UNIVERSIDAD MAYOR DE SAN ANDRES

FACULTAD DE CIENCIAS ECONÓMICAS Y FINANCIERAS

CARRERA DE CONTADURIA PÚBLICA

MÉTODO DE AUDITORÍA PARA LA SEGURIDAD DE SISTEMAS DE INFORMACIÓN BAJO EL MODELO ISO 27000

Proyecto de Grado

por

Verónica Liseth Marca Alcón

Tutor Metodológico

M.Sc. Miguel Cotaña Mier

La Paz – Bolivia

2015

INDICE

1. CAPITULO I. Marco introductorio 2
1.1.Introducción 2
1.2.Antecedentes 5
1.3.Planteamiento del Problema 6
1.4.Formulación del Problema 8
1.5.Objetivos 8
1.5.1. Objetivo General 8
1.5.2. Objetivos Específicos 8
1.6.Importancia y Justificación del Estudio 8
1.6.1. Justificación económica 9
1.6.2. Justificación Social 9
1.6.3. Viabilidad 9
1.7.Alcances y Aportes 9
1.7.1. Alcances 9
1.7.2. Aportes 10
1.8.Marco Metodológico 10

2. CAPITULO II. Marco Teórico 12
2.1. Seguridad 12
2.1.1. Incidentes de seguridad 14
2.1.2. ¿Cuál es el objetivo? 14
2.1.3. ¿Qué entendemos por control? 15
2.1.4. ¿Qué entendemos por seguridad? 15
2.1.5. ¿Qué queremos proteger? 16
2.1.6. ¿Cuál es la información más valiosa? 17
2.1.7. ¿De qué nos queremos proteger? 17
2.1.8. Elementos que comprometen la seguridad 20

2.1.9. ¿Cómo nos podemos proteger? 28
2.1.10. Mecanismos de seguridad 30
2.1.11. Seguridad física 32
2.2. Administración del riesgo 32
2.2.1. Elementos principales 33
2.2.2. Proceso de administración del riesgo 34
2.3. Modelo OSI 17799 43
2.3.1. ISO/UNE/IEC 17799 44
2.4. Modelo ISO 27000 54
2.4.1. Sistemas de Gestión de Seguridad de la Información (SGSI) 57
2.4.1.1. Esquema general 58
2.4.1.2. Modelo de gobierno y gestión para las TIC 66
2.5. Normas de Auditoría de las Tecnologías de Información y Comunicación 68
2.5.1. Enfoques de la auditoría 68
2.5.2. Normas de auditoría de TIC´s 70
2.6. Auditoría 75
2.6.1. Clases de auditoría 77
2.6.2. Definición de auditoría 78
2.6.3. Importancia de la auditoría 78
2.6.4. El proceso de la auditoría informática 78
3. CAPITULO III. Marco institucional 82
3.1. Antecedentes de la organización 82
3.2. Justificación 82
3.3. Fundamentos institucionales 84
3.3.1. Historia institucional 84
3.3.2. Naturaleza jurídica 86
3.3.3. El FNDR y su adecuación a las políticas de cambio 87
3.4. Misión 90

3.5. Visión 90
3.6. Objetivos 91
3.6.1.Objetivos estratégicos 91
3.6.2. Objetivos institucionales 91
3.7. Estructura orgánica institucional 92
3.8. Departamento de sistemas del FNDR 93

4. CAPITULO IV. Marco aplicativo 95
4.1. Contexto 95
4.2. Proceso metodológico 95
4.2.1. Planificar 96
4.2.2. Hacer 96
4.2.2.1. Política de seguridad 101
4.2.2.2. Estructura organizativa 101
4.2.2.3. Clasificación y control de activos 103
4.2.2.4. Seguridad ligada al personal 104
4.2.2.5. Seguridad física y del entorno 106
4.2.2.6. Gestión de comunicaciones y operaciones 108
4.2.2.7. Control de accesos 113
4.2.2.8. Desarrollo y mantenimiento de los sistemas 117
4.2.2.9. Gestión de incidentes de seguridad 120
4.2.2.10. Gestión de continuidad del negocio 121
4.2.2.11. Conformidad y cumplimiento 122
4.2.3. Verificar 123
4.2.4. Actuar 124
5. CAPITULO IV. CONCLUSIONES Y RECOMENDACIONES 127
5.1. Conclusiones 127
2.2. Recomendaciones 128

Referencia bibliográfica
Documentos

CAPITULO I.

Marco Introductorio

CAPÍTULO I. Marco Introductorio

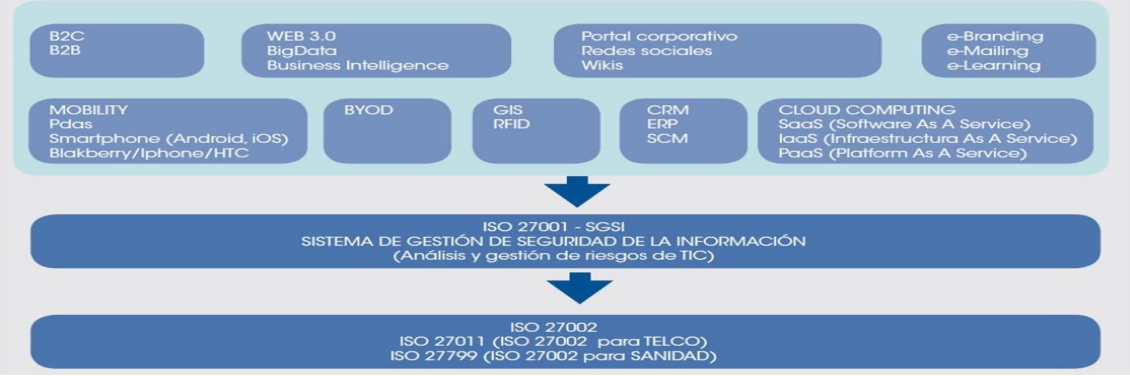
1.1.Introducción

La información es como el aparato circulatorio para las organizaciones y requiere que se proteja ante cualquier amenaza que pueda poner en peligro las empresas tanto públicas como privadas, pues en otro caso podría dañarse la salud empresarial.

La información es un activo que, como otros activos importantes del negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada. Esto es importante en un mundo interconectado. Como resultado de esta creciente actividad, la información está expuesta a un mayor rango de amenazas y vulnerabilidades.

La información adopta diversas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, enviada por correo o medios electrónicos, mostrada en video o hablada en conversación. Debería protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene.

La realidad nos muestra que las organizaciones se enfrentan en la actualidad con un alto número de riesgos e inseguridades procedentes de una amplia variedad de fuentes (ver figura 1.1), entre las que se encuentran los nuevos negocios y nuevas herramientas de las Tecnologías de la Información y la Comunicación (TIC), que los CEO (Directores Generales) y CIO (Directores de Informática) deberían aplicar.



FUENTE: AENOR. Figura 1.1 Nuevos negocios y herramientas TIC para CEO, CIO

Todas estas herramientas deben aplicarse según objetivos empresariales con la mayor seguridad, garantizando la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (garantizando que la información es fiable y exacta) y disponibilidad (asegurando que los usuarios autorizados tienen el acceso debido a la información).

La información, como uno de los principales activos de las organizaciones, debe protegerse a través de la implantación, mantenimiento y mejora de las medidas de seguridad para que cualquier empresa logre sus objetivos de negocio, garantice el cumplimiento legal, de prestigio y de imagen de la compañía. Por lo que se deben tomar las medidas preventivas, detectivas y/o correctivas de seguridad y protección de la información.

Los datos que son la base para generar información que tiene una organización almacenada en una Base de Datos, posiblemente sea el fruto de años de trabajo, es con toda probabilidad su activo más valioso, ya que si se perdieran toda la información referente a los clientes, a los proveedores o a la actividad que la entidad realiza, es posible que no se pudiera continuar.

Tradicionalmente esta información se almacenaba en grandes ficheros, pero con la implantación de los Sistemas de Información, hoy en día se hace en ordenadores. Esto ha facilitado que el nivel de información que se maneja sea mucho mayor, ya que en un simple ordenador se pude almacenar la misma información que en varias toneladas de papel.

Con este volumen de información se ha aumentado enormemente la dependencia de las organizaciones hacia esta, hasta llegar al punto actual, donde es imposible prosperar en cualquier campo sin un buen Sistema de Información.

A medida que el valor de la información se fue incrementando, también lo han hecho sus amenazas. Hace algunos años atrás, a ningún empresario se le podía ocurrir

que le robaran un archivo con sus clientes, sin embargo hoy día, esta información es un objetivo de ladrones como cualquier otro.

Otro factor importante que ha hecho que sean más las amenazas hacia la información es el propio desconocimiento de los Sistemas de Información empleados en las organizaciones.

Lamentablemente, aún hoy en día, muchos empresarios y altos cargos de grandes entidades no dan a la información la importancia que tiene, por lo que no conocen las posibles amenazas que pueden ponerla en peligro, ni los sistemas que existen para asegurarla.

La Seguridad de Sistemas de Información, tanto física como lógica, consiste en asegurar que los recursos tecnológicos (Software, hardware, comunicaciones y datos) de una organización sean utilizados de la manera como se planeó.

La necesidad de contar con una guía para una eventual Auditoría para la Seguridad de Sistemas de Información es una demanda de las empresas y/o instituciones, puesto que la ejecución de auditorías ayuda a minimizar los riesgos y vulnerabilidades de los sistemas frente a ataques tanto externos como internos.

La auditoría consiste en la emisión de una opinión profesional sobre un determinado objeto. El objeto, ahora es Tecnología de la Información (TI). Es de este aspecto que se deriva puntualmente la Auditoria para la Seguridad de los Sistemas de Información.

La ISO 27000 es la norma que explica cómo implantar un Sistema de Gestión de Seguridad de la Información en una empresa. La implantación de una *ISO 27000* en una organización permite proteger la información de ésta de la forma más fiable posible. Se persiguen 3 objetivos:

1. Preservar la confidencialidad de los datos de la empresa
2. Conservar la integridad de estos datos
3. Hacer que la información protegida se encuentre disponible

El presente proyecto de grado, hace un aporte significativo al proporcionar un método y/o metodología de auditoría para la seguridad de sistemas de información bajo el estándar internacional ISO 27000 aplicable al Fondo Nacional de Desarrollo Regional (FNDR), que a través de la Unidad de Sistemas, tiene el objetivo de mantener a la institución tecnológicamente actualizada aplicando políticas, procedimientos y reglamentos adecuados.

1.2.Antecedentes

La información es el activo más importante de cada organización. Evidentemente se tendrán otros activos, pero todos ellos será posible adquirirlos de algún modo, sin embargo si tenemos algún problema de seguridad con la información de la empresa no será posible volverla a adquirir. Este es el principal motivo por el que debemos dedicamos a garantizar, de alguna manera, la seguridad de la información corporativa.

A nivel mundial y particularmente en nuestro país, la amenaza más común se centra en la perforación de los niveles de seguridad de los Sistemas de Información. A esto, debemos añadir la revolución de las telecomunicaciones y la dependencia de los procesos de negocio de la empresa con tecnología informática.

De la investigación efectuada, se ha podido consultar los siguientes trabajos existentes en la biblioteca de la Carrera de Contaduría Pública:

- ✓ Evaluación de los Sistemas de Información y su tecnología como base para determinar el grado de confianza en el procesamiento de la Información Financiera. Trabajo Dirigido, defendido el 2005 por: José Antonio Celis Rioja. El objetivo fue proporcionar a la auditoría financiera una metodología que contenga procedimientos y técnicas para evaluar los Sistemas de Información y su tecnología, y determinar el grado de confianza en el procesamiento de la información financiera.
- ✓ Un enfoque metodológico para auditoría de Tecnologías de la Información y Comunicaciones. Caso: Registro único para la administración tributaria

municipal. Tesis de Grado, defendido el 2012 por: Janhett Ramos Maldonado. El objetivo fue la elaboración y sistematización de un enfoque metodológico para la ejecución de auditorías de Tecnologías de la Información y Comunicación en el marco de las Normas de Auditoria Gubernamental de Tecnologías de la Información y Comunicación en los procesos tecnológicos de la administración pública.

- ✓ Guía de gestión de seguridad de la información del auditor en las entidades comerciales de la ciudad de La Paz. Tesis de grado, defendido el 2008 por: Erick Mendoza Gorriti. El trabajo de investigación desarrolla la guía de gestión de seguridad de la información, ante la falta de políticas y procedimientos en seguridad en las entidades comerciales.

1.3.Planteamiento del problema

La información es el activo más importante de cada organización. Evidentemente se tendrán otros activos, pero todos ellos será posible adquirirlos de algún modo, sin embargo si tenemos algún problema de seguridad con la información de la empresa no será posible volverla a adquirir. Este es el principal motivo por el que debemos dedicamos a garantizar, de alguna manera, la seguridad de la información corporativa.

Lamentablemente, la gestión de la seguridad de la información en una empresa está descoordinada, no sigue un criterio común definido, cada departamento o área funcional del negocio, especialmente el de Tecnologías de la Información (TI), tiene sus propias políticas y procedimientos, establecidos sin una visión global de las necesidades de la organización, incluso alejadas de los objetivos del negocio. O peor aún, no tiene normas, procedimientos, políticas que garantice la seguridad tanto física como lógica de los Sistemas de Información.

Hoy en día la amenaza más común se centra en la perforación de los niveles de seguridad de los Sistemas de Información. A esto, debemos añadir la revolución de

las telecomunicaciones y la dependencia de los procesos de negocio de la empresa con tecnología informática.

Los procesos de negocio de la organización, en la actualidad, están automatizados de alguna manera. Pero, no se puede garantizar la seguridad plena. La Seguridad de los Sistemas de Información, en un problema de la gente, es un problema cultural, en el que el usuario juega un rol determinante.

La implantación de un método y/o metodología de auditoría para la seguridad de sistemas de información bajo el estándar internacional ISO 27000 aplicable al Fondo Nacional de Desarrollo Regional (FNDR), será la manera más eficaz de conseguir esta coordinación y gestión necesaria para poder orientar los esfuerzos y recursos, dedicados a la seguridad de la información, hacia una dirección que refuerce la consecución de los objetivos de la organización.

La gestión de la seguridad debe ser un proceso de mejora continua y de constante adaptación a los cambios en la organización en cuanto a procesos de negocio y a la tecnología implicada.

La seguridad de la información se desarrolla atendiendo a tres dimensiones principales:

Confidencialidad: entendida como la garantía del acceso a la información únicamente de los usuarios autorizados;

Integridad: entendida como la preservación de la información de forma completa y exacta;

Disponibilidad: Entendida como la garantía del acceso a la información en el instante en que el usuario la necesita.

1.4.Formulación del problema

¿El diseño de un método de auditoría para la seguridad de Sistemas de Información basada en la norma internacional ISO 27000 proporcionará una herramienta

lógica y formal para facilitar y guiar en las actividades de aseguramiento de un entorno automatizado?

1.5.Objetivos

1.5.1. Objetivo General

Desarrollar un método de auditoría para la seguridad de entornos informáticos basado en el estándar ISO 27000 aplicable al Fondo Nacional de Desarrollo Regional (FNDR).

1.5.2. Objetivos Específicos

- ✓ Investigar fuentes bibliográficas referentes a la práctica de auditoría y seguridad en ambientes computarizados;
- ✓ Revisar normas, procedimientos, políticas y estándares que dan soporte a la implementación de seguridad lógica y física.
- ✓ Analizar e identificar las amenazas y vulnerabilidades;
- ✓ Investigar ISO 9126, ISO 17799, ISO 2700;
- ✓ Desarrollar el método.

1.6.Importancia y Justificación del Estudio

El desarrollo de un método y/o metodología de auditoria para la seguridad de Sistemas de Información basado en el estándar de la familia ISO 27000 facilita que esta se convierta en una guía especializada o herramienta para quienes realizan procesos de auditoría, ya que se deben definir una serie de actividades, acciones y tareas metódicos que apunten a lo que se quiere concluir y que genere una lista de recomendaciones que mejoren las falencias encontradas.

Este trabajo de grado se justifica porque puede convertirse en una fuente de documentación sobre el tema y en una herramienta para verificar la seguridad de la información y la detección de riesgos en los Sistemas de Información con que cuenta la entidad.

1.6.1. Justificación económica

El uso de un método y/o metodología de auditoria para la seguridad, agrega valor a la entidad, porque minimiza costos teniendo a disposición una referencia metodológica.

1.6.2. Justificación social

Una nueva cultura de control, da paso de una sociedad industrial a una sociedad de sobreabundancia de información y comunicación; pasar de la simple idea de mitigar riesgos y amenazas a la capacidad de brindar garantía razonable de seguridad, integridad, confiabilidad, disponibilidad y auditabilidad de los datos contenidos en un Sistema de Información

1.6.3. Viabilidad

El alcance del objetivo de este trabajo será viable solo si los integrantes de la empresa u organización cambien de actitud. Y acepten que no podemos quedar aislados del resto del mundo en cuanto a la gestión de la seguridad.

1.7.Alcances y aportes

1.7.1. Alcances

El estudio de la auditoria a la seguridad a Sistemas de Información es extenso, por lo que limitaremos nuestro alcance a la aplicación de la NAG-270 que son de aplicación obligatoria en nuestro Estado Plurinacional, para entidades públicas, bajo los siguientes enfoques:

- Enfoque a las seguridades;
- Enfoque a la información;
- Enfoque a la infraestructura tecnológica;
- Enfoque al software de aplicación;
- Enfoque a las comunicaciones y redes.

Asimismo, nos apoyaremos en conceptos de gestión de riesgos, bajo el modelo ISO.

1.7.2. Aportes

Proponer y diseñar un método y/o metodología de auditoría de la seguridad, aplicable al Fondo Nacional de Desarrollo Regional (FNDR),

1.8.Marco metodológico

El estudio que se realizará consiste en una investigación que consiste en la investigación documental, exploratorio deductivo.

Diseño de la investigación

Es un plan global que integra de un modo coherente y adecuadamente correcto. Esta investigación se sustenta en fuentes mixtas por originarse en investigación documental (referencias de materiales impresos y de información existente en la red Internet, documentos y/o bibliografía existente que sirva de base al estudio y al fundamento teórico, principalmente velar por la seguridad de los Sistemas de Información

La investigación documental se centra en el estudio del problema de control de la información y las tecnologías que la soportan al interior de las organizaciones. Aplicando diferentes técnicas como: Observación, entrevistas, simulación, cuestionarios, análisis de la información documental entregada por el auditado, revisión y Análisis de Estándares, revisión.

CAPITULO II.

Marco Teórico

El presente capítulo, pretende mostrar las bases teóricas para luego, ofrecer un modelo para establecer, implementar, operar, monitorear, mantener y mejorar un efectivo Sistema de Gestión de Seguridad de la Información. La adopción de un modelo de seguridad, debe ser una decisión estratégica para una determinada organización. El diseño e implementación del modelo, está influenciado por las necesidades y objetivos del negocio, requisitos de seguridad, procesos, tamaño y estructura de la organización.

2.1. Seguridad

La seguridad no es un problema que pueda resolverse una vez y para siempre. Es una tira y afloja entre buenos y malos. La clave es garantizar que la organización esté consciente acerca de la seguridad y la ejercita con sentido común.

