger la parte del registro de los sistemas puede ocasionar el ingreso de intrusos que puedan cambiarla y traer consecuencias graves para los sistemas. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.10.10.4*** Registros del administrador y operador. | No se registra las actividades del administrador ni operador del sistema. | El no registrar las actividades, pueden incurrir en que puedan manipular e incurrir en faltas graves al sistema. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.10.10.5*** Registro de fallas. | No se realiza un registro de fallas. | Si no se realiza un registro de fallas, no se puede establecer un procedimiento que ayude a solucionar rápidamente fallas futuras. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| ***A.10.10.6*** Sincronización de relojes. | No existe sincronización de relojes con una fuente de tiempo exacta. | Si no se cuenta con una sincronización de relojes, es posible que no se tenga una cronología lógica de actividades que puedan presentarse. | No garantizar la disponibilidad de la información. |
| ***A.11.1.1*** Política del control de acceso. | No se ha establecido políticas de control de acceso documentadas para ninguna de los departamentos del Grupo Social FEPP. | Incurrimos en los mismos riesgos ya mencionados anteriormente ya que puede ocasionar el acceso de usuarios no autorizados a información confidencial. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.11.2.1*** Inscripción del usuario. | No existe un procedimiento de inscripción de otorgamiento de accesos a los sistemas de información. | Si no existen procedimientos de otorgamiento de acceso a los sistemas pueden incurrir a que no exista un control | No garantizar la confidencialidad, integridad y disponibilidad de la información. |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| | | efectivo de accesos tanto autorizados como no autorizados. | |
| ***A.11.2.2*** Gestión de privilegios. | No se realiza el control del uso de privilegios ya que no existe un proceso formal que ayude en esta tarea. | El riesgo que este provoca es que se permita acceso a personas no autorizadas a utilizar o manipular información confidencial. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.11.2.3*** Gestión de la clave del usuario. | No se tiene un proceso formal en gestiones de claves para usuarios. | Si no se cuenta con procedimientos documentados para asignar claves a los usuarios, es posible que estas sean conocidas por intrusos que pueden afectar a la seguridad de la información. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.11.2.4*** Revisión de los | No se realiza ninguna revisión de | Si no se revisa los derechos | No garantizar la confidencialidad, |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| derechos de acceso del usuario. | derechos de acceso del usuario. | de acceso al usuario es posible que quien asigna conceda derechos que no les corresponden a otros usuarios. | integridad y disponibilidad de la información. |
| ***A.11.3.1*** Uso de clave. | No se tiene buenas prácticas de uso de claves por parte de los usuarios. | Este problema genera en que los usuarios olviden fácilmente sus claves. | No garantizar la disponibilidad de la información. |
| ***A.11.3.2*** Equipo de usuario desatendido. | El usuario no se asegura de dar una adecuada protección al equipo. | Si el usuario no cuida su equipo, corre el riesgo de que se dañe y pierda toda su información. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.11.3.3*** Política de pantalla y escritorio limpio. | No se han adoptado políticas. | El contar con una política de este tipo puede acarrear que el usuario pueda perder la información que se encuentra en el escritorio o que se | No garantizar la, integridad y disponibilidad de la información. |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| | | coloque pantallas que quizá no sean las más adecuadas. | |
| ***A.11.4.1*** Política sobre el uso de servicios de red. | No se tiene políticas definidas de uso de red. | El riesgo que se genera al no tener políticas de uso de red es que el usuario tenga acceso a servicios no autorizados para usar. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.11.4.2*** Autenticación del usuario para conexiones externas. | No se tiene ningún método establecido de autenticación para usuarios remotos. | Si no existe un método de autenticación seguro es posible que ingresen usuarios no autorizados a los equipos y pueda causar daños a los sistemas. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.11.4.3*** Identificación del equipo en red. | Se identifica el equipo en red pero todavía no es un estándar para todos | Si no se identifican los equipos en red es posible que no se puedan autentificar las | No garantizar la confidencialidad, integridad y disponibilidad de la |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| | los equipos del Grupo Social FEPP. | conexiones desde equipos y ubicaciones específicas. | información. |
| ***A.11.4.4*** Protección del puerto de diagnóstico remoto. | No existe protección de puertos. | Se pueden producir ataques a través de estos puertos produciendo daños irreparables al sistema. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.11.4.5*** Segregación en redes. | No existe segregación de redes. | El no tener segregada la red provoca que si no se tiene un control efectivo de la red los usuarios tengan libre acceso a la información y recursos de la red. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.11.4.6*** Control de conexión de redes. | El control de conexión de redes es consecuencia de la norma 11.1 no se tiene políticas de control de acceso. | El no tener un control de conexión de redes puede causar que otros usuarios se encuentren conectándose a la | No garantizar la confidencialidad, integridad y disponibilidad de la información. |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| | | red sin autorización alguna. | |
| ***A.11.5.1*** Procedimientos de registro en el Terminal. | No existe procedimiento de registros seguros. | El no tener procedimientos que permitan registrar las conexiones no seguras puede ocasionar que se tenga conexiones que afecten a la red. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.11.5.2*** Identificación y autenticación del usuario. | No se ha establecido una técnica de autenticación adecuada para verificar la identidad de usuario. | Si el usuario no se autenticaría no podría ingresar a la red y tampoco hacer uso de los servicios disponibles en la red. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.11.5.3*** Sistema de gestión de claves. | No existe un adecuado manejo de claves. | el no contar con un procedimiento de asignación de claves puede llevar a que las claves no sean asignadas | No garantizar la confidencialidad, integridad y disponibilidad de la información. |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| | | de forma segura. | |
| ***A.11.5.4*** Uso de utilidades del sistema. | No existe control sobre el uso de programas de utilidad. | Es posible que al ingresar a las utilidades del sistema están sean modificadas ya sea de forma intencional o no, lo que ocasionaría un gran daño al equipo. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.11.5.5*** Sesión inactiva. | Los usuarios no aplican sesiones inactivas. | Al no hacer uso de la sesión inactiva puede ocasionar que otros usuarios no autorizados hagan uso del equipo y se pueda sufrir de robo de información o divulgación de la misma. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.11.5.6*** Limitación de | No se hace restricción sobre los tiempos de conexión a las | Esto provoca que se haga mal uso de las aplicaciones y | No garantizar la confidencialidad, integridad y disponibilidad de la |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| tiempo de conexión. | aplicaciones. | servicios que la red proporciona a los usuarios. | información. |
| ***A.11.6.1*** Restricción al acceso a la información. | No existen políticas de control de acceso definidas. | Si no se controla el acceso a la información, esta puede sufrir modificaciones que podrían dañar su integridad. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.11.6.2*** Aislamiento del sistema sensible. | No se cuenta con sistemas sensibles en el Grupo Social FEPP. | N/A | N/A |
| ***A.11.7.1*** Computación móvil y comunicaciones. | No se aplica en el Grupo Social FEPP. | N/A | N/A |
| ***A.11.7.2*** Tele-trabajo | No se aplica en el Grupo Social FEPP. | N/A | N/A |
| ***A.12.1.1*** Análisis y especificación de los requerimientos de | No existen enunciados que ayuden a mejorar los requerimientos de controles de seguridad en los | Si no se cuenta con una lista de requerimientos formales es posible de que después estos | No garantizar la confidencialidad, integridad y disponibilidad de la |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| seguridad. | sistemas existentes. | no sean contemplados en los respectivos presupuestos y por ende ocasionen algún retraso en las actividades en donde se les requiera. | información. |
| ***A.12.2.2*** Control de procesamiento interno. | No se realiza controles de chequeos de validación en las aplicaciones. | Esto conlleva un grave problema en la seguridad de la información ya que se puede corromper la información. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.12.2.3*** Integridad del mensaje. | No se han identificado los controles apropiados para identificar los requerimientos para proteger la integridad del mensaje en las aplicaciones. | si no se contara con mensajes que alerten al usuario las aplicaciones podrían sufrir cualquier tipo de daño que ponga en riesgo la integridad de la información. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.12.3.1*** Política sobre el | No se cuenta con políticas para el | Al no contar con controles | No garantizar la confidencialidad, |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| uso de controles criptográficos. | uso de controles criptográficos. | criptográficos puede poner en riesgo la confidencialidad de la información. | integridad y disponibilidad de la información. |
| ***A.12.3.2*** Gestión clave. | No se tiene una gestión clave para el uso de técnicas de criptografía. | Al no tener un procedimiento claro para la administración de claves puede ocasionar que constantes redundancias e inconsistencias en la aplicación de claves. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.12.4.1*** Control de software operacional. | No se cuenta con procedimientos de control en la instalación de software. | Si no se cuenta con un control de software se produciría un mal funcionamiento si no se instala correctamente. | No garantizar la integridad y disponibilidad de la información. |
| ***A.12.4.2*** Protección de la data de prueba del | No se cuenta con protección alguna. | Si los datos de prueba de sistemas no son protegidos no se podría realizar una | No garantizar la integridad y disponibilidad de la información. |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| sistema. | | adecuada restauración de ellos. | |
| ***A.12.4.3*** Control de acceso al código fuente del programa. | Las restricciones al código fuente son mínimas. | Si no se controla estos accesos puede que estos sean modificados por personas no autorizadas. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.12.5.1*** Procedimientos de control de cambio. | No se cuenta con procedimientos formales para el control de cambios. | El no tener lineamientos que definan procedimientos de control de cambios puede llevar a que estos se vuelvan una resistencia por parte de los usuarios. | No garantizar la disponibilidad de la información. |
| ***A.12.5.2*** Revisión técnica de las aplicaciones después de cambios en | No se realiza una revisión profunda de las aplicaciones después del cambio de sistema operativo. | Si no se realizan pruebas de funcionamiento cuando un sistema operativo es cambiado estos podrían no funcionar de | No garantizar la disponibilidad de la información. |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| el sistema operativo. | | forma correcta debiendo quizás a instalar nuevamente el sistema anterior si esto no se prevé. | |
| ***A.12.5.3*** Restricciones sobre los cambios en los paquetes de software. | No se realiza un control estricto sobre cambios en los paquetes de software. | Si no se restringe los cambios de paquetes de software es posible de que se realicen cambios innecesarios. | No garantizar la integridad y disponibilidad de la información. |
| ***A.12.5.4*** Filtración de información. | No existe un control efectivo que permita evitar la filtración de la información. | Si no se cuenta con controles de fuga de información esta podría ser susceptible de robos mal intencionados. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.12.6.1*** Control de vulnerabilidades técnicas. | No se obtiene información oportuna sobre las vulnerabilidades técnicas de sistemas de información. | Si no se revisa material que puede ayudar a evitar cierta vulnerabilidad estas pueden ocasionar grandes daños en | No garantizar la confidencialidad, integridad y disponibilidad de la información. |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| | | los sistemas que quizás incluso sean irreparables. | |
| ***A.13.1.1*** Reporte de eventos en la seguridad de la información. | No se reportan eventos de seguridad apropiadamente. | El no poder contar con un registro de eventos puede provocar que no se puedan tomar correctivos de una forma oportuna. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.13.1.2*** Reporte de debilidades en la seguridad. | No se reportan por parte de los usuarios debilidades en la seguridad de los sistemas o servicios. | Si no se cuenta con estos reportes es posible que se produzcan daños en cuanto a la integridad de la información. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.13.2.1*** Responsabilidades y procedimientos. | No se han establecido responsabilidades ni procedimientos ante incidentes de seguridad. | El no tener claro cuáles son las responsabilidades de cada funcionario cuando se | No garantizar la confidencialidad, integridad y disponibilidad de la información. |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| | | presenta una atentado contra la seguridad de la información, puede llevar a que este evento no sea atendido de forma inmediata. | |
| ***A.13.2.2*** Aprendizaje de los incidentes en la seguridad de la información. | No existe mecanismo alguno que permita identificar costos de incidentes en la seguridad de información. | Si no se tiene registros de riesgos sucedidos, entonces quiere decir que no se pudo aprender de ellos para evitar que no vuelvan a suceder. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.13.2.3*** Recolección de evidencia. | Se realiza seguimiento de control y recolección de evidencias tras un incidente en la seguridad de la información. | Si no se recolecta evidencias no será posible que quienes cometieron los delitos sean sancionados de forma oportuna. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| ***A.14.1.1*** Incluir seguridad de la información en el proceso de gestión de continuidad comercial. | No aplica | N/A | N/A |
| ***A.14.1.2*** Continuidad comercial y evaluación del riesgo. | No aplica | N/A | N/A |
| ***A.14.1.3*** Desarrollar e implementar planes de continuidad incluyendo seguridad de la información. | No aplica | N/A | N/A |
| ***A.14.1.4*** Marco referencial para la planeación de la | No aplica | N/A | N/A |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| continuidad comercial. | | | |
| ***A.14.1.5*** Prueba, mantenimiento y re-evaluación de planes de continuidad comerciales. | No aplica | N/A | N/A |
| ***A.15.1.1*** Identificación de legislación aplicable. | No se han definido requerimientos estatutarios reguladores y contractuales para cada sistema de información. | El no tener una legislación actualizada puede acarrar problemas contractuales. | Mal uso de los sistemas de información. |
| ***A.15.1.2*** Derechos de propiedad intelectual (IPR). | Se encuentra en etapa de trámite. | Al no contar con controles de protejan los derechos de propiedad intelectual es posible que este se encuentre en peligro de plagio. | Plagio de la información. |
| ***A.15.1.3*** Protección los | Se protege los registros | Si no se protege los registros | No garantizar la confidencialidad, |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| registros organizacionales. | organizacionales contra perdida destrucción y falsificación de la información. | importantes de la Institución puede acarrear problemas graves como son perdidas, destrucción y falsificación. | integridad y disponibilidad de la información. |
| ***A.15.1.4*** Protección de data y privacidad de información personal. | Existe privacidad de información personal. | El no tener un control que defina procedimientos para asegurar la información personal puede llevar a que esta información se pueda extraviar. | No garantizar la confidencialidad, integridad de la información. |
| ***A.15.1.5*** Prevención de mal uso de medios de procesamiento de información. | No se realiza prevención a los usuarios de utilizar medios de procesamiento para propósitos no autorizados. | Si los usuarios hacen uso de los medios de procesamiento para su beneficio es posible que al usarlos puedan ocasionar un uso inadecuado a estos medios. | Manejo inadecuado de la información. |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| ***A.15.1.6*** Regulación de controles criptográficos. | No se realiza controles. | Al no contar con controles criptográficos conlleva un grave problema de seguridad de la información. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.15.2.1*** Cumplimiento con las políticas y estándares de seguridad. | No se cumple ya que no se cuenta con políticas y estándares de seguridad. | No contar con un documento que contenga lineamientos, escritos puede ocasionar que no se proceda de forma correcta en salvaguardar la información. | No garantizar la confidencialidad, integridad y disponibilidad de la información. |
| ***A.15.2.2*** Chequeo de cumplimiento técnico. | No se realiza chequeo técnico. | No contar con un documento que contenga lineamientos, escritos puede ocasionar que no se proceda de forma correcta en salvaguardar la información. | Fuga de información. |

| ISO | GSFEPP | RIESGOS | AMENAZAS Y VULNERABILIDADES |
|---|---|---|---|
| ***A.15.3.1*** Controles de auditoría de sistemas de información. | No se planea ni ejecuta actividades de auditoría de sistemas de información. | El no contar con auditorias no se podría ver la situación real de la Institución. | Manejo inadecuado de los sistemas de información. |
| ***A.15.3.2*** Protección de las herramientas de auditoría de los sistemas de información. | No se protege porque no se cuenta con herramientas de auditoría. | Debido a que no se cuenta con ese tipo de herramientas no se registra un efecto. | Manejo inadecuado de los sistemas de información. |

# CAPÍTULO IV

# 4 PROPUESTA DE IMPLANTACIÓN

El paso previo a intentar la certificación es la implantación en la institución del sistema de gestión de seguridad de la información según ISO 27001:2005.

Este sistema deberá tener un historial de funcionamiento demostrable de al menos tres meses antes de solicitar el proceso formal de auditoría para su primera certificación.

Para esto hemos definido que en esta propuesta realizaremos la fase de Planificación, esto es:

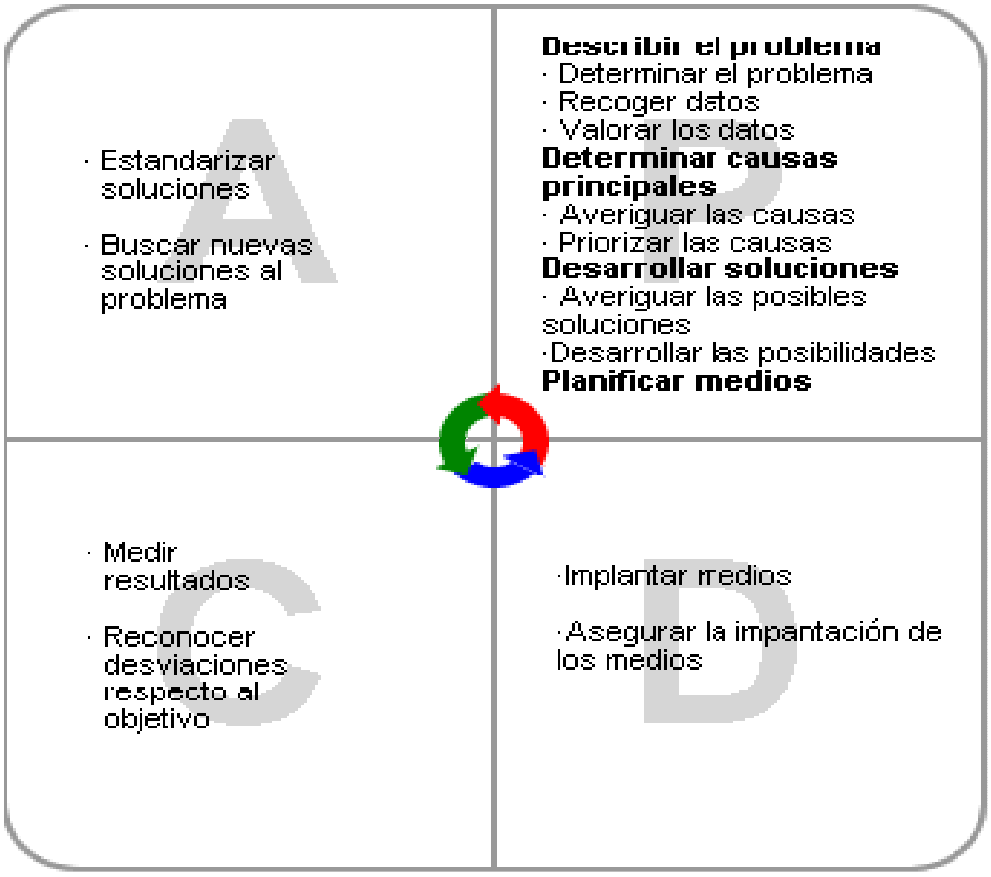


Ilustración 4.- Fase de realización (PLAN)[79]

[79]Fuente: Sistema de gestión Integral: http://www.fecyt.es/especiales/calidad/8.htm

ISO 27001 exige que el SGSI contemple los siguientes puntos:

- Implicación de la Dirección.
- Alcance del SGSI y política de seguridad.
- Inventario de todos los activos de información.
- Identificación de amenazas, vulnerabilidades e impactos.
- Análisis y evaluación de riesgos.
- Selección de controles para el tratamiento de riesgos.
- Declaración de aplicabilidad.
- Plan de tratamiento de riesgos.
- Implementación de controles, documentación de políticas, procedimientos e instrucciones de trabajo.
- Definición de un método de medida de la eficacia de los controles y puesta en marcha del mismo.
- Formación y concienciación en lo relativo a seguridad de la información a todo el personal.
- Monitorización constante y registro de todas las incidencias.
- Realización de auditorías internas.
- Evaluación de riesgos periódica, revisión del nivel de riesgo residual, del propio SGSI y de su alcance.
- Mejora continua del SGSI.

La documentación del SGSI deberá incluir:

- Política y objetivos de seguridad.
- Alcance del SGSI.
- Procedimientos y controles que apoyan el SGSI.
- Informe resultante de la evaluación del riesgo.
- Plan de tratamiento de riesgos.
- Procedimientos de planificación, manejo y control de los procesos de seguridad de la información y de medición de la eficacia de los controles.
- Registros.
- Declaración de aplicabilidad (SOA -Statement of Applicability-).
- Procedimiento de gestión de toda la documentación del SGSI.

Para cumplir con estos ítems se propondrá que:

- El alcance del SGSI abarque a todo el Grupo Social FEPP, esto es a todas sus empresas y regionales que sirven de apoyo para tal objetivo.
- Esto se lo podrá realizar gracias a que sus procesos en cuanto al manejo de la información son similares y por tanto se podrá establecer de forma clara y precisa un Sistema de Gestión de Seguridad de la Información.
- El informe de la evaluación de riesgos se la trato en el capítulo III del presente documento.
- La política de seguridad, los procedimientos, controles y el plan de tratamiento de riesgos a seguir se la detalla en la siguiente propuesta.

# 4.1 PROPUESTA

## 4.1.1 IDENTIFICACIÓN DE ACCIONES

*La norma ISO 27001:2005 menciona: "8.2.- Acción correctiva.- La organización debe tomar acciones para eliminar la causa de las no conformidades respecto de los requisitos del SGSI de cara a evitar que éstas vuelvan a ocurrir. El procedimiento documentado para acción correctiva debe definir los requisitos para: - identificar no conformidades, - determinar la causa de las no conformidades, - evaluar la necesidad de acciones para asegurar que éstas no vuelven a ocurrir, - determinar e implementar la acción correctiva requerida, - registrar los resultados de la acción acometida, - revisar la acción correctiva acometida.*

*8.3.- Acción preventiva.- La organización debe determinar acciones para eliminar la causa de no conformidades potenciales respecto de los requisitos del SGSI de cara a prevenir que estas ocurran. Las acciones preventivas tomadas deben de ser apropiadas al impacto de los potenciales problemas. El procedimiento documentado para acciones preventivas debe definir requisitos para: - identificar no conformidades potenciales y sus causas, - evaluar la necesidad de acciones para prevenir la ocurrencia de no conformidades, - determinar e implementar las acciones preventivas requeridas, - registrar los resultados de las acciones acometidas, - revisar la acción preventiva acometida. La organización debe determinar los riesgos que han cambiado e identificar los requisitos de las acciones preventivas centrando la atención en cambios significativos en los riesgos. La prioridad de las acciones preventivas debe determinarse en base a los resultados del Risk Assessment. Nota: Las acciones*

*para prevenir no conformidades son usualmente más eficaces en cuanto a coste que las acciones correctivas."*[80]

Se debe definir una Política de Seguridad acorde con la misión, visión y objetivos del Grupo Social FEPP, para esto se propone lo siguiente:

#### 4.1.1.1 Objetivo

El objetivo de la política de seguridad consistirá en fijar objetivos para el Grupo Social FEPP en lo que respecta a la protección de sus activos de información para reducir al mínimo el riesgo de daño de la información previniendo incidentes de seguridad.