Debemos estar conscientes que:

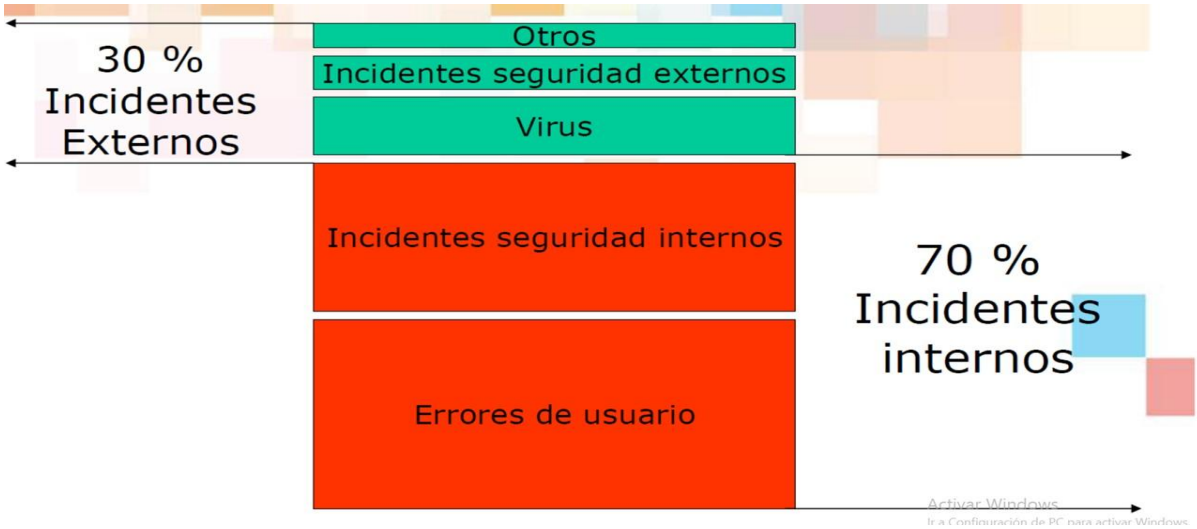
- No existe la "verdad absoluta" en Seguridad Informática;
- No es posible eliminar todos los riesgos;
- No se puede ser especialista en todos los temas;
- Cada vez los riesgos y el impacto en los negocios son mayores;
- No se puede dejar de hacer algo en este tema.

Principales riesgos (ver figura 2.1 y 2.2)

FUENTE: ORACLE 2005. Figura 2.1 Amenazas

FUENTE: ORACLE 2005. Figura 2.2 Amenazas

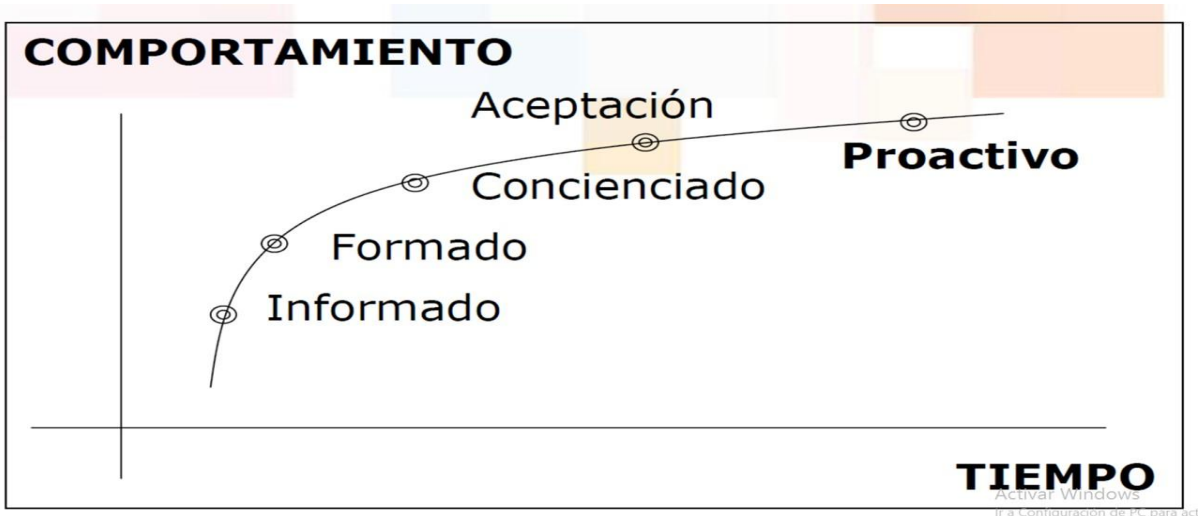
2.1.1 Incidentes de seguridad ¿Quién es quién?. (ver figura 2.3)



FUENTE: NEXTEL. Figura 2.3 Incidentes de seguridad

2.1.2 ¿Cuál es el objetivo?

Proteger al negocio (aplicar seguridad) a cada una de las actividades, acciones y tareas de la organización (la información) mediante el conjunto de personas que cumplen distintos roles en la entidad (ver figura 2.4)



FUENTE: NEXTEL. Figura 2.4. Cambio de actitud

2.1.3. ¿Qué entendemos por control?

Conjunto de estructuras, políticas y procedimientos que permiten:

- Verificar el cumplimiento de los objetivos y estrategias de gestión fijados por la Dirección
- Conocer y gestionar los riesgos a los que está expuesta la entidad

Entonces, Control se define como las políticas, procedimientos, prácticas e infraestructuras organizativas, diseñadas para garantizar razonablemente, que los objetivos de negocio se llevarán a cabo, y que las incidencias no deseadas se pueden prevenir o detectar y corregir. (COSO 1992)

Objetivo de control de TI, Se define como el propósito o resultado que se desea alcanzar, mediante la implantación de procedimientos de control para una actividad de TI específica.

2.1.4. ¿Qué entendemos por seguridad?

Podemos indicar que es una característica de cualquier sistema (informático o no) que nos indica que ese sistema está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible.

Es muy difícil de conseguir seguridad total, por lo que podemos hablar de fiabilidad (probabilidad de que un sistema se comporte tal y como se espera de él). Se habla de sistemas fiables en lugar de hacerlo de sistemas seguros.

Se puede definir a la seguridad como: “Calidad de estar libre y cubierto de todo riesgo”. Extraído del Diccionario de la Real Academia Española de Lengua.

La seguridad absoluta es inalcanzable. Llega un momento en el que los gastos en seguridad dejan de ser rentables. La seguridad absoluta tendría un costo infinito.

Otra definición: “Calidad relativa resultado del equilibrio entre el riesgo (constituido por amenazas, vulnerabilidades e impacto) y las medidas adoptadas para paliarlo”

Ésta es una definición mucho más amplia, dice que si el riesgo es grande las medidas que se tomarán para paliarlo serán extremas, por el contrario si el riesgo es pequeño, las medidas serán pequeñas. También se tendrá que tener presente la repercusión que tendría el que cierto elemento quede desprotegido. Las medidas de seguridad han de ser proporcionales a los medios que queremos proteger.

A grandes rasgos se entiende que mantener un sistema seguro (o fiable) consiste básicamente en garantizar tres aspectos:

a) **Confidencialidad:** La información sólo debe ser conocida por los usuarios, entidades o procesos autorizados en el tiempo y forma previstos. Podemos indicar que cuando la información hace referencia a datos de carácter personal, se podría denominar privacidad, aunque éste término nos indica que el individuo tiene derecho a controlar la recogida y almacenamiento de los datos;
b) **Integridad:** La información solo debe ser alterada o modificada por los usuarios autorizados y registrada para posteriores controles o auditorias. La información debe ser exacta y completa. Proyecto de Fin de Carrera Auditoría Informática de la Seguridad Física
c) **Disponibilidad:** Los usuarios deben poder acceder a la información en el tiempo y la forma autorizada. Esto requiere que la información se mantenga correctamente almacenada.

2.1.5. ¿Qué queremos proteger?

En cualquier sistema informático existen generalmente los siguientes elementos principales a proteger, que son:

- ✓ Software;
- ✓ Hardware;
- ✓ Comunicaciones;
- ✓ Datos;
- ✓ Fungibles.

El último elemento, del que se habla generalmente en las auditorías de seguridad, los fungibles, son elementos que se gastan o desgastan con el uso continuo, como papel de impresora y su tóner o tinta o cabezales de impresión. También se pueden denominar fungibles a los CDs, CD-ROMs, cintas y disquetes.

2.1.6. ¿Cuál es la información más valiosa que manejamos?

- La información asociado a nuestros clientes;
- La información asociado a nuestras ventas;
- La información asociada a nuestro personal;
- La información asociada a nuestros productos;
- La información asociada a nuestras operaciones.

2.1.7. ¿De qué nos queremos proteger?

Como en la mayoría de los trabajos de investigación que se hacen sobre seguridad de Sistemas de Información, vamos a intentar clasificar los diferentes elementos que pueden atacar nuestro sistema.

Con frecuencia, especialmente en las obras menos técnicas y más orientadas a otros aspectos de la seguridad, se suele identificar a los atacantes únicamente como personas; esto tiene sentido si hablamos por ejemplo de responsabilidades por un delito informático.

Pero es preferible hablar de "elementos" y no de personas: aunque a veces lo olvidemos, nuestro sistema puede verse perjudicado por múltiples entidades aparte de humanos, como por ejemplo programas o fallos de hardware, catástrofes naturales, incendios o inundaciones; si una empresa pierde la base de datos de todos sus clientes, poco le importará que haya sido un intruso, un virus, un simple error del hardware o una inundación (salvo quizá por temas de seguros y lo que esté cubierto, etc.).

Se puede clasificar a continuación varias agrupaciones de los elementos que pueden atacar nuestra entidad, dependiendo de:

a) Su origen:

i) Naturales. Se producen de manera espontánea y son causadas por fenómenos

naturales.

- Terremotos. Aunque casi inexistentes en nuestro País, hasta los pequeños temblores pueden provocar grandes pérdidas;
- Tormentas eléctricas. Pueden provocar daños eléctricos, así como incendios y otros daños;
- Temperatura. Las temperaturas extremas, sobre todo el calor, pueden provocar daños y malfuncionamiento en los equipos;
- Humedad. Al igual que la temperatura, puede dañar seriamente los equipos eléctricos;
- Lluvias. Pueden ser la causa de inundaciones;
- Otros Factores. Menos importantes, pueden ser el viento, el granizo, etc.

ii) Accidentales. Son los que se producen de manera espontánea pero no son causa de la naturaleza.

- Errores humanos (accidentes). Tiene una importancia alta y son muy comunes.
- Pueden afectar a casi todos los factores de seguridad de la entidad;
- Fallos en equipos (hardware). Son poco habituales;
- Malfuncionamiento de programas (software). Son bastante habituales e
- importantes;
- Radiaciones electromagnéticas. Son poco habituales, pero dada la creciente red de tecnologías Wi-Fi y móviles, va muy en aumento.

iii) Deliberadas o Intencionadas. Son las que se producen a propósito. Pueden tener

múltiples fines.

- Fraudes. Son muy frecuentes;
- Sabotajes. Pueden ser materiales (como la rotura de los canales de comunicaciones, etc.) o inmateriales (por medio de virus, etc.);
- Hurtos. Igualmente pueden ser materiales (los que todos conocemos, equipos, dinero, etc.) o inmateriales (robo de software, datos, etc.).

b) Su actuación:

i) Pasivas. No alteran el estado de la información por lo que son las más difíciles de

descubrir. Amenazan a la confidencialidad.

- Interceptación. Leen nuestra información, por ejemplo, pinchando una línea de
- Datos;
- Copia. Hacen una copia de los datos desde el sitio físico en el que se encuentran.

ii) Activas. Estas alteran el estado de la información.

- Interrupción. Amenaza la disponibilidad. Por ejemplo, cortando el cable de datos, la red eléctrica, etc.;
- Modificación (de los datos). Amenaza la integridad. Por ejemplo, entrando en el sistema (remotamente o desde el lugar físico);
- Fabricación. Generar datos o software e integrarlos en el sistema. Afecta a la Integridad;
- Destrucción. Borran o destruyen documentos, equipos o software de la entidad.

c) Su procedencia:

- Errores internos. Fuente de mayores pérdidas en conjunto. Provocada por la aparición de errores en el software, hardware, sistemas de ventilación, errores humanos, etc.;

- Empleados infieles. Por múltiples motivos: empleados descontentos, intereses económicos, etc.;
- Desastres. Son los menos habituales, pero si no se está preparado, son los más destructivos. Por ejemplo una inundación o un incendio;
- Acciones de terceros. Vienen del exterior de la entidad. Tienen múltiples orígenes y objetivos y pueden ser intencionados o no.

2.1.8. Elementos que comprometen la seguridad

Los posibles elementos que comprometen la seguridad de una entidad son:

a) Personas: Debemos estar conscientes que la mayoría de ataques a nuestra entidad van a provenir en última instancia de personas que, intencionada o inintencionadamente, pueden causarnos enormes pérdidas. A nivel lógico, podemos hablar de piratas que, con distintos fines, intentan conseguir el control o acceso a los sistemas aprovechando alguno de los riesgos lógicos, especialmente agujeros del software. Pero con demasiada frecuencia se suele olvidar que los piratas "clásicos" no son los únicos que amenazan nuestros equipos. Es especialmente preocupante que mientras que hoy en día cualquier administrador mínimamente preocupado por la seguridad va a conseguir un sistema relativamente fiable de una forma lógica (permaneciendo atento a vulnerabilidades de su software, restringiendo servicios, utilizando cifrado de datos, etc.), pocos administradores tienen en cuenta factores físicos**,** como el acceso a la sala donde existen elementos vulnerables o un buen sistema de recuperación de datos, ya que podemos ser víctimas de sabotajes.

   Aquí se describen brevemente los diferentes tipos de personas que de una u otra forma pueden constituir un riesgo para nuestros sistemas; generalmente se dividen en dos grandes grupos: los atacantes pasivos, aquellos que fisgonean por el sistema pero no lo modifican (o destruyen), y los activos, aquellos que dañan el objetivo atacado, o lo modifican en su favor. Generalmente los curiosos y los crackers realizan ataques pasivos (que se pueden convertir en activos), mientras que los terroristas y exempleados

realizan ataques activos puros; los intrusos remunerados suelen ser atacantes pasivos si nuestra red o equipo no es su objetivo, y activos en caso contrario. El personal realiza ambos tipos indistintamente, dependiendo de la situación concreta. ;

- El personal: Las amenazas a la seguridad de un sistema provenientes del personal de la propia entidad rara vez son tomadas en cuenta; se presupone un entorno de confianza donde a veces no existe, por lo que se pasa por alto el hecho de que casi cualquier persona de la entidad, incluso el personal ajeno a la infraestructura informática (secretariado, personal de seguridad, personal de limpieza y mantenimiento, etc.) puede comprometer la seguridad de los equipos, los datos y la entidad en general.

  Lo más normal es que más que de ataques se trate de accidentes causados por un error o por desconocimiento de las normas básicas de seguridad: un empleado de mantenimiento que corta el suministro eléctrico para hacer una reparación o un cigarrillo olvidado pueden ser tanto o más peligrosos como el más experto de los administradores que se equivoca al teclear una orden y borra todos los sistemas de ficheros. En los dos primeros casos, los "atacantes" ni siquiera han de tener acceso lógico (ni físico) a los equipos, ni conocer nada sobre seguridad.

  Sin embargo, los ataques intencionados son extremadamente dañinos y peligrosos, recordemos que nadie mejor que el propio personal de la entidad conoce mejor los sistemas y sus debilidades. Estos pueden deberse a múltiples cusas, pero el soborno de terceros a personal de la entidad para conseguir datos o accesos es lo más normal. Los ataques llevados a cabo por el personal de la entidad tiene además la característica de que pueden no ser descubiertos jamás;
- Ex empleados: Otro gran grupo de personas potencialmente interesadas en atacar nuestra entidad son los antiguos empleados o trabajadores de la misma, especialmente los que no abandonaron el entorno por voluntad propia (y en el

caso de redes de empresas, los que pasaron a la competencia). Generalmente, se trata de personas descontentas con la entidad, conocen y han tenido acceso previo al sistema y pueden intentar acceder a él para dañarlo como venganza por algún hecho que no consideran justo, para obtener información y venderla a terceros o incluso para modificar datos de cuentas y nóminas de la entidad y así seguir cobrando como si aún trabajaran para ésta. Además pueden obtener información delicada para la entidad o para el personal, y de esta manera chantajear a sus ex-jefes o ex-compañeros.

Podemos incluir en este grupo a personas externas a la entidad, que han trabajado para ésta o con ésta y tienen conocimiento del sistema, incluso de las contraseñas de acceso. Por eso es muy importante que la entidad permita el acceso al sistema sólo durante el periodo de tiempo necesario y sepa en todo momento quién y cuándo accede;

- Los Curiosos: Junto con los crackers, los curiosos son los atacantes más habituales de sistemas informáticos. Suelen ser personas ajenas al sistema pero con curiosidad por la seguridad del mismo. No suelen tener malas intenciones.

  Teniendo en cuenta que tanto futuros profesionales de la informática y las telecomunicaciones como profesionales ya consagrados en éstas áreas, son personas que a priori tiene mucho interés por las nuevas tecnologías; y recordemos que las personas suelen ser curiosas por naturaleza. Esta combinación produce una avalancha de estudiantes o personal intentando conseguir mayor privilegio del que tienen o intentando acceder a sistemas a los que oficialmente no tienen acceso. Y en la mayoría de ocasiones esto se hace simplemente para leer el correo de un amigo, enterarse de cuánto cobra un compañero, copiar un trabajo o comprobar que es posible romper la seguridad de un sistema concreto. Aunque en la mayoría de situaciones se trata de ataques no destructivos (a excepción del borrado de huellas para evitar

la detección), parece claro que no benefician en absoluto al entorno de fiabilidad que podamos generar en un determinado sistema;

- Los Crackers: Su objetivo es romper el sistema de seguridad. Están especializados en sistemas de protección de software de seguridad media, aunque sus técnicas se utilizan también para romper sistemas de protección de acceso a aplicaciones. Estos entornos de seguridad media (redes de I+D, universidades, etc.) son un objetivo típico de los intrusos, ya sea para fisgonear, para utilizarlas como enlace hacia otras redes o simplemente por diversión. Por un lado, son redes generalmente abiertas, y la seguridad no es un factor tenido muy en cuenta en ellas; por otro, el gran número y variedad de sistemas conectados a estas redes provoca, casi por simple probabilidad, que al menos algunos de sus equipos (cuando no la mayoría) sean vulnerables a problemas conocidos de antemano. De esta forma un atacante sólo ha de utilizar un escáner de seguridad contra el dominio completo y luego atacar mediante un simple *exploit (*Programa o técnica que aprovecha un error de programación para obtener diversos privilegios) los equipos que presentan vulnerabilidades.