La política de seguridad proporcionará la base para la aplicación de controles de seguridad que reduzcan los riesgos y las vulnerabilidades. Al aclarar las responsabilidades de los usuarios y las medidas que deben adoptar para proteger la información y sistemas, el Grupo Social FEPP evitará pérdidas graves o divulgación no autorizada. Por otra parte, el buen nombre del Grupo Social FEPP se deberá en parte a la forma en que protegerá su información y sus sistemas de información. Por último, una política de seguridad podrá ser útil como prueba de que en el Grupo Social FEPP existe transparencia en sus procesos de administración de financiamiento externo e interno.

[80] Fuente Norma ISO 27001:2005 Cap. 8

#### 4.1.1.2 Marco de Gestión de Seguridad

Todas las políticas y procedimientos que figurarán en esta propuesta deberán ser aprobados, apoyados y defendidos por la dirección del Grupo Social FEPP. La información deberá ser protegida de acuerdo a la criticidad y sensibilidad de la misma.

Las medidas de seguridad deberán ser tomadas, independientemente de los medios de almacenamiento donde se guarde la información, los sistemas utilizados para procesar la información o los métodos utilizados para la transferencia de información. La información debe ser protegida de acuerdo a su clasificación de seguridad, sin tener en cuenta la fase del ciclo de vida de la información en la que se encuentra.

#### 4.1.1.3 Política

El objetivo de la política será proteger la información del Grupo Social FEPP contra todas las amenazas internas, externas deliberadas o accidentales.

El Gerente de Seguridad deberá aprobar la política de seguridad de la información.

La política de seguridad garantizará que:

- ✓ La información será protegida contra cualquier acceso no autorizado.
- ✓ La confidencialidad de la información será asegurada.

- ✓ La integridad de la información deberá ser mantenida.
- ✓ La disponibilidad de la información para procesos de la organización será mantenida.
- ✓ Se reunirán todos los requerimientos legislativos y regulatorios que involucren la seguridad de la información.
- ✓ La educación en seguridad de la información estará disponible para todos los usuarios.
- ✓ Todas las actuales o presuntas brechas de seguridad de la información serán informadas al Gerente de Seguridad de Información las cuales serán investigadas a fondo.

Deberán establecer procedimientos para apoyar la política, que incluyan medidas de control de virus, contraseñas y proyectos de continuidad.

Las necesidades del Grupo Social FEPP en la disponibilidad de la información y sistemas serán satisfechas.

El Gerente de Seguridad de la Información será responsable de mantener la política y proporcionar el apoyo y asesoramiento durante su puesta en práctica.

Todos los Coordinadores de las distintas empresas y regionales que conforman el Grupo Social FEPP serán directamente responsables de poner en práctica la política y asegurar el cumplimiento de personal en sus empresas y regionales respectivas.

El cumplimiento con la Política de Seguridad de la Información será obligatorio.

La política será revisada cada año por el encargado de Seguridad de Información.

#### 4.1.1.4 Ámbito de Aplicación

*De los empleados*

La seguridad de la información es un esfuerzo de equipo, se requiere la participación y el apoyo de todos los miembros de la institución que trabajan con sistemas de información y manipulen información. Así, cada empleado deberá cumplir con los requisitos de la política de seguridad de la información y la documentación que le asisten. Los empleados que deliberadamente o por negligencia[81] infrinjan las políticas de seguridad de la información serán objeto de medidas disciplinarias o el despido.

Todos los empleados, usuarios y demás estarán obligados a concientizarse y familiarizarse con todas las políticas de seguridad de la información, procedimientos, normas y legislación aplicable. Deberán comprender perfectamente estos requisitos y cumplir con ellas.

### 4.1.2 ROLES Y RESPONSABILIDADES

*Según la norma ISO 27001:2005 dice: "7.1 Lograr mantener la protección adecuada de los activos de la organización.*

*Todos los activos se deben incluir y deben tener un dueño designado.*

[81] Refiérase al glosario de términos.

*Se deberían identificar los dueños para todos los activos y asignar la responsabilidad para el mantenimiento de los controles adecuados. La implementación de los controles específicos puede ser delegada por el dueño según el caso, pero él sigue siendo responsable de la protección adecuada de los activos."*[82]

A fin de coordinar los esfuerzos de seguridad, el Grupo Social FEPP dividirá las responsabilidades de sus miembros en tres categorías.

#### 4.1.2.1 Propietario

Por lo general los jefes o coordinadores de departamentos, son responsables de la gestión y protección de información. Ellos pueden tomar todas las decisiones necesarias que conciernen a la información que controlan a fin de mantener su integridad y su confidencialidad.

El propietario es normalmente un empleado permanente de la institución.

##### *4.1.2.1.1 Responsabilidades*

- Entiende los principales riesgos involucrados con todos los usos internos de un tipo específico de información.
- Determina la sensibilidad, nivel de criticidad de la información y su clasificación.
- Especifica los métodos de control adicionales requeridos para proteger esta información.

[82] Fuente Norma ISO 27001:2005, Anexo A.

- Aprueba peticiones de los usuarios que quieran acceder a la información.
- Revisa la lista de control de acceso de usuarios para determinar si los privilegios deberían ser retirados o no.

#### 4.1.2.2 Administrador

Los administradores son por lo general miembros del Departamento de Seguridad de Información y pueden tener otros cargos como administradores de sistema u operadores de control de datos. Mantienen la información, administran los sistemas de procesamiento de la información y supervisan el acceso a la información.

Los administradores son empleados permanentes.

##### *4.1.2.2.1 Responsabilidades*

- Custodia la información de la institución o de la información que fue encargada a la misma.
- Sigue las instrucciones del propietario para procesar y manejar la información.
- Con regularidad provee al propietario con listas de personas que regularmente han accedido a la información.
- Sugiere nuevas tecnologías y procedimientos al propietario.
- Mantiene la fiabilidad de acceso a los equipos que contienen la información.

- Implementa las directivas especificadas por el propietario.
- Instala mecanismos de seguridad con el fin de evitar accesos no autorizados que eviten la divulgación no autorizada de la información.
- Regularmente realiza copias de seguridad y restaura los datos de copias de seguridad cuando sean requeridos.

#### 4.1.2.3 Usuarios

El usuario puede ser funcionario de la institución o un tercero que tiene acceso o utiliza esta información exclusivamente para fines profesionales.

Terceros y subcontratistas deberán firmar un acuerdo confidencialidad a fin poder acceder a la información.

##### *4.1.2.3.1 Responsabilidades*

- Piden al propietario acceso a la información y al sistema.
- No usa los sistemas de información sin autorización.
- Utiliza un equipo de acceso seguro proporcionado por el administrador.
- Se adhiere a los controles establecidos por el propietario y por la dirección.

- Informa de errores, anomalías al propietario del sistema.
- Informa de las vulnerabilidades y violaciones al Departamento de Seguridad de la Información.

### 4.1.3 NIVELES DE CLASIFICACIÓN DE LA INFORMACIÓN

*La norma ISO 27001:2005 menciona en el numeral 7 del Anexo A:*
*"7.2 Asegurar que la información recibe el nivel de protección adecuado.*

*La información se debería clasificar para indicar la necesidad, las prioridades y el grado esperado de protección al manejar la información.*

*La información tiene diferentes grados de sensibilidad e importancia. Algunos elementos pueden requerir un grado adicional de protección o manejo especial. Se recomienda utilizar un esquema de clasificación de la información para definir un conjunto apropiado de niveles de protección y comunicar la necesidad de medidas especiales de manejo."*[83]

La clasificación de la información constituye un elemento importante de la gestión de riesgos, ya que determina las necesidades, la prioridad y el grado de protección necesario para cada tipo de información.

El Grupo Social FEPP deberá adoptar una estructura de clasificación de la información, que definirá el nivel adecuado de protección e

[83] Fuente: Norma ISO 27001:2005, Anexo A.

informará a los responsables de cualquier medida especial o tratamiento requerido.

Toda la información deberá ser integrada en una de las siguientes categorías:

- Confidencial
- Privado
- De uso interno
- Público

Para garantizar la protección de la información, todos los usuarios deben familiarizarse con la definición de cada categoría, así como de las medidas necesarias.

### 4.1.4 ETIQUETADO DE LA INFORMACIÓN

*La norma ISO 27001:2005 menciona en el numeral 7 del Anexo A:*
*"7.2 Asegurar que la información recibe el nivel de protección adecuado.*

*La información se debería clasificar para indicar la necesidad, las prioridades y el grado esperado de protección al manejar la información.*

*La información tiene diferentes grados de sensibilidad e importancia. Algunos elementos pueden requerir un grado adicional de protección o manejo especial. Se recomienda utilizar un esquema de clasificación de la información para definir un conjunto apropiado de niveles de protección y comunicar la necesidad de medidas especiales de manejo."*[84]

[84] Fuente: Norma ISO 27001:2005, Anexo A.

El Grupo Social FEPP deberá desarrollar procedimientos adecuados para el etiquetado y el manejo de la información de acuerdo a estructura de la clasificación que haya adoptado. En las etiquetas de identificación deberá figurar la clasificación, instrucciones de uso, manipulación y la ubicación si es necesario. Las etiquetas deberán aparecer en los pies de página de los documentos del Grupo Social FEPP.

### 4.1.5 ORGANIZACIÓN DE SEGURIDAD

*Según la norma ISO 27001:2005:*
*"A.6* Organización de la información de seguridad.

**Organización Interna:*
*Autorizaciones, acuerdos de confidencialidad, contactos con autoridades y grupos de interés en temas de seguridad, revisiones independientes.*

**Partes externas: Riesgos relacionados con terceros, gobierno de la seguridad respecto a clientes y socios de negocio.*

*En este grupo de controles, lo ideal es diseñar e implementar una simple base de datos, que permita de forma amigable, el alta, baja y/o modificación de cualquiera de estos campos. La redacción de la documentación inicial de responsables: derechos y obligaciones (para personal interno y ajeno) y el conjunto de medidas a adoptar con cada uno de ellos. Una vez lanzado este punto de partida, se debe documentar la metodología de actualización, auditabildad y periodicidad de informes de la misma."*[85]

[85] Fuente: Norma ISO 27001:2005, Anexo A

#### 4.1.5.1 Divulgación

Información de la etiqueta que no sea “pública” deberá ser protegida de la divulgación a terceros.