  Esto convierte a las redes de I+D, a las de empresas, o a las de *ISPs* (*Internet Service Provider*. hace referencia al sistema informático remoto al cual se conecta un ordenador personal y a través del cual se accede a Internet.) en un objetivo fácil y apetecible para piratas con cualquier nivel de conocimientos, desde los más novatos (y a veces más peligrosos) hasta los expertos, que pueden utilizar toda la red para probar nuevos ataques o como nodo intermedio en un ataque a otros organismos, con el consiguiente deterioro de imagen (y a veces de presupuesto) que supone para una universidad ser, sin desearlo, un apoyo a los piratas que atacan sistemas teóricamente
  más protegidos, como los militares.
- Los terroristas: Por "terroristas" no debemos entender simplemente a los que se dedican a poner bombas o quemar autobuses; bajo esta definición se engloba a cualquier persona que ataca al sistema simplemente por causar

algún tipo de daño en él. Por ejemplo, alguien puede intentar borrar las bases de datos o destruir los sistemas de ficheros de un servidor que alberga páginas WEB.

En el caso de redes de I+D, típicos ataques son la destrucción de sistemas de prácticas o la modificación de páginas WEB de algún departamento o de ciertos profesores, generalmente por parte de alumnos descontentos. Su principal objetivo es por tanto, la destrucción.

- Los intrusos remunerados: Este es el grupo de atacantes de un sistema más peligroso, aunque por fortuna el menos habitual en redes normales; suele afectar más a las grandes - muy grandes - entidades o a organismos de defensa. Se trata de piratas con gran experiencia en problemas de seguridad y un amplio conocimiento del sistema, que son pagados por una tercera parte generalmente para robar secretos (el nuevo diseño de un procesador, una base de datos de clientes, información confidencial sobre las posiciones de satélites espía, etc.) o simplemente para dañar la imagen de la entidad afectada. Esta tercera parte suele ser una empresa de la competencia o un organismo de inteligencia, es decir, una organización que puede permitirse un gran gasto en el ataque; de ahí su peligrosidad: se suele pagar bien a los mejores piratas y, por si esto fuera poco, los atacantes van a tener todos los medios necesarios a su alcance.;

b) Las amenazas lógicas: Bajo la etiqueta de “amenazas lógicas” encontramos todo tipo de programas que de una forma u otra pueden dañar a nuestro sistema, creados de forma intencionada para ello (software malicioso, también conocido como *malware* (viene de *malicius software*, son programas o archivos dañinos para el ordenador, están diseñados para insertar virus, gusanos, troyanos o *spyware* para conseguir algún objetivo, como podría ser el de recoger información sobre el usuario o sobre el ordenador en sí) o simplemente por error (*bugs,* error de software, resultado de un fallo de programación en el proceso de creación del software o agujeros).

- Software incorrecto: Las amenazas más habituales a un sistema informático provienen de errores cometidos de forma involuntaria por los programadores de sistemas operativos o de aplicaciones. Una situación no contemplada a la hora de diseñar el sistema de red o un error accediendo a memoria en un fichero pueden comprometer local o remotamente al sistema.

  A estos errores de programación se les denomina *bugs* (agujeros), y a los programas utilizados para aprovechar uno de estos fallos y atacar al sistema, *exploits*. Como se indicó líneas arriba, representan la amenaza más común contra los sistemas, ya que cualquiera puede conseguir un *exploit* y utilizarlo contra nuestra máquina sin ni siquiera saber cómo funciona y sin unos conocimientos mínimos. Incluso, hay *exploits* que dañan seriamente la integridad de un sistema (negaciones de servicio o accesos privilegiados remotos) y están preparados para ser utilizados desde cualquier sistema operativo y sin ningún conocimiento de informática, con lo que cualquier pirata novato o *Script Kiddie* (persona que presume de ser un *hacker* o *cracker* cuando en realidad no posee un grado de conocimientos suficientes. Normalmente usa *cracks, exploits* y programas similares construidos por personas con grandes conocimientos pero cuyo uso está al alcance de cualquiera) puede utilizarlos contra un servidor y conseguir un control total de una máquina de millones de dólares desde su PC, sin saber nada del sistema atacado;
- Herramientas de seguridad: Cualquier herramienta de seguridad representa un arma de doble filo: de la misma forma que un administrador las utiliza para detectar y solucionar fallos en sus sistemas o en la subred completa, un potencial intruso las puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar los equipos. Herramientas como NESSUS, SAINT o SATAN pasan de ser útiles a ser peligrosas cuando las utilizan

crackers que buscan información sobre las vulnerabilidades de un *host* o de una red completa.

La conveniencia de diseñar y distribuir libremente herramientas que puedan facilitar un ataque es un tema serio; incluso expertos reconocidos como Alec Muffet (autor del adivinador de contraseñas *Crack*) han recibido enormes críticas por diseñar determinadas herramientas de seguridad. Tras numerosos debates sobre el tema, ha quedado bastante claro que no se puede basar la seguridad de un sistema en el supuesto desconocimiento de sus problemas por parte de los atacantes: esta política, denominada *Security Through Obscurity*, se ha demostrado inservible en múltiples ocasiones. Si los administradores no utilizan herramientas de seguridad que muestren las debilidades de los sistemas (para corregirlas), tenemos que estar seguro que un atacante no va a dudar en utilizar tales herramientas (para explotar las debilidades encontradas); por tanto, hemos de agradecer a los diseñadores de tales programas el esfuerzo que han realizado (y nos han ahorrado) en pro de sistemas más seguros.

- Puertas traseras: Durante el desarrollo de aplicaciones grandes o de sistemas operativos es habitual entre los programadores insertar "atajos" en los sistemas habituales de autenticación del programa o del núcleo que se está diseñando. A estos atajos se les denomina puertas traseras, y con ellos se consigue mayor velocidad a la hora de detectar y depurar fallos: por ejemplo, los diseñadores de un software de gestión de bases de datos en el que para acceder a una tabla se necesiten cuatro claves diferentes de diez caracteres cada una pueden insertar una rutina para conseguir ese acceso mediante una única clave "especial", con el objetivo de perder menos tiempo al depurar el sistema. Algunos programadores pueden dejar estos atajos en las versiones definitivas de su software para facilitar un mantenimiento posterior, para garantizar su propio acceso, o simplemente por descuido; la cuestión es que si un atacante descubre una de estas puertas traseras (no nos importa el método que utilice para hacerlo) va a

tener un acceso global a datos que no debería poder leer, lo que obviamente supone un grave peligro para la integridad de nuestro sistema;

- Bombas lógicas: Las bombas lógicas son partes de código de ciertos programas que permanecen sin realizar ninguna función hasta que son activadas; en ese punto, la función que realizan no es la original del programa, sino que generalmente se trata de una acción perjudicial. Los activadores más comunes de estas bombas lógicas pueden ser la ausencia o presencia de ciertos ficheros, la ejecución bajo un determinado *login* o la llegada de una fecha concreta; cuando la bomba se activa va a poder realizar cualquier tarea que pueda realizar la persona que ejecuta el programa: si las activa el administrador los efectos obviamente pueden ser fatales;
- Canales abiertos: Los canales cubiertos (o canales ocultos, según otras traducciones) son canales de comunicación que permiten a un proceso transferir información de forma que viole la política de seguridad del sistema; dicho de otra forma, un proceso transmite información a otros (locales o remotos) que no están autorizados a leer dicha información. Los canales cubiertos no son una amenaza demasiado habitual en redes de I+D, ya que suele ser mucho más fácil para un atacante aprovechar cualquier otro mecanismo de ataque lógico; sin embargo, es posible su existencia, y en este caso su detección suele ser difícil: algo tan simple como el puerto *finger* (puerto que permite saber qué usuarios están conectados a la máquina. Se puede acceder a él por telnet) abierto en una máquina puede ser utilizado a modo de canal cubierto por un pirata con algo de experiencia;
- Virus: Un virus es una secuencia de código que se inserta en un fichero ejecutable (denominado huésped), de forma que cuando el archivo se ejecuta, el virus también lo hace, insertándose a sí mismo en otros programas.

En mayor o menor medida, todo el mundo conoce, incluso a padecido los efectos de los virus. Estos efectos son muy variados: formatear el disco duro, dañar el sector de arranque del PC, hacer que se reinicie, dañar algunos programas en concreto, mal funciones de video, etc. La mayoría de los efectos son perceptibles por el usuario, si bien existen virus que pueden actuar de manera más "silenciosa" haciendo que se relentice el sistema o se desconfigure. Esto podría dar más problemas, ya que si el usuario no sabe que está infectado no pondrá medios para subsanar este problema;

- Caballos de troya: Los troyanos o caballos de Troya son instrucciones escondidas en un programa de forma que éste parezca realizar las tareas que un usuario espera de él, pero que realmente ejecute funciones ocultas (generalmente en detrimento de la seguridad) sin el conocimiento del usuario; como el Caballo de Troya de la mitología griega, al que deben su nombre, ocultan su función real bajo la apariencia de un programa inofensivo que a primera vista funciona correctamente.

  De esta manera, cuando un intruso penetra en el sistema, instala troyanos para no ser descubierto o garantizarse el poder volver a entrar. Estos troyanos sustituyen a los programas habituales del sistema de modo que el usuario no se percate de que el atacante se encuentra conectado a su sistema
- Gusanos: Un gusano es un programa capaz de ejecutarse y propagarse por sí mismo a través de redes, en ocasiones portando virus o aprovechando *bugs* de los sistemas a los que conecta para dañarlos. Al ser difíciles de programar su número no es muy elevado, pero el daño que pueden causar es muy grande: el mayor incidente de seguridad en Internet fué precisamente el *Internet Worm*, un gusano que en 1988 causó pérdidas millonarias al infectar y detener más de 6.000 máquinas conectadas a la red.

Hemos de pensar que un gusano puede automatizar y ejecutar en unos segundos todos los pasos que seguiría un atacante humano para acceder a nuestro sistema: mientras que una persona, por muchos conocimientos y medios que posea, tardaría como mínimo horas en controlar nuestra red completa (un tiempo más que razonable para detectarlo), un gusano puede hacer eso mismo en pocos minutos: de ahí su enorme peligro y sus devastadores efectos.

2.1.9. ¿Cómo nos podemos proteger?

Para proteger nuestro sistema hemos de realizar un análisis de las amenazas potenciales que puede sufrir, las pérdidas que podrían generar, y la probabilidad de su ocurrencia; a partir de este análisis hemos de diseñar una política de seguridad que defina responsabilidades y reglas a seguir para evitar tales amenazas o minimizar sus efectos en caso de que se produzcan. A las medidas utilizadas para implementar esta política de seguridad se les denomina medidas de seguridad; su propósito es disminuir los riesgos (amenazas, vulnerabilidades, etc.) asociados a un activo en un momento y espacio concreto. No se habla de eliminar el riesgo, ya que siempre existirá un riesgo residual.

Podemos clasificar las medidas de seguridad en base a dos taxonomías:

a) Según su forma de actuación

- **Prevención**: Son aquellos que evitan que una amenaza se materialice. Aumentan la seguridad de un sistema durante el funcionamiento normal de éste, previniendo la ocurrencia de violaciones a la seguridad. Los ataques a la confidencialidad solo pueden protegerse mediante medidas de prevención. En el caso del incendio, un ejemplo sería instalar muebles ignífugos.
- **Detección:** Por medidas de detección se conoce a aquellas que se utilizan para detectar y avisar violaciones de la seguridad o intentos de violación que se están produciendo. Por ejemplo los sistemas de detección (no extinción) de incendios, como sensores de humo o de calor.

- **Corrección:** Las medidas de corrección son aquellas que corrigen o eliminan las violaciones de seguridad una vez que se han producido. Por ejemplo extintores o los sistemas de extinción de incendios.
- **Recuperación:** Son aquellas que se aplican cuando una violación del sistema se ha consumado, para retornar a éste a su estado anterior. Por ejemplo las primas de los seguros o las copias backup de los datos.
- **Análisis forense:** Es un subgrupo de la recuperación, cuyo objetivo no es simplemente retornar el sistema al estado anterior al ataque, sino averiguar el alcance de la violación, las actividades de un intruso en el sistema, las debilidades de la seguridad, etc. De esta forma se previenen ataques posteriores y se detectan ataques a otros sistemas de nuestra red. En el caso del incendio consistiría en ver como se ha producido, los activos afectados, como se ha sofocado, etc.

b) Según su naturaleza:

- Legales;
- Administrativo / Organizativas;
- Físicas;
- Técnicas.

2.1.10. Mecanismos de seguridad

Para poder aplicar medidas de seguridad y protección expuestas anteriormente se han de implementar una serie de mecanismos de seguridad. Estos mecanismos se implementan con software, hardware u otros dispositivos y reciben en ocasiones los mismos nombres que las medidas de seguridad. Los tipos de mecanismos son:

a) Mecanismos de autenticación e identificación: Estos mecanismos hacen posible identificar entidades del sistema de una forma única, y posteriormente, una vez identificadas, autenticarlas (comprobar que la entidad es quién dice ser). Son los mecanismos más importantes en cualquier sistema, ya que

forman la base de otros mecanismos que basan su funcionamiento en la identidad de las entidades que acceden a un objeto.

Un grupo especialmente importante de estos mecanismos son los denominados Sistemas de Autenticación de Usuarios, ya que es con lo primero que se van a encontrar los usuarios del sistema y la primera traba para los posibles atacantes;

b) Mecanismos de control de acceso: Cualquier objeto del sistema ha de estar protegido mediante mecanismos de control de acceso, que controlan todos los tipos de acceso sobre el objeto por parte de cualquier entidad del sistema;

c) Mecanismos de separación: Cualquier sistema con diferentes niveles de seguridad ha de implementar mecanismos que permitan separar los objetos dentro de cada nivel, evitando el flujo de información entre objetos y entidades de diferentes niveles siempre que no exista una autorización expresa del mecanismo de control de acceso. Los mecanismos de separación se dividen en cinco grandes grupos, en función de cómo separan a los objetos:

- Separación física;
- Temporal;
- Lógica;
- Criptográfica;
- Fragmentación.

d) Mecanismos de cifrado de datos: Son mecanismos básicos para la confidencialidad y la integridad. Existen múltiples técnicas de cifrado y en ellas se va a basar gran parte de la seguridad de los datos de la entidad, ya que, como hemos comentado antes, los ataques a la confidencialidad solo pueden ser protegidos por medidas de prevención, y el cifrado es un mecanismo utilizado en medidas de prevención;

e) Mecanismos de firma digital: Es un mecanismo que emplean las medidas de no repudio, verificando que una persona no pueda negar lo que ha hecho. La firma digital se encuentra incorporada en multitud de aplicaciones, tales como la presentación de la declaración del IRPF, la descarga de *plug-ins* auto

instalables en los navegadores, el acceso seguro a servidores WEB, el pago mediante tarjeta de crédito, etc. Sin embargo, la aplicación más popular e intuitiva de la firma digital es el correo electrónico;

f) Mecanismos de funciones resumen: Este mecanismo proporciona integridad a los datos. Consiste en la proyección de un conjunto, esto es, partiendo de un conjunto con un número elevado elementos (los datos) se llega mediante la función resumen a un conjunto con un número mucho menor de elementos (resumen). En criptografía ha de cumplir los siguientes requisitos:

- La entrada puede ser de un tamaño indeterminado;
- La salida es de un tamaño fijo, varios órdenes de magnitud menor que la entrada;
- Calcular la función resumen es computacionalmente barato;
- Es irreversible, esto es, con el resumen no se puede obtener la entrada;
- No presenta colisiones, esto es, a entradas distintas le corresponden resúmenes distintos.

g) Mecanismos de registros de auditoria: Se emplean en las medidas de auditoria. Son ficheros en los que se almacena información sobre quién y qué se hace. Además existen programas que interactúan con estos ficheros pueden decirnos, incluso en tiempo real, si existe algún problema en nuestro sistema, si alguien ha hecho algo que no debía o incluso si se ha equivocado más de dos veces al introducir su contraseña.

2.1.11. Seguridad física

2.1.11.1 ¿Qué entendemos por Seguridad Física?

Por lo general, cuando se habla de seguridad informática siempre se piensa en errores de software, virus, intrusos de red, etc. En definitiva, pensamos en software. La realidad es que la seguridad informática también implica otro aspecto muy importante y que generalmente permanece desatendido. Se trata de la Seguridad Física de un sistema.

¿De qué sirve que nadie pueda acceder de forma autorizada a los recursos lógicos del sistema, si cualquiera puede entrar por la puerta y llevarse el equipo debajo del brazo?

Por lo tanto, se deben tomar medidas en lo que respecta a la seguridad física del sistema, y por supuesto, cuando se definen dichas medidas hay que tener en cuenta a las personas que trabajan con los equipos informáticos.

> *"... la seguridad física de los sistemas informáticos consiste en la aplicación de barreras **físicas** y procedimientos de control como medidas de prevención y contramedidas contra las amenazas a los recursos y la información confidencial"*

Más claramente, por Seguridad Física podemos entender todos aquellos mecanismos destinados a proteger **físicamente** cualquier recurso del sistema. Estos recursos son desde un simple teclado hasta una cinta de backup con toda la información de nuestra entidad, pasando por la propia CPU de la máquina, el cableado eléctrico o el edificio al completo.

2.2. Administración del riesgo

La administración de riesgos es una parte integral del proceso de administración. La administración de riesgos es un proceso multifacético, aspectos apropiados del cual son a menudo llevados a cabo mejor por un equipo multidisciplinario. Es un proceso iterativo de mejora continua.

2.2.1 Elementos principales

Los elementos principales del proceso de administración de riesgos, son los siguientes:

a) **Establecer el contexto**: Establecer el contexto estratégico, organizacional y de administración de riesgos en el cual tendrá lugar el resto del proceso. Deberían

establecerse criterios contra los cuales se evaluarán los riesgos y definirse la estructura del análisis.

b) **Identificar riesgos:** Identificar qué, por qué y cómo pueden surgir las cosas como base para análisis posterior.

c) **Analizar riesgos**: Determinar los controles existentes y analizar riesgos en términos de consecuencias y probabilidades en el contexto de esos controles. El análisis debería considerar el rango de consecuencias potenciales y cuán probable es que ocurran esas consecuencias. Consecuencias y probabilidades pueden ser combinadas para producir un nivel estimado de riesgo.

d) **Evaluar riesgos:** Comparar niveles estimados de riesgos contra los criterios preestablecidos. Esto posibilita que los riesgos sean ordenados como para identificar las prioridades de administración. Si los niveles de riesgo establecidos son bajos, los riesgos podrían caer en una categoría aceptable y no se requeriría un tratamiento.

e) **Tratar riesgos:** Aceptar y monitorear los riesgos de baja prioridad. Para otros riesgos, desarrollar e implementar un plan de administración específico que incluya consideraciones de fondeo.

f) **Monitorear y revisar**: Monitorear y revisar el desempeño del sistema de administración de riesgos y los cambios que podrían afectarlo.

g) **Comunicar y consultar**: Comunicar y consultar con interesados internos y externos según corresponda en cada etapa del proceso de administración de riesgos y concerniendo al proceso como un todo.

La administración de riesgos se puede aplicar en una organización a muchos niveles. Se lo puede aplicar a nivel estratégico y a niveles operativos. Se lo puede aplicar a proyectos específicos, para asistir con decisiones específicas o para administrar áreas específicas reconocidas de riesgo.

La administración de riesgos es un proceso iterativo que puede contribuir a la mejora organizacional. Con cada ciclo, los criterios de riesgos se pueden fortalecer para alcanzar progresivamente mejores niveles de administración de riesgos. Para

cada etapa del proceso deberían llevarse registros adecuados, suficientes como para satisfacer a una auditoría independiente.

2.2.2 Proceso de administración del riesgo

2.2.2.1 Proceso de administración de riesgos

El proceso ocurre dentro de la estructura del contexto estratégico, organizacional y de administración de riesgos de una organización. Esto necesita ser establecido para definir los parámetros básicos dentro de los cuales deben administrarse los riesgos y para proveer una guía para las decisiones dentro de estudios de administración de riesgos más detallados. Esto establece el alcance para el resto del proceso de administración de riesgos.

2.2.2.2 Identificación de riesgos

General: Este paso busca identificar los riesgos a administrar. Es crítica una identificación amplia utilizando un proceso sistemático bien estructurado, porque los riesgos potenciales que no se identifican en esta etapa son excluidos de un análisis posterior. La identificación debería incluir todos los riesgos, estén o no bajo control de la organización.

Qué puede suceder: La intención es generar una lista amplia de eventos que podrían afectar a cada elemento de la estructura.

Cómo y por qué pueden suceder: Habiendo identificado una lista de eventos, es necesario considerar causas y escenarios posibles. Hay muchas formas en que se puede iniciar un evento. Es importante que no se omitan las causas significativas.

Herramientas y técnicas: Los enfoques utilizados para identificar riesgos incluyen:

- "checklists",
- Juicios basados en la experiencia y en los registros,
- Diagramas de flujo,
- "brainstorming",
- Análisis de sistemas,
- Análisis de escenarios;

- Técnicas de ingeniería de sistemas.

El enfoque utilizado dependerá de la naturaleza de las actividades bajo revisión y los tipos de riesgos.

2.2.2.3 Análisis de riesgos

Los objetivos de análisis son separar los riesgos menores aceptables de los riesgos mayores, y proveer datos para asistir en la evaluación y tratamiento de los riesgos. El análisis de riesgos involucra prestar consideración a las fuentes de riesgos, sus consecuencias y las probabilidades de que puedan ocurrir esas consecuencias. Pueden identificarse los factores que afectan a las consecuencias y probabilidades. Se analiza el riesgo combinando estimaciones de consecuencias y probabilidades en el contexto de las medidas de control existentes.

Se puede llevar a cabo un análisis preliminar para excluir del estudio detallado los riesgos similares o de bajo impacto. De ser posible los riesgos excluidos deberían listarse para demostrar que se realizó un análisis de riesgos completo.

Para determinar los controles existentes Identificar la administración, sistemas técnicos y procedimientos existentes para controlar los riesgos y evaluar sus fortalezas y debilidades. Pueden ser apropiadas las herramientas mencionadas líneas arriba, como asimismo los enfoques tales como inspecciones y técnicas de auto-evaluación de controles.

Por otro lado, la magnitud de las consecuencias de un evento, si el mismo ocurriera, y la probabilidad del evento y sus consecuencias asociadas, se evalúan en el contexto de los controles existentes. Las consecuencias y probabilidades se combinan para producir un nivel de riesgo. Se pueden determinar las consecuencias y probabilidades utilizando análisis y cálculos estadísticos. Alternativamente cuando no se dispone de datos anteriores, se pueden realizar estimaciones subjetivas que reflejan el grado de convicción de un individuo o grupo de que podrá ocurrir un evento o resultado particular. Para evitar prejuicios subjetivos cuando se analizan

consecuencias y probabilidades, deberían utilizarse las mejores técnicas y fuentes de información disponibles. Se pueden incluir las siguientes fuentes de información:

a) Registros anteriores;

b) Experiencia relevante;

c) Prácticas y experiencia de la industria;

d) Literatura relevante publicada;

e) Comprobaciones de marketing e investigaciones de mercado;

f) Experimentos y prototipos;

g) Modelos económicos, de ingeniería u otros;

h) Opiniones y juicios de especialistas y expertos.

Las técnicas incluyen:

i) entrevistas estructuradas con expertos en el área de interés;

ii) utilización de grupos multidisciplinarios de expertos;

iii) evaluaciones individuales utilizando cuestionarios;

iv) uso de modelos de computador u otros; y

v) uso de árboles de fallas y árboles de eventos.

Siempre que sea posible, debería incluirse el nivel de confianza asignado a las estimaciones de los niveles de riesgo.

El análisis de riesgos puede ser llevado con distintos grados de refinamiento dependiendo de la información de riesgos y datos disponibles. Dependiendo de las circunstancias, el análisis puede ser:

- cualitativo;
- semi-cuantitativo;
- cuantitativo;
- una combinación de estos.

El orden de complejidad y costos de estos análisis en orden ascendente, es cualitativo, semi-cuantitativo y cuantitativo. En la práctica, a menudo se utiliza primero el análisis cualitativo para obtener una indicación general del nivel de riesgo.

Luego puede ser necesario llevar a cabo un análisis cuantitativo más específico. El detalle de los tipos de análisis es el siguiente:

a) **Análisis cualitativo**: utiliza formatos de palabras o escalas descriptivas para describir la magnitud de las consecuencias potenciales y la probabilidad de que esas consecuencias ocurran. Estas escalas se pueden modificar o ajustar para adaptarlas a las circunstancias, y se pueden utilizar distintas descripciones para riesgos diferentes.

   El análisis cualitativo se utiliza:

   i. como una actividad inicial de tamiz, para identificar los riesgos que requieren un análisis más detallado;

   ii. cuando el nivel de riesgo no justifica el tiempo y esfuerzo requerido para un análisis más completo;

   iii. cuando los datos numéricos son inadecuados para un análisis cuantitativo.

b) **Análisis semi-cuantitativo**: En el análisis semi-cuantitativo, a las escalas cualitativas, se les asignan valores. El número asignado a cada descripción no tiene que guardar una relación precisa con la magnitud real de las consecuencias o probabilidades. Los números pueden ser combinados en cualquier rango de fórmula dado que el sistema utilizado para priorizar confronta el sistema seleccionado para asignar números y combinarlos. El objetivo es producir un ordenamiento de prioridades más detallado que el que se logra normalmente en el análisis cualitativo, y no sugerir valores realistas para los riesgos tales como los que se procuran en el análisis cuantitativo.

   Se debe tener cuidado con el uso del análisis semi-cuantitativo porque los números seleccionados podrían no reflejar apropiadamente las relatividades, lo que podría conducir a resultados inconsistentes. El análisis semi-cuantitativo puede no diferenciar apropiadamente entre

distintos riesgos, particularmente cuando las consecuencias o las probabilidades son extremas.

A veces es apropiado considerar la probabilidad compuesta de dos elementos, a los que se refiere generalmente como frecuencia de la exposición y probabilidad.

Frecuencia de la exposición es la extensión a la cual una fuente de riesgo existe, y probabilidad es la chance de que, cuando existe esa fuente de riesgo, le seguirán las consecuencias. Deberá ejercerse precaución en las situaciones en que las relaciones entre los dos elementos no es completamente independiente.

c) **Análisis cuantitativo** El análisis cuantitativo utiliza valores numéricos para las consecuencias y probabilidades (en lugar de las escalas descriptivas utilizadas en los análisis cualitativos y semicuantitativos) utilizando datos de distintas fuentes.

La calidad del análisis depende de la precisión e integridad de los valores numéricos utilizados. Las consecuencias pueden ser estimadas modelando los resultados de un evento o conjunto de eventos, o extrapolando a partir de estudios experimentales o datos del pasado. Las consecuencias pueden ser expresadas en términos de criterios monetarios, técnicos o humanos.

En algunos casos se requiere más de un valor numérico para especificar las consecuencias para distintos momentos, lugares, grupos o situaciones. La probabilidad es expresada generalmente como una probabilidad, una frecuencia, o una combinación de exposición y probabilidad. La forma en que se expresan las probabilidades y las consecuencias y las formas en que las mismas son combinadas para proveer un nivel de riesgo variarán de acuerdo con el tipo de riesgo y el contexto en el cual se va a utilizar el nivel de riesgo.

2.2.2.4 Evaluación de riesgos

La evaluación de riesgos involucra comparar el nivel de riesgo detectado durante el proceso de análisis con criterios de riesgo establecidos previamente.

El análisis de riesgo y los criterios contra los cuales se comparan los riesgos en la evaluación de riesgos deberían considerarse sobre la misma base. En consecuencia, la evaluación cualitativa involucra la comparación de un nivel cualitativo de riesgo contra criterios cualitativos, y la evaluación cuantitativa involucra la comparación de un nivel numérico de riesgo contra criterios que pueden ser expresados como un número específico, tal como, un valor de fatalidad, frecuencia o monetario.

El producto de una evaluación de riesgo es una lista de riesgos con prioridades para una acción posterior. Deberían considerarse los objetivos de la organización y el grado de oportunidad que podrían resultar de tomar el riesgo. Las decisiones deben tener en cuenta el amplio contexto del riesgo e incluir consideración de la tolerabilidad de los riesgos sostenidos por las partes fuera de la organización que se benefician de ellos.

Si los riesgos resultantes caen dentro de las categorías de riesgos bajos o aceptables, pueden ser aceptados con un tratamiento futuro mínimo. Los riesgos bajos y aceptados deberían ser monitoreados y revisados periódicamente para asegurar que se mantienen aceptables. Si los riesgos no caen dentro de la categoría de riesgos bajos o aceptables, deberían ser tratados.

2.2.2.5 Tratamiento de los riesgos

El tratamiento de los riesgos involucra identificar el rango de opciones para tratar los riesgos, evaluar esas opciones, preparar planes para tratamiento de los riesgos e implementarlos.

Identificar opciones para tratamiento de los riesgos

a) Evitar el riesgo decidiendo no proceder con la actividad que probablemente generaría el riesgo (cuando esto es practicable). Evitar riesgos puede ocurrir inadecuadamente por una actitud de aversión al riesgo, que es una tendencia en mucha gente (a menudo influenciada por el sistema interno de una organización). Evitar inadecuadamente algunos riesgos puede aumentar la significación de otros. La aversión a riesgos tiene como resultado:

i) decisiones de evitar o ignorar riesgos independientemente de la información disponible y de los costos incurridos en el tratamiento de esos riesgos.

ii) fallas en tratar los riesgos;

iii) dejar las opciones críticas y/o decisiones en otras partes;

iv) diferir las decisiones que la organización no puede evitar;

v) seleccionar una opción porque representa un riesgo potencial más bajo independientemente de los beneficios.

b) Reducir la probabilidad de la ocurrencia;

c) Reducir las consecuencias;

d) Transferir los riesgos Esto involucra que otra parte soporte o comparta parte del riesgo. Los mecanismos incluyen el uso de contratos, arreglos de seguros y estructuras organizacionales tales como sociedades y "joint ventures". La transferencia de un riesgo a otras partes, o la transferencia física a otros lugares, reducirán el riesgo para la organización original, pero puede no disminuir el nivel general del riesgo para la sociedad. Cuando los riesgos son total o parcialmente transferidos, la organización que transfiere los riesgos ha adquirido un nuevo riesgo, que la organización a la cual ha transferido el riesgo no pueda administrarlo efectivamente.

e) Retener los riesgos Luego de que los riesgos hayan sido reducidos o transferidos, podría haber riesgos residuales que sean retenidos. Deberían ponerse en práctica planes para administrar las consecuencias de esos riesgos si los mismos ocurrieran, incluyendo identificar medios de financiar dichos riesgos. Los riesgos también pueden ser retenidos en forma predeterminada.

Según la [ISO 27000], el riesgo nunca es totalmente eliminable -ni sería rentable hacerlo-, por lo que es necesario definir una estrategia de aceptación de riesgo estableciendo criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable. Lo primordial de la metodología es que los resultados obtenidos sean comparables y repetibles para evitar grados de subjetividad que falseen la valoración de los riesgos. Existen numerosas metodologías estandarizadas para la evaluación de riesgos y la organización puede optar por una de ellas, aplicar una combinación de varias o crear la suya propia. ISO 27001:2005 no impone ninguna para que cada organización pueda aplicar la que estime más oportuno y funcional según el esfuerzo de análisis y recursos que pueda aplicar.

Identificar los riesgos:

- identificar todos aquellos activos de información que tienen algún valor para la organización que están dentro del alcance del SGSI y a sus responsables directos, denominados propietarios;
- identificar las amenazas relevantes asociadas a los activos identificados;
- identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas;
- identificar el impacto que podría suponer una pérdida de confidencialidad, integridad y disponibilidad para cada activo.

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;

- estimar los niveles de riesgo;
- determinar, según los criterios de aceptación de riesgo previamente establecidos, si el riesgo es aceptable o necesita ser tratado.

Identificar y evaluar las distintas opciones de <u>tratamiento de los riesgos</u> para:

- aplicar controles adecuados (mitigación);
- aceptar el riesgo (de forma consciente), siempre y cuando se siga cumpliendo con las políticas y criterios establecidos para la aceptación de los riesgos;
- evitar el riesgo;
- transferir el riesgo total o parcialmente a terceros.

La gestión de riesgos (ver figura 2.5) debe ser llevada a cabo con mucha responsabilidad.

FUENTE: ISO 27000. Figura 2.5. Gestión de riesgos

A la reducción de las consecuencias y probabilidades se las puede referir como control de riesgos. El control de riesgos involucra determinar el beneficio

relativo de nuevos controles a la luz de la efectividad de los controles existentes. Los controles pueden involucrar políticas de efectividad, procedimientos o cambios físicos.

Asimismo, sin lugar a dudas podemos señalar que, la seguridad de la información es parte de la gestión global del riesgo en una empresa (ver figura 2.6), hay aspectos que se superponen con la ciberseguridad, con la gestión de la continuidad del negocio y con la tecnología de la información:

FUENTE: ISO 27001. Figura 2.6. Gestión de riesgos

2.3. Modelo ISO 17799

Es un estándar para la administración de la seguridad de la información, e implica la implementación de toda una estructura documental que debe contar con un fuerte apoyo de la alta dirección de cualquier organización. Este estándar fue publicado por la International Organization for Standardization (ISO) en diciembre de 2000 con el objeto de desarrollar un marco de seguridad sobre el cual trabajen las organizaciones. Esta norma internacional ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización.

En la actualidad cualquier organización debe reconocer que el buen funcionamiento de los sistemas de información es crítico en el desarrollo de sus actividades y, al mismo tiempo, que dichos sistemas se encuentran en situación de riesgo tanto por la propia vulnerabilidad de los sistemas como por una insuficiente implantación de políticas y normas de seguridad. Estas vulnerabilidades pueden producir perdidas de activos de la organización o perdida de la continuidad del negocio cuyo alcance hay que conocer para poder decidir el nivel de riesgo que se está dispuesto a asumir. En esta situación se aborda la elaboración de un Plan de Seguridad para la organización con el objetivo de conocer el nivel de seguridad que presentan los sistemas informáticos, definir y diseñar el modelo de seguridad que se desea conseguir y planificar las acciones necesarias para ajustarse a ese modelo. Para responder a estas necesidades se plantea como hilo conductor la norma ISO/UNE/IEC 17799 de buenas prácticas en la gestión de la seguridad.

2.3.1. ISO/UNE/IEC 17799

Tiene su origen en la Británica BS7799 y más concretamente en su revisión del año 1999, adoptándose como ISO/IEC 17799 en el 2000. En el 2004 se publica una nueva revisión BS7799-2 que se utiliza para establecer la norma UNE 71502, más enfocada a la auditoria de seguridad. La ISO/IEC 17799 es un reconocido estándar internacional usado como base común para desarrollar normas de seguridad dentro de las organizaciones. La norma define la seguridad como la preservación de la confidencialidad, integridad y disponibilidad de la información, siendo necesario para ello no solo medidas técnicas sino también políticas y organizativas. Para alcanzarla define diez áreas de control [Mora, 2006]:

1. **Políticas de seguridad:** El objetivo principal es la elaboración de un documento de políticas de seguridad publicado por el máximo nivel directivo de la organización con una declaración apoyando sus objetivos y principios. En este documento se describirán brevemente las políticas, principios y normas que en materia de seguridad se consideren esenciales y se establecerá

la jerarquía de responsabilidades en la gestión de la seguridad indicando claramente quien se hace responsable de los activos. Incluirá referencias a la legislación aplicable y a los documentos de detalle donde se encuentran desarrolladas las normas. Se debe asegurar que se comunica esta política a todos los usuarios del sistema y que es fácilmente comprensible por todos ellos ya que es el medio de dar a conocer la implicación de la Dirección en las políticas de seguridad además de su contenido;

2. **Organización de la seguridad**: Se trata de desarrollar el documento gerencial de políticas de seguridad desde tres puntos de vista distintos: cuando los sistemas son gestionados por la propia organización, cuando existen accesos de terceras partes (asistencia técnica, por ejemplo) y cuando todos los sistemas de información están externalizados;

3. **Clasificación y control de activos:** Para mantener una adecuada protección de los activos hay que identificar claramente cuales son y asignarles un grado de protección según su sensibilidad y criticidad, indicando en cada caso como ha de ser tratado y protegido. Lo primero será contar con un exhaustivo inventario de activos que incluirá los recursos de información de todo tipo, recursos software y hardware, servicios informáticos y de comunicaciones y aquellos otros recursos que nos afecten como climatización, suministro eléctrico, etc. Una vez realizado se le asignará a cada recurso un grado de protección que marcara las medidas de seguridad que le serán aplicables y el tiempo durante el cual estarán vigentes siendo responsable de esta asignación el dueño o responsable del activo. Por último es conveniente manejar esta información de una manera organizada incluyendo algún tipo de clasificación sistemática que ayude a su mantenimiento y control;

4. **Seguridad del personal**: En cuanto al personal la seguridad se basará en tres pilares básicos, la seguridad inherente al puesto desempeñado, la formación en materia de seguridad y la respuesta ante incidentes.

La seguridad del puesto deberá enfocarse a evitar que personal malintencionado utilice los medios de la organización para provocar fallos de

seguridad y se evitan con una adecuada política de selección de personal, tanto propio como contratado temporalmente, e incluyendo condiciones y términos en los contratos que indiquen claramente las responsabilidades y las obligaciones. El trabajo de todo el personal debe ser periódicamente revisado y nuevamente aprobado por un superior jerárquico.