Acceso de terceros a la información de la organización podrá ser autorizada si se ha demostrado que esta información es necesaria para que el tercero pueda cumplir con una cierta tarea encomendada por una cierta autoridad de la institución. Sin embargo, un acuerdo de no divulgación con el Grupo Social FEPP primero debe ser firmado (acuerdo de confidencialidad) y la divulgación debe ser autorizada expresamente por el propietario de la información.

Cualquier pérdida, acceso no autorizado o la presunta revelación de información sensible deberá ser reportado inmediatamente al propietario de la información y al departamento de Seguridad de la Información.

#### 4.1.5.2 Copia no autorizada de la información

Se prohibirá a los usuarios copiar, sin justificación valida y sin la autorización correspondiente la información de la institución o de software.

Los responsables de la transmisión no autorizada de información copiada a terceros estarán sujetos a acción disciplinaria.

Sin embargo se autorizará realizar copias de seguridad de la información.

#### 4.1.5.3 Derechos de vigilancia

La administración se reserva el derecho de supervisar e inspeccionar los sistemas de información de la institución en cualquier momento.

Estas inspecciones pueden llevarse a cabo con o sin el consentimiento y la presencia de los empleados involucrados.

Los sistemas de información que pueda ser sometido a dicha inspección incluyen la actividad de los registros de usuarios, archivos de disco duro y de correo electrónico. Sin embargo, los documentos impresos, cajones y aéreas de almacenamiento también puede estar sujetos a inspección.

Las inspecciones solo se deberán realizar después de haber obtenido la aprobación del departamento legal y de seguridad. La Administración se reservara el derecho de confiscar cualquier material ofensivo.

#### 4.1.5.4 Acceso a internet

Todos los empleados del Grupo Social FEPP tienen acceso a internet en sus puestos de trabajo. Este acceso puede ser retirado en cualquier momento. Este acceso a internet estará controlado para asegurar su uso adecuado y el cumplimiento de las políticas de seguridad.

Cualquier información extraña a las actividades que fuere recibida a través de internet debe ser observada con recelo hasta que se pueda confirmar si la fuente es confiable.

Se prohíbe publicar material, información del Grupo Social FEPP a menos que esté autorizado por el propietario de los activos y el Departamento de la Seguridad de la información.

La Información confidencial como contraseñas y números de tarjetas de crédito no deben ser entregados a través de Internet, a menos que se envíen encriptados.

#### 4.1.5.5 Correo Electrónico

El Grupo Social FEPP ofrece a todos sus empleados una dirección de correo electrónico y sus servicios con el fin de facilitar la comunicación y desempeño de sus funciones. Todas las comunicaciones e información deben ser enviadas y recibidas a través de esta dirección de correo electrónico.

Las cuentas de personales de correo electrónico (Yahoo, Hotmail, etc.) no pueden ser usadas para enviar información sensible relativa a la institución.

Todo el personal debe utilizar una firma estándar que incluye nombre y apellidos, cargo, dirección y número de teléfono. Los mensajes importantes no deben ser almacenados en la bandeja de entrada de correo electrónico sino en una carpeta especial creada por cada usuario para evitar la eliminación involuntaria de correos electrónicos.

#### 4.1.5.6 Respaldo de datos y restauración

La información individual debe ser objeto de copia de seguridad y se lo deberá realizar en algún medio de almacenamiento magnético o masivo externo.

Cuando sea solicitado el departamento de informática deberá proporcionar asistencia técnica para la instalación de hardware o software y copias de seguridad.

Todas las copias de seguridad de la información crítica o sensible deben ser almacenadas en un área aprobada con acceso controlado.

Estas copias deberán ser guardadas únicamente con el fin de restaurar el sistema debido a una infección de virus de computadora, defectos o problemas de disco duro.

Un plan de emergencia debe ser desarrollado para todas las aplicaciones que manejan la información operativa crítica. El propietario de la información debe garantizar que el plan se ha desarrollado adecuadamente, y deberá ser actualizado y revisado periódicamente.

#### 4.1.5.7 Control de acceso a la información y servicios

Acceso a oficinas, servidores y área de trabajo que contengan información sensible deberá ser restringido y solo se considera a los empleados que tengan necesidad de una base de conocimiento.

La información confidencial siempre deberá estar protegida contra la divulgación no autorizada.

Documentos impresos que contengan información sensible deberán ser almacenados en un gabinete de archivo con llave.

La información sensible deberá estar almacenada en una instalación cerrada durante las horas de trabajo.

Se recomienda una política de escritorio limpio con el fin de restringir aún más el acceso a los documentos.

Las pantallas de la computadora deberán colocarse de tal manera que se reduzca el punto de vista de su contenido.

Se prohíbe el uso de Pendrives para transferir la información de un sitio a otro cuando la información sea etiquetada de confidencial.

#### 4.1.5.8 Protección contra robo

Los sistemas y equipos de red deberán ser protegidos físicamente contra el robo cuando se encuentran en una oficina abierta.

La Red de área local (LAN), servidores y otros sistemas multi-usuarios deben ser colocados en habitaciones cerradas.

Los ordenadores portátiles deben estar protegidos por cable antirrobo colocados en gabinetes con cerrojos o asegurados por otros mecanismos de protección cuando se encuentren en un entorno sin supervisión.

### 4.1.6 CONTROLES DE SEGURIDAD

*La norma ISO 27001:2005 menciona: "Mejora continua.- La organización debe mejorar de forma continua la eficacia del SGSI a través del uso de la Política de Seguridad de la Información, Objetivos de Seguridad de la Información, resultados de auditorías, análisis de eventos monitorizados, acciones correctivas y preventivas y la revisión por la dirección."*[86]

#### 4.1.6.1 Identificación y autenticación de usuarios

El Grupo Social FEPP requerirá que todos sus empleados que tienen acceso a sus sistemas tengan una sola identificación de usuario y una contraseña privada.

La identificación de usuario deberá ser usada para restringir los privilegios de acceso de acuerdo a las funciones, responsabilidades y actividades de cada usuario.

Todos los empleados son responsables de proteger sus identificadores de usuario y contraseña.

#### 4.1.6.2 Uso y Manejo de Contraseñas

Los usuarios del sistema deberán elegir contraseñas que sean difíciles de adivinar y que no contengan información relacionada con el trabajo o vida personal. Por ejemplo, números de identificación personal (PIN[87], licencia de conducir, numero de seguridad social, los números de

[86] Fuente norma ISO 27001:2005 Cap. 8
[87] Personal Identify Number (Número de identificación personal).

teléfono, nombres de los cónyuges, direcciones postales, nombres propios, lugares conocidos o términos técnicos no deben ser utilizados).

Los usuarios no deberán crear contraseñas que sean iguales o parecidas a las anteriores.

Las contraseñas deberán contar con al menos 8 dígitos, y se modificaran a intervalos de no más de 90 días.

El sistema de gestión de contraseñas obligara a los usuarios a que combinen letras y números, y no permitirá el uso repetido de una contraseña en un periodo de tiempo determinado.

Las contraseñas por ningún motivo deberán ser escritas y dejadas a simple vista, como por ejemplo pegadas en los monitores.

Cuando la información que no sea etiquetada de confidencial y deba ser compartida, los empleados deberán hacerlo mediante correo electrónico, o directorios públicos situados en los servidores de red de área local.

Las contraseñas nunca deben ser compartidas o divulgadas.

Los administradores de sistemas y el personal técnico nunca deberán preguntar a los empleados sus claves personales. La única excepción será en el caso de cambio de una contraseña temporal cuando el usuario accede al sistema por primera vez.

Si los usuarios sospechan que alguien está usando su ID de usuario y contraseñas, será su responsabilidad notificar inmediatamente a los administradores del sistema y departamento encargado de seguridades.

#### 4.1.6.3 Manejo de Software malicioso

Los usuarios del sistema no deberán cancelar el proceso de actualización automáticas del antivirus.

Todos los archivos del computador deberán ser analizados y escaneados por el software de detección de virus.

Un análisis deberá ejecutarse antes de la apertura de nuevos archivos de datos y antes de ejecutar nuevos programas informáticos.

#### 4.1.6.4 Eliminación de virus

A la primera señal de un posible virus informático, los empleados deberán cesar de inmediato su trabajo y llamar a soporte técnico.
Todos los medios de almacenamiento magnéticos utilizados en el ordenador infectado no deberán ser utilizados en otro equipo hasta que el virus sea eliminado.

La computadora infectada debe ser puesta en cuarentena (aislada de la red interna). Los usuarios no deben intentar eliminar los virus por sí mismos.

Los miembros del personal calificado deberán garantizar el mínimo daño para evitar destrucción de datos o pérdidas de información.

Si en la computadora existiera información etiquetada de confidencial se deberá realizar un trabajo cuidadoso,

siguiendo con los procedimientos establecidos por seguridades físicas para este tipo de casos.

#### 4.1.6.5 Seguridades en la Red

Todas las computadoras que almacenan información sensible y están permanentemente o intermitentemente conectadas a las redes informáticas internas de la institución deberán tener un sistema de control de acceso aprobado por el departamento encargado de la Seguridad de la información.

Todos los otros tipos de sistemas de procesamiento de la información deberán estar equipados con una contraseña de protector de pantalla que se cierra después de un periodo de terminado de inactividad. La pantalla se vuelve a activar cuando la contraseña correcta sea digitada.

Para los sistemas multi usuario se deberá utilizar un mecanismo de cierre de sesión en el cual cierre automáticamente la sesión de usuario después de un periodo determinado de inactividad.

Los empleados no deben establecer conexiones con redes externas (proveedores de servicios de internet) utilizando los sistemas y/o equipos de la institución sin la aprobación previa del Departamento de Seguridad de la Información.

Excepto en casos de emergencia, todos los cambios de las redes informáticas del Grupo Social FEPP se deberán registrar en una solicitud de mantenimiento y deberá ser aprobado por el departamento de Informática.

Todos los cambios a las redes internas deberán llevarse a cabo por el personal autorizado por el Departamento de Informática.

Este proceso reducirá el riesgo de divulgación no autorizada y de los cambios realizados, sin el conocimiento del Departamento de Informática.

Este proceso se aplica no solo a los empleados del Grupo Social FEPP, sino también a los proveedores de servicios.

### 4.1.7 CUMPLIMIENTO

*La norma ISO 27001:2005 menciona: "Cumplimiento : incluye cumplimiento de varias leyes (reguladoras) civiles, criminales y administrativas tales como leyes de propiedad intelectual, secretos comerciales, derechos de propiedad intelectual, marcas, patentes y protección de información."*[88]

El Grupo Social FEPP realizara periódicamente auditorias de seguridad para garantizar el cumplimiento con las políticas aplicables, los procedimientos y las leyes.

### 4.1.8 CUMPLIMIENTO DE LAS POLÍTICAS Y PROCEDIMIENTOS

*Según la norma ISO 27001:2005 menciona en cuanto a este particular : "Cumplimiento Legal: incluye cumplimiento de varias leyes (reguladoras) civiles, criminales y administrativas tales como leyes de propiedad intelectual, secretos comerciales, derechos de*

[88] Fuente : Norma ISO 27001:2005, Anexo A

*propiedad intelectual, marcas, patentes y protección de información."*[89]

Todos los empleados deben cumplir con las políticas de seguridad de la información y documentos relacionados. Los empleados que, por negligencia, violen las políticas de seguridad serán objeto de medidas disciplinarias o el despido.

### 4.1.9 CUMPLIMIENTO DE LA LEGISLACIÓN Y NORMATIVA

*Según la norma ISO 27001:2005 menciona en cuanto a este particular : "Cumplimiento Legal: incluye cumplimiento de varias leyes (reguladoras) civiles, criminales y administrativas tales como leyes de propiedad intelectual, secretos comerciales, derechos de propiedad intelectual, marcas, patentes y protección de información."*[90]

Todas las políticas de seguridad de la información deberán cumplir con la legislación aplicable, como las leyes sobre protección de datos, acceso a la información, la protección de la información personal y documentos electrónicos.

### 4.1.10 RÉGIMEN DISCIPLINARIO

*La norma ISO 27001:2005 en cuanto al régimen disciplinario: "Se deberá crear una política de sanciones para el personal q no cumpla con las distintas responsabilidades q se le asignaron con el objetivo*

[89] Fuente : Norma ISO 27001:2005, Anexo A
[90] Fuente : Norma ISO 27001:2005, Anexo A

*de regularizar el proceso de producción y generar el producto a tiempo y con alta calidad."*[91]

Sospecha de violación de la política de seguridad que pueden comprometer la integridad, confidencialidad y disponibilidad de la información deberá ser reportada inmediatamente al departamento de Seguridad de la Información.

Violación comprobada o de incumplimiento con las políticas de seguridad de la información supone graves consecuencias para los infractores. Las medidas disciplinarias varían de acuerdo a la gravedad de la violación, y pueden conducir al despido.

Esta propuesta tiene como fin ordenar el caos dentro de la institución ya que contaría con políticas, controles y tratamientos a los riesgos establecidos para una adecuada gestión en el manejo de la seguridad de la información, contando con gente capacitada, involucrada y comprometida en la gestión de la seguridad de la información, cumpliendo con el objetivo de llegar a un nivel 2 de madurez.

## 4.2 DECLARACIÓN DE APLICABILIDAD

Basados en los resultados de los procesos de evaluación realizados en el capítulo anterior, se propone que en el documento de declaración de aplicabilidad conste los objetivos de control ya descritos anteriormente.

[91] Fuente: : Norma ISO 27001:2005

# 5 CONCLUSIONES

- Implantar un Sistema de Gestión de Seguridad de la información (SGSI), es de mucha ayuda para entidades que basan su sostenibilidad en la claridad y respaldo de la información que esta genera en el aspecto de manejo financiero y de proyectos, ya que así seguirán recibiendo financiamiento de entidades extranjeras, pero las dificultades aparecen durante la explicación del proceso de análisis de riesgos y vulnerabilidades y se intensifican con la necesidad de colaboración de una parte importante de las personas de la empresa con la dirección al frente, esto se debe a la cultura poco participativa de nuestra sociedad.

- El Grupo Social FEPP es una entidad q se sostiene por financiamiento de entidades extranjeras en su mayoría y estas solicitan q la información que reciben sea validada por alguna norma internacional; es por eso que en el Grupo Social FEPP es urgente empezar con el proceso para aplicar a una futura certificación ISO 27001:2005.

- En el Grupo Social Fondo ecuatoriano Populorum Progressio no existe una política de estandarización y normalización de los procesos que en esta institución se generan ya sean procesos de índole técnica o financiero contable.

- Al no mantener una política de estandarización y normalización no se puede monitorear la fuga de información que se produce por todos los medios posibles como se detalló en el capítulo III.

- El traslado de la información financiera y de proyectos se lo realiza si el más mínimo control ni seguridad y se lo hace x medios q no garantizan la autenticidad de la información final.

- Tratar el tema de “seguridad” y “gasto” es hablar de lo mismo motivo por el cual muchas de las instituciones no gubernamentales (ONG) no consideran necesario la inversión en un SGSI, pero la aceptación de un SGSI debe vencer al temor de la dirección a incluir este monto en su presupuesto anual ya que cuando se lo logre concluir los beneficios serán mucho mayores versus los gastos.

- Para disipar estos miedos, se destacan ventajas como, precisamente, la efectividad y control de los gastos que la empresa realizará en seguridad, la mejora y adaptación continua del grado de seguridad a los cambios del entorno y la buena reputación de la empresa ligada al cumplimiento puntual de sus obligaciones legales.

- La estructura del Grupo Social FEPP tiene la particularidad de no dividirse por departamentos ,como es común en otras organizaciones no gubernamentales, sino por empresas cada una en su campo de acción, pero ante las entidades reguladoras el Grupo Social FEPP es una sola institución y por este motivo su información tributaria se la debe consolidar, siendo esta la razón por la cual el traslado de información sensible de una empresa a otra es indispensable y se debería adoptar políticas que garanticen su segura manipulación y tratamiento.

- La empresa que presta servicios con respecto a la parte informática se denomina INFOFEPP, dicha empresa no cuenta al momento con personal capacitado para asumir la responsabilidad de la Generación de políticas de Seguridad que lleven a ensamblar un Sistema de Gestión de Seguridad Informática (SGSI).

- INFOFEPP actualmente no tiene una adecuada distribución de trabajo y este es una razón por la seria prácticamente imposible poder asumir el papel de Gestionador de políticas de seguridad.

- Actualmente no existe un real inventario de los equipos de cómputo propiedad del Grupo Social FEPP por lo cual no se puede realizar una asignación de permisos para el acceso a la Red y al Internet.

- Todas las computadoras propiedad del Grupo Social FEPP tienen privilegios de administrador por lo que no se puede restringir el acceso a la información.

- El lugar donde se mantienen los servidores no cuenta con las características físicas ni tecnológicas adecuadas para poder brindar una pronta solución a los problemas que podrían surgir como por ejemplo recuperar información de un respaldo.

- Si el Grupo Social Fondo ecuatoriano Populorum Progressio considera seriamente la privacidad dentro de sus valores principales potenciarán su trabajo y campo de ayuda a los ecuatorianos, explotarán al máximo su imagen y certificación en ISO 27001, adaptará y mejorará continuamente su nivel de protección sin tener que reducir el nivel de satisfacción de clientes o empleados, garantizarán la continuidad del negocio en cualquier situación y disfrutará de las ventajas y herramientas esenciales para identificar y explotar puntualmente las oportunidades que los mercados ofrezcan en cada momento.

# 6 RECOMENDACIONES

- Existe muchas empresas que han intentado realizar un Sistema de Gestión de Seguridad de la Información (SGSI), pero no lo han logrado debido a que estas empresas avizoraron a la norma ISO 27001 como un simple “sello” útil en temas de imagen; se recomienda por lo tanto al Grupo Social Fondo Ecuatoriano Populorum Progressio evite tener esta concepción ya que el aplicar a la norma de seguridad ISO 27001 implica un cambio en el manejo funcional de la institución esto incluye al ambiente físico, tecnológico y recurso humano, por lo tanto las mejoras que se den para alcanzar una certificación se las debe mantener para que este proceso sea exitoso.

- La oficina central que es el departamento directamente encargado de la gestión de la información financiera y de manjar los proyectos desde el aspecto financiero, debería dar el primer paso exigiendo a las demás empresas que la información que le envía se lo haga usando medios que seas validados por el plan del Sistema de Gestión de Seguridad de la Información que se realizara en la institución.

- Los Sistemas de Gestión de Seguridad de la Información (SGSI) y la privacidad habilitan a las empresas a establecer relaciones de confianza que intensifican positivamente las actividades comerciales con sus clientes y empresas colaboradoras que en el caso puntual del Grupo Social FEPP son las instituciones financistas; también facilitan su propagación a clientes potenciales, y además a nivel interno, se favorece la relación que la propia institución establece con sus empleados, la coordinación, el directorio y otras partes interesadas y se mejora la eficacia entre los distintos ámbitos organizativos y físicos establecido; por lo tanto se recomienda comenzar cuanto antes con la formulación de las políticas institucionales para aplicar a un SGSI y mediante este a una certificación ISO 27001.

- Un conocimiento más preciso de los niveles de satisfacción alcanzados en las actividades y procesos de negocio ayuda, además, a introducir cambios con una mayor garantía en los resultados que se desean obtener y reduce el nivel de incertidumbre y de posibles pérdidas económicas posibles en decisiones comprometidas.

- Se debe crear un departamento especializado que se encargue de la generación de un plan para la creación del Sistema de Gestión de la Seguridad de la Información.

- Se debe capacitar al personal de INFOFEPP que será el que a futuro se encargue de verificar que las políticas para la seguridad de la información se cumplan y no causen problemas innecesarios.

- Es importante que INFOFEPP realice un inventario de los equipos existentes en la institución para poder definir el tipo de acceso q tendrán los mismos a la Red y al Internet.

- Es de suma importancia empezar a inculcar en los empleados de la institución una cultura de buen manejo de la información con la ayuda de normas o políticas institucionales.

- Se debería involucrar a todas las empresas y regionales del Grupo Social FEPP con la creación de las políticas institucionales para la seguridad de la información y se lo debería hacer con propuestas y sugerencias sobre las necesidades de cada empresa y regional.

- Se recomienda que el Directorio del Grupo Social FEPP asuma la responsabilidad de agilitar el siguiente proceso del PDCA que es el poner en práctica las recomendaciones q de este estudia han salido, para tener como meta una futura pero no lejana certificación ISO 27001:2005.

# 7 GLOSARIO

1. **Aceptación del Riesgo.-** Según [ISO/IEC Guía 73:2002]: Decisión de aceptar un riesgo.

2. **Acceso.-** De acuerdo a la Real Academia de la Lengua, acceso es permitir el ingreso a un determinado sitio.

3. **Amenaza.-** De acuerdo a la Real Academia de la Lengua, amenaza es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

4. **Activos:** De acuerdo a la Real Academia de la Lengua, es el conjunto de todos los bienes y derechos con valor monetario que son propiedad de una empresa, institución o individuo, y que se reflejan en su contabilidad.

5. **Austeridad:** Sobriedad, ausencia de adornos.

6. **Autenticación.-** Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

7. **Bases de datos:** Se define una base de datos como una serie de datos organizados y relacionados entre sí, los cuales son recolectados y explotados por los sistemas de información de una empresa o negocio en particular.
   El término de bases de datos fue escuchado por primera vez en 1963, en un simposio celebrado en California, USA. Una base de datos se puede definir como un conjunto de información relacionada que se encuentra agrupada o estructurada.

   Desde el punto de vista informático, la base de datos es un sistema formado por un conjunto de datos almacenados en discos que permiten el acceso

directo a ellos y un conjunto de programas que manipulen ese conjunto de datos.

Cada base de datos se compone de una o más tablas que guarda un conjunto de datos. Cada tabla tiene una o más columnas **y** filas. Las columnas guardan una parte de la información sobre cada elemento que queramos guardar en la tabla, cada fila de la tabla conforma un registro.

8. **Conferencia episcopal ecuatoriana.-** Institución de carácter permanente que reúne a todos los obispos del Ecuador para ejercer, en espíritu de unidad y de comunión, algunas de las funciones pastorales que les son propias, respetando, en todo caso, la autoridad y la competencia que cada obispo tiene en su Iglesia particular.