La formación en materia de seguridad implica que ningún usuario desconozca la política general de seguridad ni las normas específicas que le afectan en el desarrollo de sus funciones. Para ello se promoverán cursos de formación y actualizaciones periódicas de los conocimientos, así como todas aquellas medidas de difusión que se consideren oportunas. Es esencial para minimizar el número de incidentes de seguridad y su alcance establecer un sistema de comunicación de incidencias hardware, software o de cualquier tipo, que todos los usuarios puedan utilizar y que sirva para reaccionar con rapidez ante cualquier amenaza o para evitarla antes de que se produzca. También habrá que disponer de un procedimiento establecido de respuesta a incidentes que establezca las acciones a realizar ante un aviso de incidente. Este sistema servirá también para actualizar las políticas de seguridad de la organización teniendo en cuenta los incidentes más habituales o graves. Por último se habrá de establecer y difundir las sanciones disciplinarias cuando sean los propios empleados los que provoquen los incidentes;

5. **Seguridad física y del entorno**: Un primer objetivo será impedir el acceso a las áreas seguras de personal no autorizado. Estas zonas habrán de estar claramente delimitadas pero no de forma claramente visible sino de una manera formal, con un perímetro permanentemente controlado. Se pueden definir varios tipos de zonas seguras dependiendo del tipo de sistema informático que contengan y de su grado de criticidad y, por lo tanto, las medidas de seguridad en cada tipo serán acordes a dicho grado. Las medidas para evitar accesos no autorizados y daños en los sistemas suelen ser barreras físicas y de control de cualquier tipo, pero también la ausencia de información sobre lo que contiene un área segura y la falta de signos externos que puedan

hacer adivinar su contenido. Deberá tenerse en cuenta cuando se diseñe el sistema de información que la ubicación e infraestructuras del mismo sean las adecuadas para reducir el riesgo de amenazas naturales como incendios, vibraciones, inundaciones, etc.

También se pondrán medios para atajar aquellas no directamente relacionadas con el sistema de información pero que pueden afectar a su funcionamiento como pueden ser el suministro de energía incorporando un sistema de alimentación ininterrumpida de capacidad suficiente, proteger contra cortes o intrusiones el cableado de suministro de datos y energía, facilitar un adecuado mantenimiento de los equipos y establecer unas normas de seguridad para el equipamiento que contenga datos sensibles y que salga fuera de la organización y nunca permitir su salida sin autorización. Se debe asegurar que los soportes susceptibles de contener información sensible son físicamente destruidos o sobrescritos antes de desecharlos. Es conveniente establecer políticas de escritorios sin papeles para evitar el robo o destrucción de datos y de pantallas limpias, no dejando en la misma ningún dato sensible al dejar el puesto sin atención;

6. **Gestión de comunicaciones y operaciones**: Los procedimientos operativos, cualquiera que sea su tipo, deben estar perfectamente documentados por su política de seguridad, detallándose para cada tarea sus requerimientos de programación, interdependencias con otros sistemas, tareas de mantenimiento previstas y procedimientos de recuperación ante incidentes. Asimismo se ha de dar especial importancia a los cambios en los sistemas o instalaciones ya que son fuente frecuente de fallos del sistema y de seguridad.

Se debe establecer una serie de procedimientos de manejo de los incidentes para responder lo más rápida y eficazmente posible, estableciéndose como mínimo procedimientos para todos los tipos de incidentes probables, tratando de identificar las causas, indicando el modo de auditado del sistema afectado e incluyendo protocolos detallados de las acciones de recuperación.

Para reducir el riesgo de mal uso del sistema se deben separar las tareas de gestión de las de ejecución impidiendo que haga una misma persona todo el proceso. También se separaran las áreas de desarrollo de la de producción para evitar errores por incorrecciones en los sistemas o fallos forzados.

Cuando el sistema de información se encuentra en una instalación externa los controles deben ser los mismos pero deben encontrarse claramente especificados en el contrato.

Una adecuada monitorización del uso de los recursos del sistema nos permitirá detectar posibles cuellos de botella que derivarían en fallos del sistema y de seguridad, dando tiempo a planificar las ampliaciones o actualizaciones del sistema con la suficiente antelación. Estas ampliaciones se realizarán cuando estén perfectamente asegurado el correcto funcionamiento en el sistema existente y su adecuación a las normas de seguridad.

En cuanto a elementos software es esencial controlar la introducción de software malicioso que pudiera degradar los sistemas o introducir vulnerabilidades, para lo cual se implementarán los controles necesarios para evitar su instalación y se promoverán medidas para concienciar a los usuarios del riesgo que suponen y para formarles en un uso seguro del sistema.

Existirá un programa de copias de respaldo para todos los datos no recuperables de la organización, que se guardarán en una ubicación independiente con los mismos niveles de seguridad que en su emplazamiento original y por un periodo de tiempo que dependerá de la naturaleza y sensibilidad de los datos. Se realizarán ensayos de recuperación para comprobar la viabilidad del protocolo y validez del programa.

Se mantendrá un registro de actividades del personal de operación así como de los errores del sistema detectados, revisándolos para verificar la resolución de los fallos y que las medidas que se tomaron para ello estaban dentro de las normas.

La administración de las redes de datos deben incluir los controles necesarios para garantizar la seguridad de los datos y la protección de los servicios contra el acceso no autorizado. Se tomarán medidas adicionales, principalmente cifrado, cuando los datos sean especialmente sensibles.

Cualquier medio susceptible de almacenar datos ha de ser tenido en cuenta dentro de las políticas de seguridad y especialmente los soportes removibles como discos o papel, estableciéndose procedimientos operativos para protegerlos contra robo, daño o acceso no autorizado y procedimientos para su destrucción o borrado total cuando no vayan a ser utilizados de nuevo. La documentación del sistema debe ser también protegida ya que suele contener información valiosa y que puede ser utilizada para vulnerar el sistema.

Un apartado especial tienen los intercambios que se realizan entre distintas organizaciones que debido a la variedad de formatos implicados (correo electrónico, comercio electrónico, mensajero, fax, teléfono, etc.) exigen un control cuidadoso. Se establecerán acuerdos (preferiblemente escritos) con las otras organizaciones que respeten por una parte la política de seguridad de la organización y por otra la legislación aplicable, solo se utilizarán medios de transmisión que sean seguros y se establecerán normas para que el propio envío (datos, paquetes, etc.) incluya todas las medidas de seguridad consideradas adecuadas a su naturaleza. Respecto al correo electrónico se elaborará una política clara para todos los usuarios respecto al uso de anexos y almacenamiento de los mismos, el uso responsable de tal manera que no se comprometa a la organización y técnicas de cifrado para proteger la confidencialidad y la integridad. En definitiva se promoverá entre el personal de la organización una actitud activa por la seguridad formando sobre actos cotidianos que la comprometen y que son fáciles de evitar como intentar no ser escuchado al hablar por teléfono, no usar contestadores o el envío de fax con información sensible a números equivocados;

7. **Control de accesos**: Se deben definir y documentar las reglas y derechos de acceso a los recursos del sistema de información para cada usuario o grupo de usuarios en una declaración de política de accesos. Está política debe ser coherente con la clasificación de los activos y recorrer exhaustivamente el inventario de recursos. Por otra parte las reglas que se definan deberán ser preferiblemente restrictivas (no permitir el acceso nunca excepto cuando se necesite mejor que permitirlo siempre excepto cuando exista riesgo) y modificables solo por el administrador.

Se implementará un procedimiento formal que cubra todo el ciclo de vida del registro de un usuario, desde su alta donde se verificará que los accesos otorgados sean los adecuados a las necesidades y que exista un permiso de uso de los recursos accedidos, la cancelación inmediata de permisos ante cambios en las tareas del usuario, verificaciones periódicas de consistencia de los permisos y usuarios del sistema o utilización de identificadores únicos.

Es importante limitar todo lo posible la asignación de privilegios que permitan evitar los controles de acceso estándar ya que son la principal vulnerabilidad de un sistema, por lo que deberán estar perfectamente identificados, asignarse sobre la base de la necesidad de uso y evento por evento y a un identificador de usuario distinto al de uso habitual. Los derechos de acceso serán revisados a intervalos regulares y tras cada cambio en un usuario y los privilegios con una mayor frecuencia.

La asignación de contraseñas se controlará a través de un procedimiento formal que impida su almacenamiento o envió sin la debida protección y que incluya reglas para impedir su captura o adivinación. En entornos especialmente sensibles se proveerán sistemas de identificación más fuertes como huellas, candados hardware u otros. Por otra parte se informará a los usuarios de buenas prácticas en el uso de contraseñas como no compartirlas ni tenerlas escritas o cambiarlas regularmente y usar contraseñas de calidad. Es

conveniente bloquear por contraseña las sesiones de terminal o PC cuando el usuario se ausente del puesto.

Es esencial para la organización la protección de los servicios de red para impedir que sean interrumpidos o accedidos ilegalmente. Las normas para su protección, que han de ser coherentes con la política de control de accesos, se plasmarán en un documento de política de uso de los servicios de red. Todo usuario externo o nodo automático que intente acceder al sistema ha de ser autentificado preferiblemente con técnicas fuertes como el cifrado o candados hardware. Es recomendable la definición de caminos forzados entre terminales de usuario y los servicios del sistema así como la división de la red en subredes lógicas y aisladas. Todos los accesos a la red deben ser validados contra las reglas de control de accesos e incluir un control de origen y destino de la conexión, independientemente de las validaciones de seguridad que cada servicio del sistema incluya.

Es importante vigilar el acceso al sistema operativo ya que su control supone el dominio de una parte importante del sistema, por lo que se usarán todas las medidas de seguridad que incluya destacando la identificación y verificación segura de los usuarios, aplicaciones y terminales y el registro de los intentos de conexión al sistema. Se dispondrá de un sólido sistema de administración de contraseñas y se establecerán reglas sobre limitación del horario de uso y desconexión automática por inactividad.

El acceso a las aplicaciones estará limitado a los usuarios autorizados basándose en las normas de control de accesos y estará claramente documentado para cada aplicación su nivel de sensibilidad, aplicando las medidas de seguridad indicadas a dicho nivel.

Es esencial para preservar la seguridad del sistema la monitorización y seguimiento de todas las incidencias que se produzcan lo que permitirá la detección temprana de incidentes y la validación de la bondad de los controles

de seguridad adoptados. Se guardará un registro de los eventos de seguridad como accesos con o sin éxito a aplicaciones o a datos, usuarios que han accedido y por cuanto tiempo, alarmas del sistema y otros que se consideren necesarios para la recolección de evidencias de incidentes. Regularmente este registro debe ser revisado en busca de evidencias que indiquen algún compromiso de la seguridad.

Cuando en el sistema exista la posibilidad de teletrabajo o de computación móvil será necesario estudiar la sensibilidad de los sistemas desplazados e implementar las medidas de seguridad acordes con la misma y, al mismo tiempo, se dictarán normas específicas para este tipo de sistemas como por ejemplo sobre la seguridad física de los equipos contra robo o rotura o sobre el uso en público de los mismos;

8. **Desarrollo y mantenimiento de sistemas**: Se trata de asegurar que todos los requerimientos de seguridad que se han definido son incluidos en el sistema de información ya que es en el momento del desarrollo de los sistemas cuando más económico es implementarlos.

Las aplicaciones se deben diseñar para que incluyan los controles de acceso necesarios así como para que dejen registro de actividad. Se validarán los datos de entrada y de salida y se verificara la integridad y autenticidad de los mismos según se considere necesario.

Se utilizarán técnicas de cifrado para preservar la confidencialidad, autenticidad e integridad de la información que, tras una evaluación de los riesgos, sea considerada como especialmente sensible. Esta política en materia de cifrado tendrá en cuenta la legislación aplicable así como los estándares técnicos y las necesidades de la organización. También incorporará los casos y condiciones de uso de la firma digital o de servicio de no repudio. Es esencial la gestión de las claves de cifrado por lo que se establecerán normas y procedimientos para su administración, tanto en el caso de técnicas de clave secreta como de clave pública.

En el entorno de producción se controlará el acceso al software de sistema así como a los datos de prueba que se haya podido utilizar y a las bibliotecas de código fuente ya que contienen información interna sensible sobre el funcionamiento del sistema. En el entorno de mantenimiento se verificará que todos los cambios que se realicen en las aplicaciones están autorizados y existirá un procedimiento para llevarlos a cabo, al igual que las revisiones técnicas del sistema operativo o los cambios en los paquetes comerciales de software; todos los cambios han de quedar perfectamente documentados y tener una verificación previa de conformidad con las normas de seguridad;

9. **Gestión de la continuidad**: Toda organización ha de contar con un plan de actuación ante contingencias que permita identificar y reducir los riesgos de que se produzcan interrupciones en el servicio, atenuar en lo posible las consecuencias de los incidentes y asegurar que se reanuda la actividad lo antes posible.

La implementación de un proceso controlado para el mantenimiento de la actividad debe incluir una identificación clara de los eventos que pueden provocar su interrupción, evaluando el riesgo de ocurrencia y calculando el impacto que tendría sobre la organización, y esto para cada proceso de la organización. En base a esto se documentaran los procedimientos de actuación ante incidencias y se formará al personal que deba llevarlos a cabo, realizando las pruebas necesarias y actualizando los procedimientos cuando se produzcan cambios en el sistema o cuando las pruebas de reevaluación indiquen fallos. Estos planes contendrán como mínimo las causas de activación, el personal implicado y los procedimientos de actuación y de recuperación con sus diagramas de tiempos correspondientes, y debe tener un propietario o responsable del mismo. Asimismo se realizará el mantenimiento periódico del plan de continuidad para garantizar que es eficaz y que se encuentra vigente;

10. **Conformidad**: Se exigirá al sistema de información el total respeto a la legislación vigente. Dentro de los controles de la conformidad se incluirán la

conservación de aquellos ficheros o registros que determine el marco legal, el uso adecuado por parte del personal de los recursos de la organización y el uso que se hace de las técnicas de cifrado. Es conveniente mantener un registro de evidencias que, desde un punto de vista legal, pudiera ser utilizado en un tribunal, por lo que deberán cumplir todos los requisitos para su admisión como son la validez general a través del cumplimiento de estándares, la calidad con copias fieles y la totalidad de la prueba, conservando todo el registro de la acción. La política de seguridad de la información debe estar en permanente revisión para, por una parte, vigilar que se esté produciendo un adecuado cumplimiento de la misma por todas las áreas de la organización y por otra mediante el uso de una batería de verificaciones técnicas para comprobar que el sistema es seguro ante las incidencias que se puedan prever. Se proveerán herramientas de auditoria que deben estar separadas del resto de sistemas de información y cuyo uso estará limitado y controlado por un acuerdo donde se indique el alcance de las verificaciones y los procedimientos a llevar a cabo.

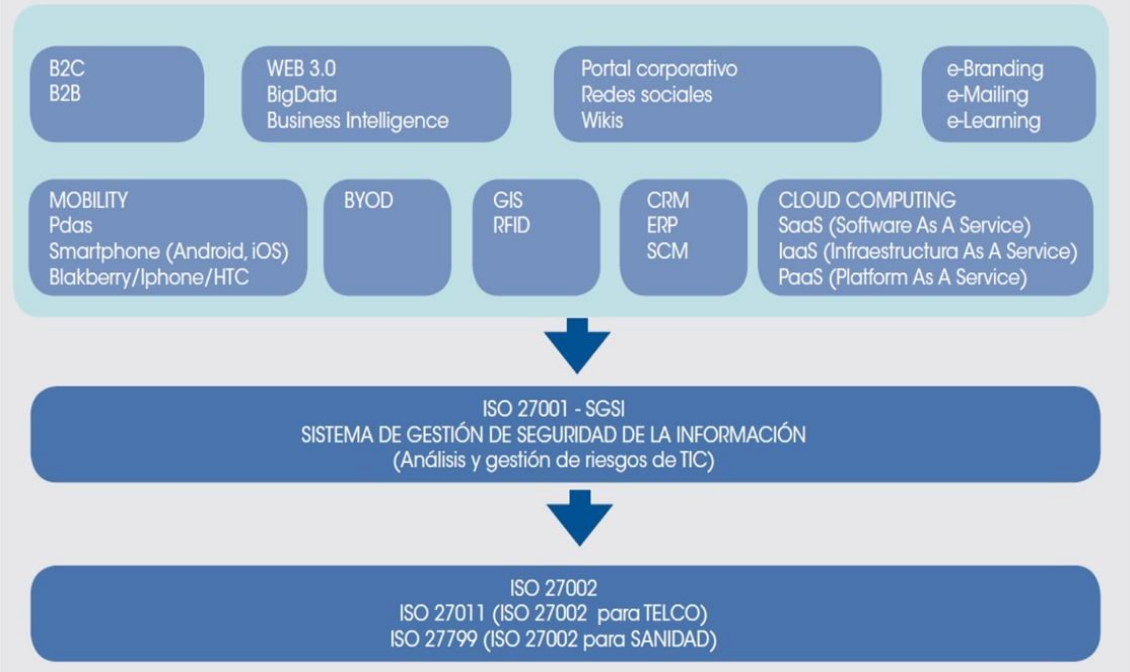
Estas áreas de control cubren todo el ámbito de gestión de la seguridad planteando sobre ellas 36 objetivos de control y un total de 127 controles que nos pueden servir para validar el grado de adecuación a la norma. En cualquier caso es importante darse cuenta que será una labor prioritaria adaptar la ISO17799, y más concretamente el peso que se da a cada una de las áreas de la norma, a las características concretas del ámbito de aplicación del Plan que se quiere elaborar.

2.4. Modelo ISO 27000

La información es como el aparato circulatorio para las organizaciones y requiere que se proteja ante cualquier amenaza que pueda poner en peligro las empresas tanto públicas como privadas, pues en otro caso podría dañarse la salud empresarial.

La realidad nos muestra que las organizaciones se enfrentan en la actualidad con un alto número de riesgos e inseguridades procedentes de una amplia variedad de

fuentes (ver figura 2.7), entre las que se encuentran los nuevos negocios y nuevas herramientas de las Tecnologías de la Información y la Comunicación (TIC), que los CEO (Directores Generales) y CIO (Directores de Informática) deberían aplicar.



FUENTE: AENOR. Figura 2.7 Nuevos negocios y herramientas TIC para CEO, CIO

Todas estas herramientas deben aplicarse según objetivos empresariales con la mayor seguridad, garantizando la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (garantizando que la información es fiable y exacta) y disponibilidad (asegurando que los usuarios autorizados tienen el acceso debido a la información).

La información, como uno de los principales activos de las organizaciones, debe protegerse a través de la implantación, mantenimiento y mejora de las medidas de seguridad para que cualquier empresa logre sus objetivos de negocio, garantice el cumplimiento legal, de prestigio y de imagen de la compañía. Por lo que se deben tomar las medidas preventivas, detectivas y/o correctivas de seguridad y protección de la información.

La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización.

Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

ISO/IEC 27000 es un conjunto de estándares desarrollados por ISO (International Organization for Standardization) 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.

ISO/IEC 27000: Publicada el 1 de Mayo de 2009, revisada con una segunda edición de 01 de Diciembre de 2012 y una tercera edición de 14 de Enero de 2014. Esta norma proporciona una visión general de las normas que componen la serie 27000, indicando para cada una de ellas su alcance de actuación y el propósito de su publicación.

Recoge todas las definiciones para la serie de normas 27000 y aporta las bases de por qué es importante la implantación de un SGSI, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora de un SGSI (la última edición no aborda ya el ciclo Plan-Do-Check-Act para evitar convertirlo en el único marco de referencia para la mejora continua).

ISO/IEC 27001: Publicada el 15 de Octubre de 2005, revisada el 25 de Septiembre de 2013. 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 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSIs de las organizaciones.

ISO/IEC 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.

ISO/IEC 27003: Publicada el 01 de Febrero de 2010. No certificable. Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001:2005. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI.

ISO/IEC 27004. Son métricas para la gestión de seguridad de la información.

ISO/IEC 27005. Trata la gestión de riesgos en seguridad de la información.

2.4.1. Sistemas de Gestión de Seguridad de la Información (SGSI)

La norma UNE-ISO/IEC 27001 está integrada por un "Sistema de Gestión de la Seguridad de la Información " y por un "Código de buenas prácticas de la gestión de la seguridad de la información", que establece las pautas a seguir para gestionar la seguridad de la información de forma adecuada y completa. La norma ISO 27001 surgió de la integración de la norma BS7799-2, "Specifications for Information Security Management Systems", y de la norma UNE-ISO/IEC 17799, "Código de buenas prácticas de la gestión de la seguridad de la información".

La idea fundamental que se persigue es la gestión de la seguridad de la información para conseguir unos niveles de seguridad mínimos, y para ello es imprescindible contar con un Sistema de Gestión de la Seguridad de la Información (SGSI), mediante un proceso sistemático, documentado y conocido por toda la

organización de forma similar a como se desarrollan los sistemas de gestión de la calidad basados en la norma ISO 9001/ISO 14001, etc.

La seguridad total no es posible al cien por cien, incluso en el caso de que se destinen recursos económicos y materiales, no se puede garantizar una seguridad total. La función que tiene un SGSI consiste en garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías, actualizándose constantemente y mejorando continuamente los sistemas y la gestión de la seguridad de la información

La norma/estándar UNE ISO/IEC 27001:2007 del "Sistema de Gestión de la Seguridad de la Información" es la solución de mejora continua más adecuada para evaluar los:

Riesgos físicos:

- Incendios;
- Inundaciones;
- Sabotajes;
- Vandalismos;
- accesos indebidos e indeseados.

Riesgos lógicos:

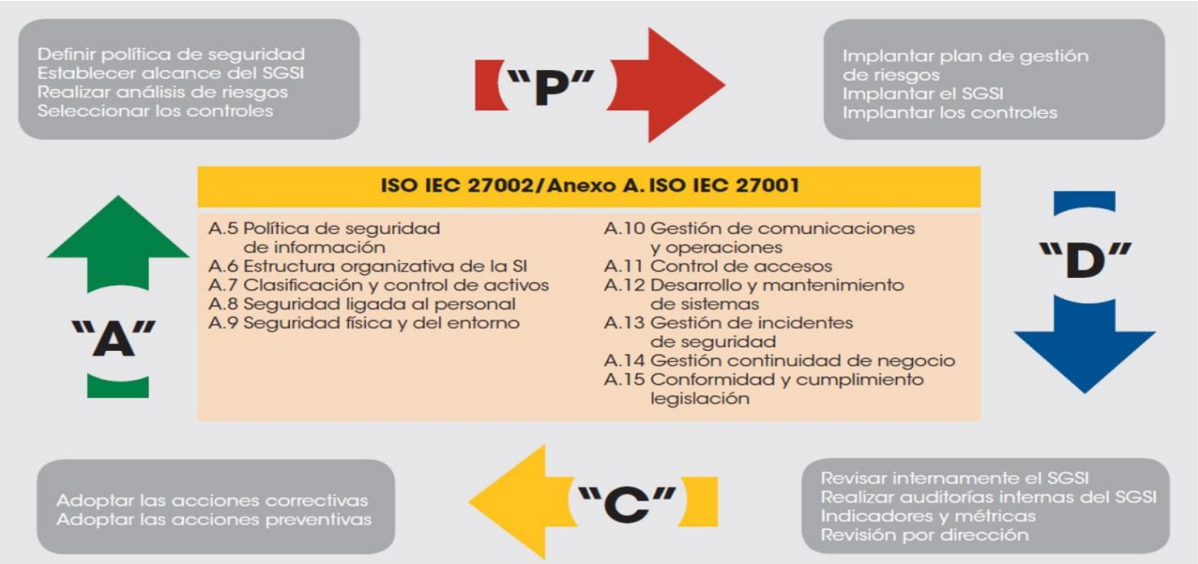
- Virus informáticos;
- ataques de intrusión o denegación de servicios

y establecer las estrategias y controles adecuados que aseguren una permanente protección y salvaguarda de la información.

2.4.1.1 Esquema general

El Sistema de Gestión de la Seguridad de la Información (SGSI) se fundamenta en la norma UNE-ISO/IEC 27001:2007, que sigue un enfoque basado en

procesos que utilizan el ciclo de mejora continua o de Deming, que consiste en Panificar-Hacer-Verificar-Actuar,más conocido con el acrónimo en inglés PDCA (Plan-DO-Check-Act) (similar a la más extendida y reconocida norma ISO 9001). Asimismo, tiene también su fundamento en la norma UNE–ISO/IEC 27002:2009, que recoge una lista de objetivos de control y controles necesarios para lograr los objetivos de seguridad de la información (ver figura 2.8).



FUENTE: AENOR. Figura 2.8. Mejora continúa

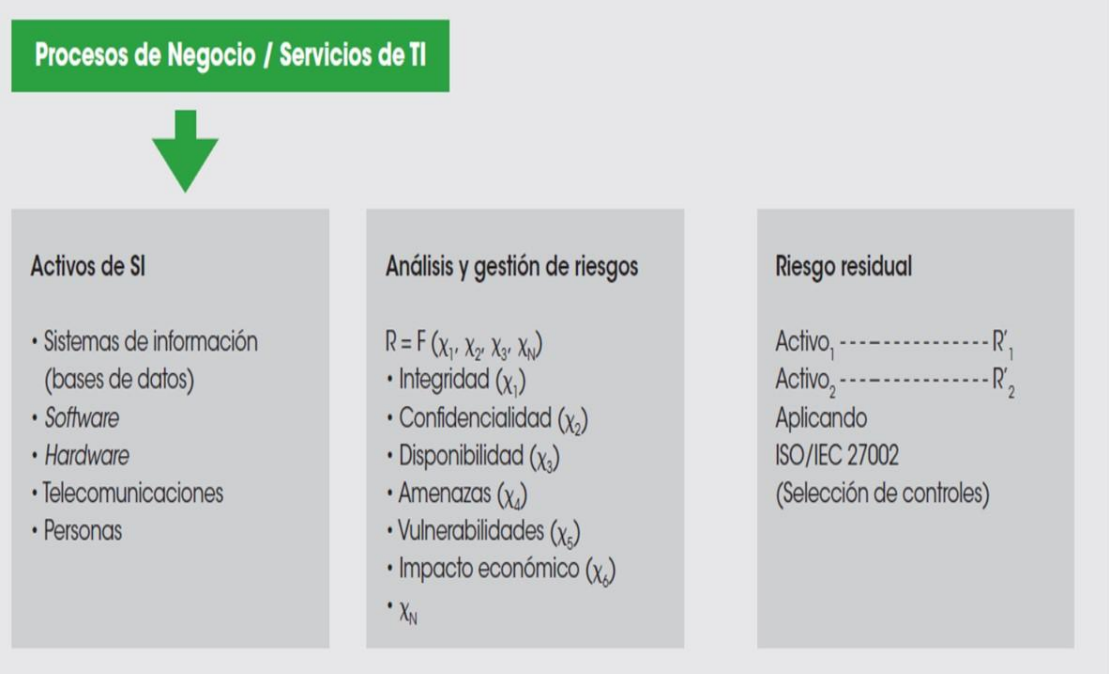
La piedra angular de este sistema SGSI-ISO 27001 es el análisis y gestión de los riesgos basados en los procesos de negocio/servicios de TI:

- CRM;
- ERP;
- *Business Inteligence;*
- Redes sociales;
- Movilidad;
- *Cloud computing;*
- Servicios externalizados;
- *Bring You Own;*

- *Device*, BYOD, etc.

El análisis y gestión de los riesgos basado en procesos de negocio/servicios de Tecnologías de Información es una herramienta muy útil para evaluar y controlar una organización con respecto a los riesgos de los sistemas de información. De esta forma los procesos de negocio/servicios de TI se fundamentan en los activos de las TIC que dan soporte a los procesos de negocio/servicios de TI.

Esto exige un análisis y gestión de los riesgos de sistemas de información realista y orientada a los objetivos de la organización. Una vez que se evalúa el riesgo y se aplican los controles adecuados de la UNE ISO/IEC 27002:2009 o de otros estándares nos queda un riesgo residual que la dirección de la empresa aprueba, y que se revisará al menos una vez al año (ver figura 2.9).



FUENTE: AENOR. Figura 2.9. Revisión del riesgo residual

Es de destacar que, como todo sistema de gestión, el SGSI-ISO 27001 tiene además del PDCA unos indicadores (objetivo de la métrica) y métricas para la medición de la eficacia y eficiencia de los controles, que aportan realismo día a día a la seguridad de los SI

El primer paso en el desarrollo de un SGSI, consiste en definir el alcance y los límites del SGSI, en términos del negocio, tipo de organización, su ubicación, sus activos, tecnología y justificación de cualquier exclusión aplicable al SGSI.

Asimismo, consiste en definir una política de seguridad que especifique el marco general, los objetivos generales que pretende alcanzar y el compromiso de la dirección con el SGSI.

Una vez definido el marco, se establecen las políticas específicas y una serie de procedimientos e instrucciones técnicas con el fin de desarrollar los conceptos aplicables al SGSI y utilizar los requisitos establecidos por la norma ISO 27001.

Una vez establecida la sistemática de trabajo, se deben generar los registros necesarios que sirvan como evidencia del funcionamiento del sistema. Estos registros van a ser el motor de la mayoría de los procesos de mejora, ya que si algo se ha hecho mal en los pasos anteriores o las acciones adoptadas no son suficientes, vamos a tener registros donde se pongan de manifiesto esas carencias y nos va a forzar a adoptar acciones correctivas con el fin de mejorar continuamente el sistema.

Etapas de la implantación de un SGSI

Las etapas que debe cumplir el desarrollo de un SGSI

Política de seguridad

La política de seguridad, básicamente, tiene que reflejar qué es lo que la organización quiere hacer con respecto a la seguridad de la información, los objetivos que se pretenden conseguir, contemplando los requisitos legales y reglamentarios aplicables y el compromiso de la dirección para conseguirlo.

Alcance del SGSI

Al igual que otros sistemas de gestión, el SGSI se aplica a un alcance determinado. Es necesario definir los servicios, procesos, actividades, departamentos, etc., a los que aplica el SGSI, con especial importancia a las oficinas o instalaciones a las que se aplica, el entorno tecnológico y las características del negocio. Se tiene que tener en cuenta, a la hora de definir el alcance de un SGSI, que se debe poder acreditar la confianza otorgada a terceros externos a la organización, es decir, a los clientes.

Análisis de riesgos

Es imprescindible definir una metodología de evaluación de los riesgos apropiada para el SGSI y los requerimientos del negocio, además de establecer los criterios de aceptación del riesgo y especificar los niveles de riesgo aceptables. Lo primordial de esta metodología es que los resultados obtenidos sean comparables y repetibles. El análisis de riesgos se entiende como un proceso global de estimación y evaluación del riesgo que nos va a permitir conocer los activos, su importancia para la organización y una valoración de los mismos para tener algo consistente en que basarnos a la hora de seleccionar los controles de seguridad que necesitamos.

Existen herramientas y metodologías para abordar un análisis de riesgos, pero la norma no especifica cuál debe aplicarse, tan solo que debe asegurarse que sean las adecuadas y permitir abordar un plan de gestión de riesgos y una selección de los controles necesarios.

Los diferentes hitos de un análisis de riesgos son:

- ✓ Identificar los riesgos:
  - identificar los activos que están dentro del alcance del SGSI y a sus responsables directos;
  - 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 identificados por la organización.

✓ 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;
- estimar los niveles de riesgo;
- determinar, según los criterios de aceptación de riesgo previamente establecidos, si el riesgo es aceptable o necesita ser tratado.

✓ 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, compañías aseguradoras o proveedores de outsourcing.

Plan de gestión de riesgos

Después de realizar el análisis de riesgo, la organización debe tomar decisiones sobre qué hacer con cada uno de ellos y plasmarlo en un plan de gestión de riesgos, teniendo en cuenta que de cada riesgo se derivan requisitos o necesidades de seguridad. Con cada riesgo identificado se pueden adoptar varias posturas:

1. Aceptarlo y no tomar ninguna acción al respecto.
2. Eliminar la causa, cambiando el nivel de disponibilidad o cancelando el contrato con el cliente.
3. Transferirlo, contratando un servicio externo, mediante la firma de un SLA (Service Level Agreement).
4. Reducirlo, implantando una serie de controles que garanticen los niveles mínimos de seguridad que se deben cumplir.

Selección de objetivos y controles

Una vez definido el plan de tratamiento de riesgos que identifica las acciones que vamos a implementar, se seleccionan los controles para cubrir los requisitos de seguridad. Los controles elegidos se seleccionan de la norma ISO 27001, aunque se pueden elegir otros controles que no se encuentran en esta norma y que complementen los controles seleccionados.

Con el fin de comprobar la eficacia de los controles seccionados y su implantación, se definen una serie de métricas que nos permiten comprobar la eficacia de los controles seleccionados.

Declaración de aplicabilidad e implantación

La selección de los controles aplicables se plasma en un documento que se denomina "Declaración de Aplicabilidad", donde se recoge para cada objetivo y cada control de la norma las razones de su selección o exclusión del SGSI con respecto a la organización, es muy importante plasmar cuales son los controles aplicables a la organización, teniendo en cuenta el tipo de negocio, organización, personal, infraestructuras, etc.

La norma tiene 133 controles de seguridad, algunos de ellos bastante selectivos, por lo que algunas organizaciones prefieren excluir del sistema varios controles y dejar un SGSI más sencillo de implantar, mantener y controlar, pero esas exclusiones deben estar perfectamente justificadas y argumentadas.

Se trata de un documento fundamental dentro del SGSI, y tendrá que estar disponible para los auditores que vayan a certificar el sistema, ya que es aquí donde van a comprobar qué controles se han implantado y las razones de su implantación, pero, sobre todo, cuáles no se han implantado y por qué.

Revisión y mejora continúa

El SGSI se debe de revisar regularmente 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, tener en cuenta que no se termina con la implantación del sistema y la certificación, sino que el sistema se debe de mejorar continuamente.

Cualquier sistema de gestión lleva consigo un proceso de revisión y mejora continua, puesto que entre otras cosas se espera de él que vaya aprendiendo de los errores y adoptando las medidas necesarias para que no se repitan los mismos problemas.

De ellos se derivan una serie de acciones correctivas y preventivas cuya finalidad es la de ir perfeccionando y mejorando el SGSI continuamente.

Todos los días tenemos riegos que atentan contra la seguridad de la información:

- ✓ Usuarios internos;
- ✓ Usuarios externos;
- ✓ Desastres naturales.

Para proteger datos e información en un entorno de Sistemas de Información, se puede implementar un Sistema de Seguridad de la Información (SGSI).

Un SGSI, permite:

- ✓ Conocer
- ✓ Gestionar

- ✓ Minimizar los riesgos que atentan contra la seguridad de la información

Asimismo, un SGSI, permite:

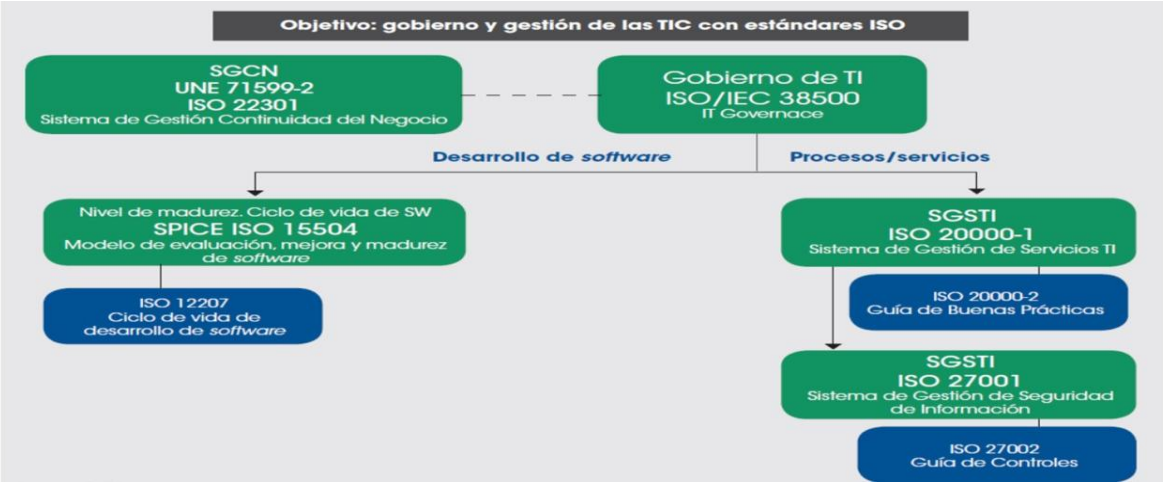
- ✓ Analizar y ordenar la estructura del Sistema de Información.
- ✓ Establecer los procedimientos de trabajo para mantener su seguridad.
- ✓ Disponer de controles para medir la eficacia de lo establecido en el punto anterior.

La idea es alcanzar un nivel de riesgo menor que el soportado por la institución, para preservar la confidencialidad, integridad y disponibilidad de la información.

2.4.1.2 Modelo de gobierno y gestión para las TIC

La norma ISO 27001 tiene relación con otras normas que conforman el modelo de gobierno y gestión de las TIC desarrollado por AENOR, basado en estándares aceptados mundialmente (ver figura 2.10). Se puede decir que, gracias a este modelo, el Centro de Proceso de Datos (CPD) y el resto de la organización comienzan hablar el mismo lenguaje y a interconectarse de manera más natural y eficiente.

Este modelo propone dos certificaciones a máximo nivel: una para el gobierno corporativo de las TIC (según la norma ISO 38500) y otra para el Sistema de Continuidad de Negocio (UNE 71599-2 e ISO 22301) en las empresas. Dentro de la primera divide a su vez la gestión en dos áreas: los Sistemas de Gestión de los Servicios de TI (UNE-ISO/IEC 20000-1) y los Sistemas de Gestión de la Seguridad de la Información (UNEISO/IEC 27001). Con la implantación de los sistemas se logra gestionar la calidad y seguridad de los servicios de Tecnologías de Información y Comunicación, lo que trae consigo la minimización de los
riesgos en la seguridad de la información y mejorar la seguridad de las TIC en el nivel del servicio de las mismas.



FUENTE: AENOR. Figura 2.10. Modelo de gobierno y gestión TIC

La otra área de gestión es donde se agrupan las actividades de desarrollo de programas *(software)*, dirigido a la calidad del proceso de ingeniería del *software*, con el modelo de evaluación, mejora y madurez del *software* (SPICE ISO 15504-ISO 12207).

Este modelo significa un cambio cultural que impacta en el mundo empresarial y de las Administraciones Públicas en su relación con las TIC, que ha supuesto el primer paso hacia la consolidación y optimización de las TIC en nuestro país.

Beneficios de implantación de un SGSI

Entre los beneficios de implantar la ISO 27001, se tiene:

- Estructura e inversiones adecuadas, costo correcto
- Control y clasificación de activos
- Dirección de operaciones y comunicaciones
- Política de Seguridad
- Evaluación de riesgos internos y a terceros
- Gestión de las personas: Seguridad del personal
- Desarrollo y mantenimiento de sistemas
- Dirección de Planes de Contingencia

• Cumplimiento con la legislación.