9. **Confiabilidad:** Confiabilidad es la "capacidad de un ítem de desempeñar una función requerida, en condiciones establecidas".

10. **Confidencialidad: E**s la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información

11. **Criptografía:** De acuerdo a la Real Academia de la Lengua, Arte de escribir con clave secreta o de un modo enigmático.

12. **Disponibilidad:** Situación de la persona o cosa que está preparada para un fin.

13. **Doctrina Social de la Iglesia.-** Por doctrina social se entiende un conjunto coherente de ideas, enseñanzas y normas referentes a valores humanos que se desea realizar y perfeccionar en cooperación social. La nueva y actual doctrina empezó a ser desarrollada por León XIII. Sabido es que la Iglesia no sostiene un único sistema económico o político para organizar la sociedad y tampoco identifica la religión con una postura política específica.

La diversidad es aceptada por la realidad de la existencia de varios caminos para realizar el bien común y administrar una comunidad.

Se desarrolla a partir de:

*El mensaje religioso y social del Nuevo Testamento, y en la misma acción religiosa que implica descubrir al prójimo y tratarlo como hermano*;
En las encíclicas de los pontífices, especialmente en las emitidas desde León XIII (1891) en adelante, y que han sido completadas con cientos de otros discursos y mensajes de distintos Papas; y

La tarea de análisis y otros aportes fruto de distintos estudios sobre los principios y temas de esta doctrina social.

Se basa en varios principios generales aptos para regular la sociedad: la solidaridad, el bien común, la subsidiariedad, el derecho natural, la justicia y la equidad.

**14.** E**ncíclica:** fue originalmente una carta circular enviada a todas las iglesias de una zona en la antigua iglesia cristiana. En ese momento, la palabra puede ser usada para una carta enviada por cualquier obispo a sus fieles.

**15. Encíclica Populorum Progressio:** (latín: *El desarrollo de los pueblos*) es la carta encíclica del Papa Pablo VI promulgada el 26 de marzo de 1967.

La encíclica está dedicada a la cooperación entre los pueblos y al problema de los países en vías de desarrollo. El Papa denuncia que el desequilibrio entre países ricos y pobres se va agravando, critica al neocolonialismo y afirma el derecho de todos los pueblos al bienestar. Además presenta una crítica al capitalismo y al colectivismo marxista. Finalmente propone la creación de un fondo mundial para ayudar a los países en vías de desarrollo.

Es una de las más famosas e importantes de Pablo VI aun cuando en su momento fue objeto de debates (por ejemplo, en cuanto al derecho de los pueblos a rebelarse incluso con la fuerza contra un régimen opresor) y críticas por parte de los ambientes más conservadores.

16. **Ethernet:** Ethernet (también conocido como *estándar IEEE 802.3*) es un estándar de transmisión de datos para redes de área local que se basa en el siguiente principio:

    Todos los equipos en una red Ethernet están conectados a la misma línea de comunicación compuesta por cables cilíndricos.

17. **Evangelio**.- Significa ("mensaje", *buena noticia*) son los escritos que narran la historia de la vida, muerte, doctrina y milagros de Jesús de Nazaret. La proclamación del evangelio se conoce como evangelización. Existen cuatro evangelios contenidos en la Biblia, llamados evangelios canónicos, reconocidos como oficiales por las diferentes confesiones cristianas. Son conocidos con el nombre de sus supuestos autores: Mateo, Marcos, Lucas y Juan. La mayoría de los expertos considera que estos cuatro evangelios fueron escritos entre los años 65 y 100 d. C., aunque otros expertos proponen fechas más tempranas.

18. **Hacking:** Término para designar a alguien con talento, conocimiento, inteligencia e ingenuidad, especialmente relacionada con las operaciones de computadora, redes, seguridad, etc.

19. **Hardware:** Conjunto de los componentes que integran la parte material de una computadora.

20. **Inactiva:** Carente de acción o movimiento.

21. **Informática:** Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores.

22. **Información**: Es un conjunto organizado de datos, que constituye un mensaje sobre un cierto fenómeno o ente. La información permite resolver problemas y tomar decisiones, ya que su uso racional es la base del conocimiento. La información es una parte fundamental y necesaria en todo proceso comunicativo en cuanto que es significada por quien la recibe si existe entre receptor y emisor un código común. La información como concepto existe en la naturaleza y en la cultura y es trasformada y re significada por esta misma cultura que la produce socialmente o la toma de la naturaleza misma. La información conlleva, en si misma, una parte teórica y otra práctica que en el pensamiento humano se presentan como separadas. La unificación que desemboca en la construcción definitiva del concepto de información, se da por la interacción dialéctica entre lo teórico y lo práctico.

23. **Integridad:** implica rectitud, bondad, honradez, habilidad; alguien en quien se puede confiar.

24. **Lucro:** Ganancia o provecho que se saca de algo.

25. **Laico**: es el nombre dado a aquel fiel de la Iglesia Católica que no es miembro del clero.

26. **Metodología**.- (del griego *metà* "más allá", *odòs* "camino" y *logos* "estudio"), hace referencia al conjunto de procedimientos basados en principios lógicos, utilizados para alcanzar una gama de objetivos que rigen en una investigación científica o en una exposición doctrinal.[2] El término puede ser aplicado a las artes cuando es necesario efectuar una observación o análisis más riguroso o explicar una forma de interpretar la obra de arte.

27. **Pablo VI**: 262ºPapa de la Iglesia católica. Ejerció su función Papal desde 21 de junio de 1963 al 6 de agosto de 1978. Las encíclicas de Pablo VI mostraron la preocupación de la Iglesia por problemas del mundo moderno como el subdesarrollo (*Populorum Progressio*, 1967) o el control de la natalidad (*Humanae vitae*, 1968). Pero demostraron también moderación ante las presiones que algunos sectores impulsaron tras el Concilio Vaticano II: en contraste con el impulso progresista de los sectores más radicalizados de la Iglesia, Pablo VI se mostró más conciliador, pragmático y conservador. Así, por ejemplo, Pablo VI se negó a alterar el sistema tradicional de elección de los papas para evitar que el cónclave se convirtiera en una especie de Parlamento democrático (1975).

28. **Proxy:** Es un programa o dispositivo que realiza una tarea acceso a Internet en lugar de otro ordenador. Un proxy es un punto intermedio entre un ordenador conectado a Internet y el servidor que está accediendo. Cuando navegamos a través de un proxy, nosotros en realidad no estamos accediendo directamente al servidor, sino que realizamos una solicitud sobre el proxy y es éste quien se conecta con el servidor que queremos acceder y nos devuelve el resultado de la solicitud.

    Cuando nos conectamos con un proxy, el servidor al que accedemos en realidad recibe la solicitud del proxy, en vez de recibirla directamente desde nuestro ordenador. Puede haber sistemas proxy que interceptan diversos servicios de Internet. Lo más habitual es el proxy web, que sirve para interceptar las \conexiones con la web y puede ser útil para incrementar la seguridad, rapidez de navegación o anonimato.

    El proxy web es un dispositivo que suele estar más cerca de nuestro ordenador que el servidor al que estamos accediendo. Este suele tener lo que denominamos una caché, con una copia de las páginas web que se van visitando. Entonces, si varias personas que acceden a Internet a través del mismo proxy acceden al primer sitio web, el proxy la primera vez accede físicamente al servidor destino, solicita la página y la guarda en la caché,

además de enviarla al usuario que la ha solicitado. En sucesivos accesos a la misma información por distintos usuarios, el proxy sólo comprueba si la página solicitada se encuentra en la caché y no ha sido modificada desde la última solicitud. En ese caso, en lugar de solicitar de nuevo la página al servidor, envía al usuario la copia que tiene en la caché. Esto mejora el rendimiento o velocidad de la conexión a Internet de los equipos que están detrás del proxy.

Otro caso típico de uso de un proxy es para navegar anónimamente. Al ser el proxy el que accede al servidor web, el proxy puede o no decir quién es el usuario que lo está utilizando. El servidor web puede entonces tener constancia de que lo están accediendo, pero puede que piense que el usuario que lo accede es el propio proxy, en lugar del usuario real que hay detrás del proxy. Hay proxies anónimos y los hay que sí informan del usuario real que está conectado a través del él.

Utilizar un proxy también tiene sus desventajas, como posibilidad de recibir contenidos que no están actualizados, tener que gestionar muchas conexiones y resultar un cuello de botella, o el abuso por personas que deseen navegar anónimamente. También el proxy puede ser un limitador, por no dejar acceder a través suyo a ciertos protocolos o puertos.

29. **Red:**Una red informática, red de computadoras o de ordenadores, es un conjunto de computadoras conectadas entre sí compartiendo información, recursos como CD-ROM, impresoras, grabadoras de DVD y servicios como e-mail, Chat, conexiones a Internet, juegos, etc.

    Podemos clasificar a cualquier red informática según la direccionalidad de los datos o por los tipos de transmisión: Red informática simplex unidireccional, en la que una computadora transmite y otra recibe. Red informática half-duplex bidireccionales, en la que solo una computadora transmite por vez. Y la Red informática full-dúplex, red en la que ambas computadoras pueden transmitir y recibir información a la vez.

Para que la transmisión de la información se produzca en una red informática es necesario el uso de lo que se conoce como protocolo de red o de comunicación. El protocolo de red es un conjunto de reglas encargadas de gestionar el orden de los mensajes que se producen entre las computadoras u ordenadores que componen la red informática.

A las redes informáticas también se las suele clasificar por su localización, así si nuestra red informática es una red de área local tendríamos una LAN (del inglés Local Area Network). Si fuese un área de red metropolitana sería una MAN (Metropolitan Area Network). Un área de red amplia WAN (Wide Area Network). O si fuese un área de red personal PAN (Personal Area Network).

Podemos establecer otra clasificación de las redes informáticas según la forma que tenga. Por ejemplo, Red de Bus: es aquella red informática que permite que una computadora transmita información y todas las demás reciben esa información. Red en Estrella: red informática que se une en un único punto como por ejemplo un concentrador de cables. Red en Anillo: red informática en la que todas las computadoras están unidas unas con otras formando un círculo por un cable común. Red en Token Ring: es una red con forma de anillo pero se diferencia de esta anterior en que cada computadora dentro del anillo controla el paso de la información y lo transmite a la que le corresponde. La información en esta red está perfectamente controla y solo se transmite a la computadora receptora de esa información.

30. **Riesgos:** Contingencia o proximidad de un daño.

31. **Seguridad:** El término seguridad proviene de la palabra *securitas* del latín. Cotidianamente se puede referir a la seguridad como la ausencia de riesgo o también a la confianza en algo o alguien. Sin embargo, el término puede tomar diversos sentidos según el área o campo a la que haga referencia. La seguridad es un estado de ánimo, una sensación, una cualidad intangible. Se

puede entender como un objetivo y un fin que el hombre anhela constantemente como una necesidad primaria.

32. **Software:** Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.

33. **Ups:**(Uninterruptible Power Supply - Sistema de alimentación ininterrumpida). Un UPS es una fuente de suministro eléctrico que posee una batería con el fin de seguir dando energía a un dispositivo en el caso de interrupción eléctrica. Los UPS son llamados en español SAI (Sistema de alimentación ininterrumpida).

    Los UPS suelen conectarse a la alimentación de las computadoras, permitiendo usarlas varios minutos en el caso de que se produzca un corte eléctrico. Algunos UPS también ofrecen aplicaciones que se encargan de realizar ciertos procedimientos automáticamente para los casos en que el Que puede ser herido o recibir lesión, física o moralmente.

    **Tipos de UPS**

    SPS (Standby Powe rSystems) u off-line: un SPS se encarga de monitorear la entrada de energía, cambiando a la batería apenas detecta problemas en el suministro eléctrico. Ese pequeño cambio de origen de la energía puede tomar algunos milisegundos. Más información en: UPS off-line.

    UPS on-line: un UPS on-line, evita esos milisegundos sin energía al producirse un corte eléctrico, pues provee alimentación constante desde su batería y no de forma directa. El UPS on-line tiene una variante llamada bypass.

    **Componentes típicos de los UPS**

Rectificador: rectifica la corriente alterna de entrada, proveyendo corriente continua para cargar la batería. Desde la batería se alimenta el inversor que nuevamente convierte la corriente en alterna. Cuando se descarga la batería, ésta se vuelve a cargar en un lapso de 8 a 10 horas, por este motivo la capacidad del cargador debe ser proporcional al tamaño de la batería necesaria.

* Batería: se encarga de suministrar la energía en caso de interrupción de la corriente eléctrica. Su capacidad, que se mide en Amperes Hora, depende de su autonomía (cantidad de tiempo que puede proveer energía sin alimentación).

* Inversor: transforma la corriente continua en corriente alterna, la cual alimenta los dispositivos conectados a la salida del UPS.

* Conmutador (By-Pass) de dos posiciones, que permite conectar la salida con la entrada del UPS (By Pass) o con la salida del inversor.

**34. VLAN:**(*Red de área local virtual* o *LAN virtual*) es una red de área local que agrupa un conjunto de equipos de manera lógica y no física.

Efectivamente, la comunicación entre los diferentes equipos en una red de área local está regida por la arquitectura física. Gracias a las redes virtuales (VLAN), es posible liberarse de las limitaciones de la arquitectura física (limitaciones geográficas, limitaciones de dirección, etc.), ya que se define una segmentación lógica basada en el agrupamiento de equipos según determinados criterios (direcciones MAC, números de puertos, protocolo, etc.).

**Tipos de VLAN**

Se han definido diversos tipos de VLAN, según criterios de conmutación y el nivel en el que se lleve a cabo:

**VLAN de nivel 1** (también denominada *VLAN basada en puerto*) define una red virtual según los puertos de conexión del conmutador;

**VLAN de nivel 2** (también denominada *VLAN basada en la dirección MAC*) define una red virtual según las direcciones MAC de las estaciones. Este tipo de VLAN es más flexible que la VLAN basada en puerto, ya que la red es independiente de la ubicación de la estación;

**VLAN de nivel 3**: existen diferentes tipos de VLAN de nivel 3:

**VLAN basada en la dirección de red** conecta subredes según la dirección IP de origen de los datagramas. Este tipo de solución brinda gran flexibilidad, en la medida en que la configuración de los conmutadores cambia automáticamente cuando se mueve una estación. En contrapartida, puede haber una ligera disminución del rendimiento, ya que la información contenida en los paquetes debe analizarse detenidamente.

**VLAN basada en protocolo** permite crear una red virtual por tipo de protocolo (por ejemplo, TCP/IP, IPX, AppleTalk, etc.). Por lo tanto, se pueden agrupar todos los equipos que utilizan el mismo protocolo en la misma red.

**Ventajas de la VLAN**

La VLAN permite definir una nueva red por encima de la red física y, por lo tanto, ofrece las siguientes ventajas:

Mayor flexibilidad en la administración y en los cambios de la red, ya que la arquitectura puede cambiarse usando los parámetros de los conmutadores; aumento de la seguridad, ya que la información se encapsula en un nivel adicional y posiblemente se analiza; disminución en la transmisión de tráfico en la red.

35. **Vulnerabilidad:** Que puede ser herido o recibir lesión, física o moralmente.

# 8 ANEXOS

**ANEXOS ISO 27001:2005:**

**Anexo A**

Al escuchar la palabra “Control”, automáticamente viene a la mente la idea de alarma, hito, evento, medición, monitorización, etc., en el caso de este estándar, el concepto de “Control”, es mucho más que eso, pues abarca todo el conjunto de acciones, documentos, medidas a adoptar, procedimientos, medidas técnicas.

Un “Control” es lo que permite garantizar que cada aspecto, que se valoró con un cierto riesgo, queda cubierto y auditable; ¿Cómo? De muchas formas posibles.

El estándar especifica en su “Anexo A” el listado completo de cada uno de ellos, agrupándolos en once rubros. Para cada uno de ellos define el objetivo y lo describe brevemente.

Cabe aclarar que el anexo A proporciona una buena base de referencia, no siendo exhaustivo, por lo tanto se pueden seleccionar más aún. Es decir, estos 133 controles (hoy) son los mínimos que se deberán aplicar, o justificar su no aplicación, pero esto no da por completa la aplicación de la norma si dentro del proceso de análisis de riesgos aparecen aspectos que quedan sin cubrir por algún tipo de control. Por lo tanto, si a través de la evaluación de riesgos se determina que es necesaria la creación de nuevos controles, la implantación del SGSI impondrá la inclusión de los mismos, sino seguramente el ciclo no estará cerrado y presentará huecos claramente identificables.

Los controles que el anexo A de esta norma propone quedan agrupados y numerados de la siguiente forma:

A.5 Política de seguridad

A.6 Organización de la información de seguridad
A.7 Administración de recursos
A.8 Seguridad de los recursos humanos

A.9 Seguridad física y del entorno
A.10 Administración de las comunicaciones y operaciones
A.11 Control de accesos
A.12 Adquisición de sistemas de información, desarrollo y mantenimiento
A.13 Administración de los incidentes de seguridad
A.14 Administración de la continuidad de negocio
A.15 Cumplimiento (legales, de estándares, técnicas y auditorías)

## II.DESARROLLO DE LOS CONTROLES

En este ítem, para ser más claro, se respetará la puntuación que la norma le asigna a cada uno de los controles.

*A.5 Política de seguridad.*

Este grupo está constituido por dos controles y es justamente el primer caso que se puede poner de manifiesto sobre el mencionado “Des concepto” sobre lo que uno piensa que es un control, pues aquí se puede apreciar claramente la complejidad que representa el diseño, planificación, preparación, implementación y revisiones de una Política de Seguridad (la revisión es justamente el segundo control que propone) como se mencionó “un Control es mucho (pero mucho), más que eso”

Todo aquel que haya sido responsable alguna vez de esta tarea, sabrá de lo que se está hablando.
La Política de Seguridad, para ser riguroso, en realidad debería dividirse en dos documentos:

-Política de seguridad (Nivel político o estratégico de la organización): Es la mayor

línea rectora, la alta dirección. Define las grandes líneas a seguir y el nivel de compromiso de la dirección con ellas.

-Plan de Seguridad (Nivel de planeamiento o táctico): Define el “Cómo”. Es decir, baja a un nivel más de detalle, para dar inicio al conjunto de acciones o líneas rectoras que se deberán cumplir.

Algo sobre lo que generalmente no se suele reflexionar o remarcar es que: Una “Política de Seguridad” bien planteada, diseñada, y desarrollada cubre la gran mayoría de los aspectos que hacen falta para un verdadero SGSI.

Haciendo abuso de la avanzada edad de este autor, es que se van a citar dos puntos de partida para la mencionada actividad que, a juicio del mismo, siguen siendo grandes referentes metodológicos a la hora de la confección de estos controles.

Se trata de lo que proponen las siguientes RFCs (Request For Comments). Política de seguridad (RFC – 2196Site Security Handbook) y también la anterior (RFC-1244, que si bien queda obsoleta por la primera es muy ilustrativa) ambas, planten una metodología muy eficiente de feedback partiendo desde el plano más alto de la Organización hasta llegar al nivel de detalle, para comparar nuevamente las decisiones tomadas y reingresar las conclusiones al sistema evaluando los resultados y modificando las deficiencias. Se trata de un ciclo permanente y sin fin cuya característica fundamental es la constancia y la actualización de conocimientos. Esta recomendación plantea muy en grande los siguientes pasos:

Política de Seguridad (RFC1244)
Análisis de riesgo
Grado de exposición
Plan de Seguridad (semejante a Certificación ISO)
Plan de contingencia

La política es el marco estratégico de la Organización, es el más alto nivel. El

análisis de riesgo y el grado de exposición determinan el impacto que puede producir los distintos niveles de clasificación de la información que se posee. Una vez determinado estos conceptos, se pasa al que es el Plan de Seguridad, el cual, si bien en esta RFC no está directamente relacionado Cómo con las normas ISO, se mencionan en este texto por la similitud en la elaboración de procedimientos de detalle para cada actividad que se implementa, y porque se reitera, su metodología se aprecia como excelente

*A.6 Organización de la información de seguridad.*

Este segundo grupo de controles abarca once de ellos y se subdivide en:

Compromiso de la Dirección, coordinaciones, responsabilidades, - Organización Interna: autorizaciones, acuerdos de confidencialidad, contactos con autoridades y grupos de interés en temas de seguridad, revisiones independientes.

- Partes externas: Riesgos relacionados con terceros, gobierno de la seguridad respecto a clientes y socios de negocio.

Lo más importante a destacar de este grupo son dos cosas fundamentales que abarcan a ambos subgrupos:

-Organizar y Mantener actualizada la cadena de contactos (internos y externos), con el mayor detalle posible (Personas, responsabilidades, activos, necesidades, acuerdos, riesgos, etc.).

-Derechos y obligaciones de cualquiera de los involucrados.

En este grupo de controles, lo ideal es diseñar e implementar una simple base de datos, que permita de forma amigable, el alta, baja y/o modificación de cualquiera de estos campos. La redacción de la documentación inicial de responsables: derechos y obligaciones (para personal interno y ajeno) y el conjunto de medidas a adoptar con cada uno de ellos. Una vez lanzado este punto de partida, se debe documentar la metodología de actualización, auditabildad y periodicidad de informes de la misma.

*A.7 Administración de recursos*

Este grupo cubre cinco controles y también se encuentra subdividido en:

-Responsabilidad en los recursos: Inventario y propietario de los recursos, empleo aceptable de los mismos.

-Clasificación de la información: Guías de clasificación y Denominación, identificación y tratamiento de la información.

Este grupo es eminentemente procedimental y no aporta nada al aspecto ya conocido en seguridad de la información, en cuanto a que todo recurso debe estar perfectamente inventariado con el máximo detalle posible, que se debe documentar el "uso adecuado de los recursos" y que toda la información deberá ser tratada de acuerdo a su nivel. En el caso de España, tanto la LOPD como la LSSI han aportado bastante a que esta tarea sea efectuada con mayor responsabilidad en los últimos años. También se puede encontrar en Internet varias referencias a la clasificación de la información por niveles.