2.5. Normas de Auditoría de Tecnologías de la Información y Comunicación

Es el examen objetivo, crítico, metodológico y selectivo de evidencia relacionada con políticas, prácticas, procesos y procedimientos en materia de tecnologías de la información y la comunicación, para expresar una opinión independiente respecto:

a) A la confidencialidad, integridad, disponibilidad y confiabilidad de la información.
b) Al uso eficaz de los recursos tecnológicos.
c) A la eficacia del control interno asociado a los procesos de las Tecnologías de la Información y la Comunicación.

Los incisos señalados, podrán ser considerados en forma individual o en conjunto.

2.5.1. Enfoques de la Auditoría

La auditoría de tecnologías de la información y la comunicación está definida principalmente por sus objetivos y puede ser orientada hacia uno o varios de los siguientes enfoques:

a) Enfoque a las seguridades: Consiste en evaluar los controles de seguridad implementados en los sistemas de información con la finalidad de mantener la confidencialidad, integridad y disponibilidad de la información.

b) Enfoque a la información: Consiste en evaluar la estructura, integridad y confiabilidad de la información gestionada por el sistema de información.

c) Enfoque a la infraestructura tecnológica: Consiste en evaluar la correspondencia de los recursos tecnológicos en relación a los objetivos previstos.

d) Enfoque al software de aplicación: Consiste en evaluar la eficacia de los procesos y controles inmersos en el software de aplicación, que el diseño conceptual de éste cumpla con el ordenamiento jurídico administrativo vigente.

e) **Enfoque a las comunicaciones y redes:** Consiste en evaluar la confiabilidad y desempeño del sistema de comunicación para mantener la disponibilidad de la información.

Para una adecuada comprensión de las Normas de Auditoría de Tecnologías de la Información y la Comunicación, se deben considerar las siguientes definiciones:

Datos: Son objetos de información, los cuales pueden ser externos o internos, estructurados y no estructurados del tipo gráfico, sonido, imágenes, números, palabras y de otra índole, etc.

Información: Datos que han sido organizados, sistematizados y presentados de manera que los patrones subyacentes resulten claros.

Tecnología: Es un conjunto ordenado de instrumentos, conocimientos, procedimientos y métodos aplicados a las áreas.

Tecnologías de la Información y la Comunicación (TIC): Comprende al conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios, que permiten la compilación, procesamiento, almacenamiento, transmisión y recepción de información, voz, datos, texto, video e imágenes. Se consideran como sus componentes el hardware, el software y los servicios.

Sistema de Información (SI): Se refiere a un conjunto de procesos y recursos de información organizados con el objetivo de proveer la información necesaria (pasada, presente, futura) en forma precisa y oportuna para apoyar la toma de decisiones en una entidad.

Software de aplicación: Se refiere a un elemento de los Sistemas de Información, es un conjunto de programas de computador diseñados y escritos para realizar tareas específicas del negocio y que permiten la interacción entre el usuario y el computador.

Sistemas de comunicación: Se refiere a la tecnología que se emplea para el intercambio de información.

Confidencialidad de la información: Se refiere a la protección de la información crítica contra su divulgación no autorizada.

Integridad de la información: Se vincula con la exactitud y la totalidad de la información así como también con su validez de acuerdo con los valores y las expectativas de la entidad.

Confiabilidad de la información: Se vincula con la provisión oportuna e íntegra de la información para coadyuvar a la consecución de los objetivos de la entidad.

Disponibilidad de la información: Se vincula con el hecho de que la información se encuentre disponible cuando el proceso la requiera. También se asocia con la protección de los recursos necesarios y las capacidades asociadas.

Técnicas de Auditoría Asistidas por Computador (TAAC): Se refiere a las técnicas de auditoría que contemplan herramientas informáticas con el objetivo de realizar más eficazmente, eficientemente y en menor tiempo pruebas de auditoría.

2.6.1. Normas de Auditoría de Tic´s

271 Planificación

01. La primera norma de auditoría de tecnologías de la información y la comunicación es:

> **La auditoría de tecnologías de la información y la comunicación se debe planificar en forma metodológica, para alcanzar eficientemente los objetivos de la misma.**

02. La planificación debe permitir un adecuado desarrollo de las etapas subsecuentes; para el efecto, se debe tomar conocimiento del sujeto y del objeto a evaluar. Además, es un proceso continuo y dinámico que puede modificarse o ampliarse durante el desarrollo de la auditoría.

03. El auditor gubernamental debe comprender del objeto de auditoría: el diseño conceptual, políticas de gestión, formas de registro, niveles de seguridad y uso de las comunicaciones para la gestión de la información y el ordenamiento jurídico administrativo relacionado con el objeto de auditoría.

04. En función de la naturaleza, complejidad y modularidad del objeto de auditoría, la evaluación del control interno y la evaluación de riesgos, se determinarán las áreas críticas, dependiendo de éstas se definirán los objetivos o el(los) enfoque(s) y el alcance de la auditoría.

05. Se deben identificar los criterios a partir de la normatividad aplicable al objeto de auditoría. En el caso de que la normativa asociada al objeto de auditoría no permita identificar criterios de evaluación, éstos serán definidos por el auditor gubernamental y comunicados a la entidad. Todo criterio debe estar sustentado por evidencia suficiente y competente.

06. Se diseñarán programas de trabajo que se aplicarán durante la ejecución del trabajo de campo, para el efecto, en función a la evaluación del control interno y evaluación de riesgos, se determinará la naturaleza, oportunidad y extensión de los procedimientos de auditoría que se aplicarán para la obtención de evidencia competente y suficiente.

07. Como resultado del proceso de planificación de la auditoría de tecnologías de la información y la comunicación, se debe elaborar el Memorándum de Planificación de Auditoría, el cual debe contener todos los aspectos detallados en la presente norma y aquéllos que se consideren necesarios incluir, y que tengan relación con los objetivos del examen, el alcance y la metodología.

Las modificaciones que ameriten, deben ser expuestas en una adenda al Memorándum de Planificación de Auditoría, que refleje los aspectos ajustados, así como su justificación.

272 Supervisión

01. La segunda norma de auditoría de tecnologías de la información y la comunicación es:

> **Personal competente debe supervisar sistemática y oportunamente el trabajo realizado por los profesionales que conformen el equipo de auditoría.**

02. La supervisión implica dirigir los esfuerzos del equipo de auditores gubernamentales hacia la consecución de los objetivos de auditoría.

03. La supervisión debe ser realizada en cada una de las etapas de la auditoría, la misma incluye:

- Examinar la factibilidad y/o razonabilidad técnica de los objetivos y alcances de la auditoría propuestos.
- Asegurar que los miembros del equipo comprendan los objetivos de la auditoría. En particular se debe asegurar que entiendan claramente el trabajo a realizar, por qué se va efectuar y qué se espera lograr.
- Guiar a los miembros del equipo de auditoría a lo largo del desarrollo de las tareas asignadas.
- Revisar oportunamente el trabajo realizado, a través de los respectivos papeles de trabajo en medios físicos y/o electrónicos.
- Ayudar a absolver problemas técnicos y administrativos.
- Detectar debilidades del personal asignado y proporcionar en consecuencia la capacitación necesaria o requerir que la misma sea proporcionada por terceros.
- Asegurar que la evidencia obtenida sea suficiente y competente.

04. La supervisión efectuada durante el desarrollo de la auditoría, debe estar evidenciada en los papeles de trabajo en medios físicos y/o electrónicos, acumulados durante la misma.

273 Control interno

01. La tercera norma de auditoría de tecnologías de la información y la comunicación es:

> **Debe obtenerse una comprensión del control interno relacionado con el objeto del examen.**

02. Se debe evaluar el control interno para identificar las áreas críticas que requieren un examen profundo y determinar su grado de confiabilidad a fin de establecer la naturaleza, alcance y oportunidad de los procedimientos de auditoría a aplicar.

03. A efectos de este tipo de auditoría, se establecen dos tipos de controles: el control general y el control específico de los sistemas de información. El control general involucra a todos los sistemas de información y el control específico está diseñado para controlar el procesamiento en sí de la información.

04. Los controles generales son políticas y procedimientos que tienen que ver con el ambiente en el cual se desarrollan, mantienen y operan los sistemas de información y respaldan el funcionamiento efectivo de los controles específicos, en consecuencia involucran a todos los sistemas de información.

05. Los controles específicos son los aplicables a los procesos de adquisición, producción, almacenamiento, tratamiento, comunicación, registro y presentación de la información.

06. El control interno es un proceso implementado por la dirección y todo el personal, diseñado con el objetivo de coadyuvar al logro de los objetivos de la entidad. Comprende el plan de organización, incluyendo la Unidad de Auditoría Interna, todos los métodos coordinados y procedimientos adoptados en la entidad para promover la eficacia y la eficiencia de las operaciones y la confiabilidad de la información, así como el cumplimiento de las políticas gerenciales, el ordenamiento jurídico administrativo y otras normas legales aplicables, y las obligaciones contractuales.

07. El control interno está conformado por cinco componentes que interactúan entre sí y se encuentran integrados al proceso de gestión: ambiente de control, evaluación de riesgos, actividades de control, información y comunicación, y supervisión.

08. El estudio y evaluación del control interno incluye dos fases:

a) Conocimiento y comprensión de los procedimientos establecidos en la entidad referente a los sistemas de información, al término del cual, el auditor gubernamental debe ser capaz de emitir una opinión preliminar presumiendo un satisfactorio cumplimiento del control interno.
b) Comprobación de que los procedimientos relativos a los controles internos están siendo aplicados tal como fueron observados en la primera fase.

274 Evidencia

01. La cuarta norma de auditoría de tecnologías de la información y la comunicación es:

> **Debe obtenerse evidencia competente y suficiente como base razonable para sustentar los hallazgos y conclusiones del auditor gubernamental.**

02. Se denomina evidencia al conjunto de hechos comprobados, suficientes y competentes que sustentan las conclusiones del auditor. Es la información específica obtenida durante la labor de auditoría a través de observación, inspección, entrevistas y examen de los registros; y otros procedimientos que sean aplicables.

03. La acumulación de evidencia es un proceso integrado a toda la ejecución de la auditoría y debe sustentar todos los atributos de los hallazgos de auditoría (condición, criterio, causa y efecto).

04. La evidencia debe ser acumulada mediante un proceso supervisado de aplicación de metodologías y técnicas de auditoría.

05. La evidencia para ser competente, debe ser válida como relevante. La evidencia es válida cuando es consistente con la realidad y los hechos, la misma ha sido obtenida de fuente independiente, por el auditor en forma directa o se ha asegurado de la confiabilidad de la información generada por la entidad. La evidencia es relevante cuando tiene directa relación con el objeto de la auditoría y contribuye a sustentar los hallazgos y conclusiones del auditor gubernamental.

06. La evidencia es suficiente si basta para sustentar la opinión del auditor gubernamental, para ello debe ejercitar su juicio profesional con el propósito de determinar la cantidad y tipos de evidencia necesarias.

07. Las Técnicas de Auditoría Asistidas por Computador (TAAC) pueden producir parte de la evidencia de auditoría, como consecuencia de ello, el auditor debe planificar y ser competente en el uso de las TAAC.

08. La evidencia obtenida por el auditor gubernamental debe conservarse en papeles de trabajo en medios físicos y/o electrónicos.

09. Respecto a las características de competencia, suficiencia y clasificación de la evidencia, y a los papeles de trabajo que la contienen, deben considerarse los aspectos mencionados en los numerales 07 al 13 de la Norma de Auditoría Financiera 224.

275 Comunicación de resultados

01. La quinta norma de auditoría de tecnologías de la información y la comunicación es:

El informe de auditoría de tecnologías de la información y la comunicación debe ser oportuno, objetivo, claro, convincente, conciso y será el medio para comunicar los resultados obtenidos durante la misma.

02. El informe de auditoría de tecnologías de la información y la comunicación debe ser emitido en forma escrita, lógica y organizada.

03. El informe debe contener información suficiente para ser entendido por los destinatarios y facilitar la acción correctiva si corresponde.

04. El contenido del informe de auditoría de tecnologías de la información y la comunicación deberá hacer referencia a:

- Los antecedentes, acciones o circunstancias que dieron origen a la auditoría.
- Los objetivos, que identificarán los propósitos específicos que se cubrirán durante la misma.
- El objeto, identifica aquello que ha sido examinado.
- El alcance, se referirá al periodo examinado; así como a la cobertura del trabajo realizado.

Se debe especificar en el alcance, que la auditoría se realizó de acuerdo con las Normas de Auditoría Gubernamental.

- Si se presentaron limitaciones que no permitieron al auditor gubernamental cumplir con los objetivos previstos, éstas deben ser mencionadas en el informe de manera expresa.
- La metodología, explicará las técnicas y procedimientos de auditoría que fueron empleados para obtener y analizar la evidencia; asimismo, se mencionarán los criterios y normas aplicadas durante el desarrollo del examen.
- En el resultado del examen, se expondrá:
    - Los hallazgos significativos que tengan relación con los objetivos de auditoría, los que incluirán la información suficiente que permita una adecuada comprensión del asunto que se informa.

- Las recomendaciones que se consideren apropiadas para eliminar o minimizar las causas que originaron las deficiencias identificadas durante el examen.

- Las conclusiones, que son inferencias lógicas sobre el objetivo de auditorías basadas en los hallazgos, deben ser expresadas explícitamente de manera convincente y persuasiva, evitando el riesgo de interpretaciones erróneas por parte de los lectores.

05. Si correspondiera, se debe hacer referencia a las auditorías especiales que se hubieran iniciado por alguna situación evidenciada en la auditoría de tecnologías de la información y la comunicación, o a los informes de auditoría especial emergentes de la misma.

2.6. Auditoria

Conceptualmente la auditoria, toda y cualquier auditoria [Hernández 2000], "es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas".

El objeto hoy en día es Tecnología de la Información (TI), algunas áreas principales son:

- ✓ Bases de Datos;
- ✓ Software;
- ✓ Hardware;
- ✓ Redes de ordenadores;
- ✓ Seguridad;
- ✓ Agentes inteligentes;
- ✓ Redes neuronales;
- ✓ Ofimática;
- ✓ Inteligencia Artificial;
- ✓ Domótica.

La auditoría es la acumulación y evaluación objetiva de evidencia para establecer e informar sobre el grado de correspondencia entre la información examinada y criterios establecidos.

Sus principales características son:

- ✓ **Contenido,** una opinión.
- ✓ **Condición,** profesional.
- ✓ **Justificación,** sustentada en determinados procedimientos (la opinión profesional se fundamenta y justifica por medio de unos procedimientos específicos tendentes a proporcionar una seguridad razonable de lo que se afirma).
- ✓ **Objeto,** una determinada información obtenida en un cierto soporte.
- ✓ **Finalidad,** determinar si presenta adecuadamente la realidad o ésta responde a las expectativas que le son atribuidas, es decir, su fiabilidad.

Es un proceso que se realiza a posteriori, en relación con actividades ya realizadas, sobre las que hay que emitir una opinión. Por lo que urge, participar desde la concepción misma del proyecto de desarrollo de sistemas.

2.6.1. Clases de Auditoria

Las principales Clases de Auditoria [Sanchez 2000] son:

- Por el sujeto que la efectúa:
  - ✓ **Interna**, auditores que forman parte en la educación superior;
  - ✓ **Externa**, auditores ajenos a la organización;
- Por su contenido y fines:
  - ✓ **De Gestión,** afecta a la situación global de la comunidad educativa;
  - ✓ **Organizativa,** analiza la adecuación de la estructura organizativa;
  - ✓ **Operacional,** hasta qué punto se están cumpliendo los objetivos establecidos e identificación de los puntos que necesitan mejorar;

- ✓ **Financiera,** examen y verificación del estado financiero, acompañado de una opinión sobre su fiabilidad;
- ✓ **Contable,** adecuación de los criterios empleados para recoger los hechos mediante apuntes contables en los estados financieros;
- ✓ **Informática,** examen y verificación del correcto funcionamiento y control del sistema informático en la educación superior;
- ✓ **Económico-Social,** diagnóstico sobre el proceso económico y los resultados sociales obtenidos.

- Por su amplitud:

- ✓ **Total,** afecta a toda la comunidad de la educación superior;
- ✓ **Parcial,** se concentra en determinados elementos;
- Por su frecuencia:
- ✓ Permanente;
- ✓ Ocasional.

2.6.2. Definición de auditoría

La Auditoría representa el examen de los Estados Financieros de una entidad, con el objeto de que el Contador Público independiente emita opinión profesional respecto a si dichos estados presentan la situación financiera, los resultados de las operaciones, las variaciones en el capital contable y los flujos de efectivo de una empresa, de acuerdo a normativa vigente.

La auditoría tiene implicaciones relacionadas a la responsabilidad que el profesional asume, la cual toca los ámbitos ético, legal y moral.

2.6.3. Importancia de la auditoría

Los auditores en los negocios son muy importantes, por cuanto la gerencia sin la práctica de una auditoría no tiene plena seguridad de que los datos económicos registrados realmente son verdaderos y confiables. Es la Auditoría la que permite conocer con bastante razonabilidad la situación real de una empresa.

2. 6.4. El proceso de la auditoría informática

El proceso de la auditoría informática es similar al que se lleva a cabo a los de estados financieros, en el cual, los objetivos principales son: salvaguardar los activos, asegurar la integridad de los datos, la consecución de los objetivos gerenciales y, la utilización racional de los recursos, con eficiencia y eficacia, para lo que se realiza la recolección y evaluación de evidencias.

Para que una auditoría sea exitosa, debe tomar en cuenta básicamente 3 etapas:

a) Planificación de la auditoría Informática;

b) Ejecución de la auditoría Informática;

c) Finalización de la auditoría Informática.

a) Planificación de la auditoría Informática

En esta fase se establecen las relaciones entre auditores y colaboradores de la organización, para determinar el alcance y objetivos. Se hace un bosquejo de la situación de la entidad, acerca de su organización, sistema contable, controles internos, estrategias y demás elementos que le permitan al auditor elaborar el programa de auditoría que se llevará a efecto.
Elementos Principales de esta Fase:

1. Conocimiento y Comprensión de la Entidad;
2. Objetivos y Alcance de la auditoría;
3. Análisis Preliminar del Control Interno;
4. Análisis de los Riesgos;
5. Planeación Específica de la auditoría;
6. Elaboración de programas de Auditoría.

b) Ejecución de la auditoría Informática

La ejecución de la auditoría informática, constituye la recopilación de la mayor cantidad de información necesaria, como son documentos y evidencias

que permitan al auditor fundamentar sus comentarios, sugerencias y recomendaciones, con respecto al manejo y administración de TI.

Para la recolección de información, se pueden aplicar las siguientes técnicas:

- ✓ Entrevistas;
- ✓ Simulación;
- ✓ Cuestionarios;
- ✓ Análisis de la información documental entregada por el auditado;
- ✓ Revisión y Análisis de Estándares;
- ✓ Revisión y Análisis de la información de auditorías anteriores.

La evidencia se clasifica de la siguiente manera:

a) Evidencia documental.

b) Evidencia física.

c) Evidencia analítica.

d) Evidencia testimonial.