Tal vez sí valga la pena mencionar aquí el problema que se suele encontrar en la gran mayoría de las empresas que cuentan con un parque informático considerable, sobre el cual, se les dificulta mucho el poder mantener actualizado su sistema de inventario. El primer comentario, es que este aspecto debe abordarse "sí o sí", pues es imposible pensar en seguridad, si no se sabe fehacientemente lo que se posee y cada elemento que queda desactualizado o no se lo ha inventariado aún, es un hueco concreto en la seguridad de todo el sistema, y de hecho suelen ser las mayores y más frecuentes puertas de entrada, pues están al margen de la infraestructura de seguridad.

El segundo comentario, es que se aprecia que las mejores metodologías a seguir para esta actividad, son las que permiten mantener "vivo" el estado de la red y por medio de ellas inventariar lo que se "escucha". Esta metodología lo que propone es, hacer un empleo lógico y completo de los elementos de red o seguridad (IDSs, Firewalls, Routers, sniffers, etc.) y aprovechar su actividad cotidiana de escucha y

tratamiento de tramas para mantener “vivo” el estado de la red. Es decir, nadie mejor que ellos saben qué direcciones de la “Home Net” se encuentran activas y cuáles no, por lo tanto, aprovechar esta funcionalidad para almacenar y enviar estos datos a un repositorio adecuado, el cual será el responsable de mantener el inventario correspondiente. Sobre este tema, se propone la lectura de dos artículos publicados hace tiempo en Internet por este autor que se denominan “Metodología Nessus-Snort” y “Matriz de Estado de Seguridad”, si bien los mismos deben ser actualizados al día de hoy, de ellos se puede obtener una clara imagen de cómo se puede realizar esta tarea y aprovechar las acciones de seguridad para mejorar el análisis de riesgo y el inventario.

*A.8 Seguridad de los recursos humanos.*

Este grupo cubre nueve controles y también se encuentra subdividido en:

- Antes del empleo: Responsabilidades y roles, verificaciones curriculares, términos y condiciones de empleo.

- Durante el empleo: Administración de responsabilidades, preparación, educación y entrenamiento en seguridad de la información, medidas disciplinarias. Finalización de responsabilidades, devolución de recursos.

-Finalización o cambio de empleo:

Este grupo, en la actualidad, debe ser el gran ausente en la mayoría de las organizaciones. Se trata de un serio trabajo a realizar entre RRHH y los responsables de Seguridad de la Información de la organización.

Se debe partir por la redacción de la documentación necesaria para la contratación de personal y la revocación de sus contratos (por solicitud, cambio o despido).En la misma deberá quedar bien claro las acciones a seguir para los diferentes perfiles de la organización, basados en la responsabilidad de manejo de información que tenga ese puesto. Como se pueda apreciar, tanto la contratación como el cese de un puesto, es una actividad conjunta de estas dos

áreas, y cada paso deberá ser coordinado, según la documentación confeccionada, para que no se pueda pasar por alto ningún detalle, pues son justamente estas pequeñas omisiones de las que luego resulta el haber quedado con alta dependencia técnica de personas cuyo perfil es peligroso, o que al tiempo de haberse ido, mantiene accesos o permisos que no se debieran (casos muy comunes).

Tanto el inicio como el cese de cualquier tipo de actividad relacionada con personal responsable de manejo de información de la organización, son actividades muy fáciles de procedimental, pues no dejan de ser un conjunto de acciones secuenciales muy conocidas que se deben seguir “a raja tabla” y que paso a paso deben ser realizadas y controladas……..se trata simplemente de¡¡¡ESCRIBIRLO!!! (y por supuesto de cumplirlo luego), esto forma parte de las pequeñas cosas que cuestan poco y valen mucho ¿Por qué será que no se hacen?

En cuanto a formación, para dar cumplimiento al estándar, no solo es necesario dar cursos.

La formación en seguridad de la información, no puede falta contar con un “Plan de formación ser una actividad aperiódica y determinada por el deseo o el dinero en un momento dado, tiene que ser tratada como cualquier otra actividad de la organización, es decir se debe plantear:

Meta a la que se desea llegar.

Determinación de los diferentes perfiles de conocimiento.

Forma de acceder al conocimiento.

Objetivos de la formación.

Metodología a seguir.

Planificación y asignación de recursos.

Confección del plan de formación.

Implementación del plan.

Medición de resultados.

Mejoras.

Si se siguen estos pasos, se llegará a la meta, pero no solo a través de la impartición de uno o varios cursos o la distribución de documentos de obligada lectura, sino con un conjunto de acciones que hará que se complementen e integren en todo el SGSI como una parte más, generando concienciación y adhesión con el mismo.

*A.9 Seguridad física y del entorno*

Este grupo cubre trece controles y también se encuentra subdividido en:

-Áreas de seguridad:

Seguridad física y perimetral, control físico de entradas, seguridad de locales edificios y recursos, protección contra amenazas externas y del entorno, el trabajo en áreas e seguridad, accesos públicos, áreas de entrega y carga.

-Seguridad de elementos: Ubicación y protección de equipos, elementos de soporte a los equipos, seguridad en el cableado, mantenimiento de equipos, seguridad en el equipamiento fuera de la organización, seguridad en la redistribución o reutilización de equipamiento, borrado de información y/o software.

A juicio del autor, uno de los mejores resultados que se pueden obtener en la organización de una infraestructura de seguridad de la información, está en plantearla siempre por niveles. Tal vez no sea necesario hacerlo con el detalle de los siete niveles del modelo ISO/OSI, pero sí por lo menos de acuerdo al modelo TCP/IP que algunos consideran de cuatro (Integrando físico y enlace) y otros de cinco niveles.

Nuevamente el criterio de este autor, aprecia que es correcto considerar separadamente el nivel físico con el de enlace, pues presentan vulnerabilidades muy diferentes. Si se presenta entonces el modelo de cinco niveles, se puede organizar una estructura de seguridad contemplando medidas y acciones por cada uno de ellos, dentro de las cuales se puede plantear, por ejemplo, lo siguiente:

Aplicación: Todo tipo de aplicaciones.

Transporte: Control de puertos UDP y TCP.

Red: Medidas a nivel protocolo IP e ICMP, túneles de nivel 3.

Enlace: Medidas de segmentación a nivel direccionamiento MAC, tablas estáticas y fijas en switchs, control de ataques ARP, control de broadcast y multicast a nivel enlace, en el caso WiFi: verificación y control de enlace y puntos de acceso, 802.X (Varios), empleo de túneles de nivel2, etc.

Físico: Instalaciones, locales, seguridad perimetral, CPDs, gabinetes de comunicaciones, control de acceso físico, conductos de comunicaciones, cables, fibras ópticas, radio enlaces, centrales telefónicas (Tema a desarrollar en este punto).

Como se puede apreciar, este es una buena línea de pensamiento para plantear cada una de las actividades y evitar que se solapen algunas de ellas y/o que queden brechas de seguridad.

En el caso físico, es conveniente también separar todas ellas, por lo menos en los siguientes documentos:

Documentación de control de accesos y seguridad perimetral general, áreas de acceso y entrega de materiales y documentación, zonas públicas, internas y restringidas, responsabilidades y obligaciones del personal de seguridad física.

Documentación de CPDs: Parámetros de diseño estándar de un CPD, medidas

de protección y alarmas contra incendios/humo, caídas de tensión, inundaciones, control de climatización (Refrigeración y ventilación), sistemas vigilancia y control de accesos, limpieza, etc.

Documentación y planos de instalaciones, canales de comunicaciones, cableado, enlaces de radio, ópticos u otros, antenas, certificación de los mismos, etc.

Empleo correcto del material informático y de comunicaciones a nivel físico debe desarrollar aquí cuales son las medidas de seguridad física que se debe tener en cuenta sobre los mismos (Ubicación, acceso al mismo, tensión eléctrica, conexiones físicas y hardware permitido y prohibido, manipulación de elementos, etc.) .No se incluye aquí lo referido a seguridad lógica o Seguridad física en el almacenamiento y transporte de material informático y de comunicaciones: Zonas y medidas de almacenamiento, metodología a seguir para el ingreso y egreso de este material, consideraciones particulares para el transporte del mismo (dentro y fuera de al organización), personal autorizado a recibir, entregar o sacar material, medidas de control. No se incluye aquí lo referido a resguardo y recuperación de información que es motivo de otro tipo de procedimientos y normativa.

Documentación de baja, redistribución o recalificación Procedimientos y conjunto de medidas a seguir ante cualquier cambio en el estado de un elemento de Hardware (Reubicación, cambio de rol, venta, alquiler, baja, destrucción, compartición con terceros, incorporación de nuevos módulos, etc.).

**Anexo B**

El anexo B es informativo, a su vez proporciona una breve guía de los principios de administración de riesgos de sistemas de información, redes y su correspondencia con el modelo PDCA.

**Anexo C**

También informativo, se resume la correspondencia entre esta norma y los estándares ISO 9001 y el ISO 14001.

# 9 BIBLIOGRAFÍA


- Carlos Ernesto Ortega, Finanzas Populares y migración: tejiendo la red para el desarrollo local, Abril 2009, ImpreFEPP, Quito-Ecuador.

- Luis María Gavilanes del Castillo, El FEPP: Llamada, pulso y Desafío, Julio 1995, ImpreFEPP, Quito-Ecuador.

- Grupo Social FEPP, Finanzas populares para una economía campesina de bienestar, Enero 2005, ImpreFEPP, Quito-Ecuador.

- Susan Engel, Trazando un camino de equidad, Septiembre 2004, ImpreFEPP, Quito-Ecuador.

- Gustavo Betarte, Hacia una Implementación Exitosa de un SGSI, Febrero 2007, La Castilla, Montevideo-Uruguay.

- Fabricio Cirilli, Implementación y Certificación de los sistemas de seguridad de la información, Madrid-España, 2007, ISMS ForumSpain.

- Alberto G. Alexander, Diseño de un sistema de gestión de seguridad de información. Óptica ISO 27001:2005, México, 2007, Alfa omega Grupo Editor.

- ICONTEC, Sistema de Gestión de la Seguridad de la Información (SGSI). Compendio, Cali-Colombia, Julio 2009, Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC

- Portal de la ISO 270001 en español, Sistema de Gestión de la Seguridad de la Información, [en línea] Madrid España, [ref. 22 noviembre 2009] Disponible en web: http://www.iso27000.es/sgsi.html

- Portal del Instituto Nacional de Tecnologías de la Comunicación (INTELCO), Centro de respuestas a incidentes de seguridad, [en línea] Madrid España Disponible en web: https://cert.inteco.es/Formacion/SGSI

- Portal ISMS ForumSpain. Asociación Española para el Fomento de la Seguridad de la Información. Disponible en Web: www.ismsforum.es

- Portal Registro internacional de organizaciones certificadas en ISO 27001 y BS 7799-2. Disponible en Web: www.iso27001certificates.com

- Portal de Cooperación Interamericana de Acreditación. Disponible en Web: www.iaac.org.mx

- Portal de la Comisión Panamericana de Normas Técnicas. Disponible en Web: www.copant.org

- Presentaciones y lecturas de la Conferencia sobre privacidad de 2005: Disponible en Web: http://www.privacyconference2005.org/index.php?id=6#present