Una vez que tenemos información real y confiable, procedemos a evaluar y probar la manera en la que han sido diseñados los controles en la organización, para el mejoramiento continuo de la misma, para esto el equipo de Auditoría utilizara medios informáticos y electrónicos que permitan obtener resultados reales.

El equipo de auditores, para poder dar una opinión sobre un sistema o proceso informático, debe comprobar el funcionamiento de los sistemas de aplicación y efectuar una revisión completa de los equipos de cómputo

c) Finalización de la auditoría Informática

Para finalizar un proceso de Auditoría Informática, se debe presentar un informe que contenga conclusiones y recomendaciones, necesarias para que una empresa este en mejoramiento continuo, esta documentación debe ser

redactada por el equipo de Auditoría y entregarse a la Alta Dirección de la empresa para su evaluación y análisis.

CAPITULO III.

Marco Institucional

CAPITULO III. Marco Institucional

3.1. Antecedentes de la organización

INTRODUCCION

El Fondo Nacional de Desarrollo Regional (FNDR) institución comprometida con el proceso de cambio que desde el año 2006 el Gobierno ha venido encarando, se caracteriza por contar con un alto espíritu de conciencia social reflejado en colaboración con el pueblo y se constituye en parte del proceso de cambio del Estado Plurinacional de Bolivia. En este sentido, es una institución que ha sabido anticiparse al futuro, al mismo tiempo de plantear medidas propositivas para una correcta adecuación a las políticas de cambio del Gobierno Nacional. Para ello se han modificado las políticas de financiamiento principalmente con el Programa Recursos Propios FNDR "Vivir Bien", se ha incluido la participación del control social en el proceso de financiamiento, desarrollando herramientas de aplicación práctica y concreta.

3.2 JUSTIFICACION

La planificación es un instrumento que establece metas y a la vez nos permite elegir medios para alcanzar dichas metas.

La palabra estrategia se ha utilizado de muchas maneras y en diferentes contextos a lo largo de los años. Su uso más frecuente ha sido en el ámbito militar, donde el concepto ha sido utilizado durante siglos. El término *estrategia* viene del griego *strategos* que significa "planificar la destrucción de los enemigos en razón del uso eficaz de los recursos". Ahora bien, definamos estrategia como una serie de actos que ejecuta una organización, empresa o institución, los cuales son seleccionados de acuerdo a una situación concreta considerando actores sociales, contexto, momento

en el tiempo, factores internos, externos y muchas otras variables, que conllevan a un fin real.

Entonces, la planificación estratégica puede definirse como un enfoque objetivo y sistemático para la toma de decisiones, por tal motivo es una herramienta técnica que permite prepararse para enfrentar las situaciones que se presentan en el futuro, ayudando con ello a orientar sus esfuerzos hacia metas realistas de desempeño. La planificación estratégica es falazmente sencilla: analiza la situación actual y la que se espera para el futuro a un plazo considerado y determina la dirección de la institución, por tanto desarrolla medios para lograr la misión institucional además es flexible para permitir modificaciones en los planes sin cambiar el objetivo de gestión específico ni el institucional. *En el Fondo Nacional de Desarrollo Regional FNDR, la planificación estratégica tendrá la función de orientar a la institución hacia el cumplimiento de una nueva visión y misión asignadas por el Plan Nacional de Desarrollo PND y la Constitución Política del Estado CPE, generando para los gobiernos autónomos municipales, departamentales e inclusive instituciones públicas priorizadas por el Gobierno Central, oportunidades de financiamiento con tasas de interés diferenciadas, sin comisiones por la administración de recursos y que sean atractivas para los sujetos de financiamiento.*

Se realizaron una serie de acciones destinadas a realizar el ordenamiento interno institucional del FNDR, habiéndose logrado el ordenamiento en el ámbito financiero y técnico (cierre de proyectos y programas).

Debe mencionarse que en el proceso de reordenamiento financiero, que tomó varias gestiones en la institución, a la fecha se tienen logros importantes, el resultado de los exámenes concluyen que los estados financieros de la institución presentan información confiable, transparente, oportuna y eficiente, entre lo que se destaca; la situación patrimonial y financiera de la institución, los resultados de las operaciones, la evolución del patrimonio del ejercicio fiscal; el estado de la cuenta, ahorro, inversión y financiamiento al 31 de diciembre de 2010.

Bajo estos antecedentes y al haberse cumplido el Plan Institucional de Mediano Plazo del FNDR 2007 – 2011, se ve la necesidad de generar un Plan que defina un horizonte institucional que sea sostenible en el tiempo, que no sea parte de una coyuntura política perecedera y que permita al FNDR seguir aportando al desarrollo del país. El fundamento del nuevo Plan Estratégico Institucional estará alineado a la actual política nacional de desarrollo expresado en los pilares "Bolivia Digna" y "Bolivia Productiva" del Plan Nacional de Desarrollo cuyo alcance trasciende aspectos coyunturales y fundamenta su sostenibilidad en un patrón de desarrollo integral y social como principales actores del proceso de cambio que atraviesa el Estado.

3.3 FUNDAMENTOS INSTITUCIONALES

3.3.1 HISTORIA INSTITUCIONAL

La profunda crisis económica que afectó al país en la década de los '80 y las políticas de ajuste estructural adoptadas a partir de 1985, a través del Decreto Supremo N° 21060 (promulgado el 29 de agosto de 1985 durante el Gobierno del Dr. Víctor Paz Estenssoro) tuvieron un costo social muy alto, afectando principalmente a las familias de bajos ingresos; es en esta compleja realidad en la que los Fondos de Inversión y Desarrollo (Fondo Social de Emergencia y Fondo Nacional de Desarrollo Regional) nacen, en el marco de las políticas de corte neoliberal que la mayoría de países latinoamericanos impulsaron entre 1985 y finales del año 2000.

El Fondo Nacional de Desarrollo Regional (FNDR) fue creado mediante Ley 926 del 25 de marzo de 1987, como una institución financiera pública, dependiente de la Presidencia de la República, cuya principal misión era fomentar el desarrollo económico y social de todas las regiones del país, mediante operaciones de crédito destinadas a financiar programas y proyectos de inversión pública.

Desde su creación sus clientes más importantes fueron Gobiernos Municipales grandes y medianos (con marcada concentración poblacional en las ciudades del eje central), las Corporaciones Regionales de Desarrollo, las Prefecturas Departamentales, entidades prestadoras de servicios públicos, cooperativas y servicios municipales.

El año 2001 mediante la promulgación de la Ley 2235, Ley del Dialogo Nacional 2000, se establece el marco institucional para uno de los pilares centrales de la política social de los gobiernos neoliberales de entonces: la Estrategia Boliviana de Reducción de la Pobreza (EBRP), la cual en líneas generales establece las prioridades de la política social y define las áreas de acción prioritarias para las entidades públicas en los distintos niveles de gestión pública (central, departamental y municipal).

Para finales del año 2005, el Fondo Nacional de Desarrollo Regional había dado algunos pasos interesantes, tendientes a promover un verdadero cambio institucional reflejados básicamente en mejoras en la gestión operativa, financiera y administrativa; sin embargo, los esfuerzos realizados no habían logrado preparar a la institución para enfrentar de manera adecuada los cambios de paradigmas y modelos de desarrollo, consecuencia de la contundente victoria electoral del Movimiento al Socialismo (MAS) en las elecciones presidenciales del 18 de diciembre de 2005.

La Revolución Democrática y Cultural comienza con la llegada de las organizaciones sociales al poder para conducir el país de una manera diferente, la histórica posición presidencial del 2006 marcó el inicio de una nueva era política en Bolivia.

Esta Revolución Democrática y Cultural, significa refundar Bolivia como un Estado Unitario Social de Derecho Plurinacional Comunitario, libre, independiente,

soberano, democrático, intercultural, descentralizado y con autonomías. Bolivia se funda en la pluralidad y el pluralismo político, económico, jurídico, cultural y lingüístico, dentro del proceso integrador del país, con la propuesta de una nueva Constitución Política del Estado **incluyente**, asimismo con una visión de país en donde sus habitantes se sientan protegidos de toda discriminación y racismo. Por ende económicamente soberana sobre sus recursos naturales y libre de analfabetismo. Estas y otras son las líneas políticas del cambio revolucionario. Hoy se le presenta al FNDR, la oportunidad de aportar y apoyar la reconstrucción del país que durante mucho tiempo fue saqueado por empresas transnacionales, con la complicidad de los gobiernos neoliberales de turno, que también han mantenido bajo control la exclusión de la política a los indígenas y a las clases empobrecidas.

3.3.2 NATURALEZA JURIDICA

El FNDR es una institución pública financiera no bancaria de desarrollo del Gobierno de Bolivia, de carácter descentralizado, bajo tuición del Ministerio de Planificación del Desarrollo (MPD), según el Decreto Supremo 29894 de Organización del Órgano Ejecutivo, con personalidad jurídica, autonomía de gestión administrativa, técnica y financiera, patrimonio propio y duración indefinida.

El marco jurídico - normativo que rige el accionar del Fondo Nacional de Desarrollo Regional en orden de importancia es el siguiente:

Constitución Política del Estado (7 de febrero de 2009)

Ley 926 (25 de marzo de 1987), creación el FNDR.

Ley 2235 Ley del Dialogo Nacional 2000 (31 de julio de 2001), transforma al FNDR en una entidad financiera no bancaria.

Además de las siguientes leyes complementarias:

Ley 1178 SAFCO (20 de julio de 1990)

Ley 2027 del Estatuto del Funcionario Público (27 de octubre de 1999)

Ley 031 Marco de Autonomías y Descentralización "Andrés Ibáñez" (19 de julio de 2010)

Ley 004 Lucha Contra la Corrupción, Enriquecimiento Ilícito e Investigación de Fortunas "Marcelo Quiroga Santa Cruz" (31 de marzo de 2010).

Ley 1632 de Telecomunicaciones (5 de julio de 1995), establece que el FNDR es el depositario de recursos para el financiamiento de proyectos de telecomunicaciones en áreas de interés social.

3.3.3 EL FNDR Y SU ADECUACIÓN A LAS POLITICAS DE CAMBIO DEL GOBIERNO NACIONAL

El 22 de enero de 2006 Bolivia inició un proceso de transformación profunda con el objetivo de **refundar** un país plurinacional, multicultural, multiétnico, incluyente, con justicia social e igualdad de oportunidades para todos.

Se promulga la Ley N° 3351 de Organización del Poder Ejecutivo (LOPE) que junto al Decreto Supremo N° 28631 reglamentan y organizan la administración pública, en el marco de la política definida por el Gobierno Nacional, esta LOPE define que el Fondo Nacional de Desarrollo Regional, como institución pública descentralizada, este bajo tuición del Ministerio de Planificación del Desarrollo (MPD).

Una vez definida su posición en la estructura del Poder Ejecutivo, el FNDR comienza un proceso de adecuación y transformación con el objetivo de garantizar su vigencia institucional y constituirse en aporte efectivo a las políticas públicas formuladas e impulsadas por el Gobierno Nacional.

Paralelamente a este proceso de transformación interna se debía continuar gestionando la cartera de créditos, desembolsando recursos para la ejecución de

proyectos de inversión pública, cumpliendo con sus obligaciones financieras (pago de deuda) a Organismos Financiadores y comprometiendo recursos para el financiamiento de nuevos proyectos.

En síntesis, la planta ejecutiva del FNDR debía garantizar la continuidad de las operaciones de financiamiento y la tarea aun más trascendente, diseñar y proponer las acciones necesarias que permitan la inserción de la institución en los nuevos paradigmas del Gobierno Nacional. Este proceso de adecuación y transformación institucional atravesó por 3 etapas que sintetizan y muestran las diferentes fases evolutivas por las que pasó la institución y que se resumen a continuación:

Primera Etapa: Enero/2006 a Diciembre/2006, el hito más importante de este periodo se da el 16 de junio de 2006, fecha en la que el Gobierno Nacional presenta en su primera versión el "Plan Nacional de Desarrollo (PND): Bolivia Digna, Soberana, Productiva y Democrática para Vivir Bien"; documento que define las políticas y líneas maestras que orientan el accionar y esfuerzos de las diferentes instituciones públicas.

Esta primera versión del PND, planteaba la creación de una entidad de financiamiento conformada por el Fondo Nacional de Desarrollo Regional (FNDR), el Fondo Nacional de Inversión Productiva y Social (FPS), la Nacional Financiera Boliviana (NAFIBO) y el Fondo de Desarrollo del Sistema Financiero y de Apoyo al Sector Productivo (FONDESIF). Esta nueva institución, financiaría (como entidad financiera de segundo piso) inversiones de largo plazo, privilegiando a la producción agropecuaria además de la pequeña y mediana empresa rural y urbana. También se llegaría con inversión en infraestructura productiva y social, en los niveles municipales, regionales y departamentales.

Sin embargo y de manera previa el FNDR debía ordenar sus operaciones de cartera, consolidar información sobre las capacidades de endeudamiento de los

Gobiernos Municipales y Prefecturas y cambiar la lógica del financiamiento de proyectos a una orientada a sujetos y/o programas en el marco del PND.

En este contexto el FNDR, el FPS y el DUF, iniciaron un trabajo orientado a definir sus futuros institucionales; en septiembre de 2006 las tres instituciones mencionadas presentaron una explicación íntegra – que incluía un diagnóstico institucional y una visualización preliminar sobre sus roles en el marco del PND - al entonces Ministro de Planificación del Desarrollo.

Como resultado de estos procesos de ilustración, discusión y construcción de un diagnóstico institucional, se evidenció el alto grado de complejidad operativa, financiera y normativa que implicaba la absorción del FNDR y FPS. De hecho el Decreto Supremo N° 28999 de 1° de enero de 2007, (mediante el cual se crea el Banco de Desarrollo Productivo Sociedad Anónima Mixta BDP – SAM) establece la creación de la Banca de Desarrollo, que nace como resultado de la adecuación institucional de la Nacional Financiera Boliviana NAFIBO en una primera etapa y la absorción gradual del FONDESIF, dejando pendiente la posibilidad de absorber al FPS y al FNDR.

Segunda Etapa: Enero/2007 a Diciembre/2007, el FNDR comenzó entonces un arduo trabajo concentrado en tres líneas de acción:

1. El diseño y cumplimento de Objetivos Estratégicos Inmediatos 2007 (la "nacionalización de recursos", el reordenamiento financiero, la conciliación de cartera con todos los sujetos de financiamiento, la inclusión del control social en los proyectos, liberando a los sujetos de crédito del centralismo e incorporando nuevas formas de financiamiento para planes, programas y proyectos), al cumplir con estos objetivos la institución cumplía con el mandato establecido en el PND y generaba las condiciones necesarias que le permitían encarar un proceso de readecuación institucional y/o enfrentar un proceso de cierre-liquidación-creación de una nueva alternativa institucional.

2. La creación de un nuevo Programa de Financiamiento (Recursos Propios FNDR Vivir Bien), el cual incorpora criterios de equidad en la asignación de recursos, transfiere responsabilidades y competencias a los sujetos de financiamiento, reorientando el proceso hacia un cambio real en la ejecución, además de la inclusión del control social en todo el ciclo del proyecto.

3. Para replantear la orientación de la institución, se elaboró el Plan Institucional de Mediano Plazo 2007–2011 (aprobado por el DUF mediante Resolución de Directorio N° 078/2007 del 2 de octubre de 2007) documento que define la Misión, Visión y los Objetivos Estratégicos e Institucionales del FNDR para ese periodo en el marco del Plan Nacional de Desarrollo.

El 12 de septiembre de 2007, a través del Decreto Supremo N° 29272 el Gobierno Nacional aprueba el Plan General de Desarrollo Económico y Social de la República, denominado: "Plan Nacional de Desarrollo: Bolivia Digna, Soberana, Productiva y Democrática para Vivir Bien -Lineamientos Estratégicos-", este documento define la Política de Financiamiento al Sector Productivo que prevé estructurar un sistema nacional de financiamiento público y privado, que será un mecanismo de promoción y articulación económica con equidad, sin embargo elimina especificidades relacionadas con los Fondos de Inversión y Desarrollo.

Tercera Etapa: Enero/2008 a Junio/2010, el año 2009, con la aprobación de la nueva Constitución Política del Estado se profundiza el Proceso de Cambio orientado a construir un nuevo Estado, si a este trascendental hecho se añade la reelección del Presidente Evo Morales (con niveles altos de aprobación), situación que originó la estructuración del Programa de Gobierno (2010-2015) con objetivos y metas más ambiciosas y concretas a las originalmente propuestas en el PND y la promulgación de un conjunto de leyes que reestructuran el ordenamiento jurídico del Estado; se establece un nuevo escenario de acción al cual debe acoplarse el FNDR, situación que

obliga a pensar en plantear un nuevo Plan Estratégico Institucional para el periodo 2012-2016.

3.4. MISION

Contribuir al Vivir Bien, mediante operaciones financieras, en forma oportuna y transparente, a través de planes, programas y proyectos de inversión socialmente productiva

3.5. VISION

Ser una institución financiera que cuenta con una oferta de recursos sostenible, diversificada, efectiva y oportuna, integrada con el control social, permitiendo el acceso de los actores regionales al financiamiento, contribuyendo al desarrollo del Estado Plurinacional.

3.6. OBJETIVOS

3.6.1 OBJETIVOS ESTRATÉGICOS

Ofrecer alter

instituciones priorizadas por el Gobierno del Estado Plurinacional.

Impulsar la inversión pública en el periodo 2012-2016, mediante la otorgación de recursos a los Sujetos de Financiamiento para la ejecución de planes, programas y proyectos de desarrollo, apoyando el proceso productivo (Bolivia Productiva).

Cumplir los lineamientos del PND respecto al financiamiento público con equidad, con el fin de reducir la pobreza (Bolivia Digna).

Implementar el proceso de cambio y transformación institucional en el marco de las nuevas políticas del Estado Plurinacional de Bolivia.

3.6.2 OBJETIVOS INSTITUCIONALES

1. Diseñar y ejecutar políticas financieras que permitan el acceso con equidad al financiamiento de las entidades territoriales y/o instituciones públicas priorizadas por el Gobierno del Estado Plurinacional.

2. Contribuir al desarrollo de las unidades territoriales mediante el financiamiento para infraestructura socialmente productiva.

3. Gestionar nuevos recursos internos y/o externos orientados a mejorar la oferta de financiamiento a las entidades territoriales y/o instituciones públicas priorizadas por el Gobierno del Estado Plurinacional.

4. Facilitar el acceso oportuno a recursos financieros para inversión socialmente productiva.

5. Asegurar la sostenibilidad financiera de la institución con nuevas políticas operativas y financieras.

6. Optimizar los procesos claves (de forma permanente) relacionados con la planificación y operación institucional en un ambiente de control adecuado con un enfoque basado en gestión de riesgos.

7. Colocar recursos para el financiamiento de planes, programas y/o proyectos de inversión pública por un valor proyectado de 460 millones de bolivianos hasta el año 2016.

8. Orientar y asistir técnicamente a los sujetos de financiamiento para fortalecer sus capacidades operativas y financieras para la administración de los recursos otorgados.

9. Apoyar al sector productivo con tasas de interés competitivas respecto al sistema financiero público y privado.

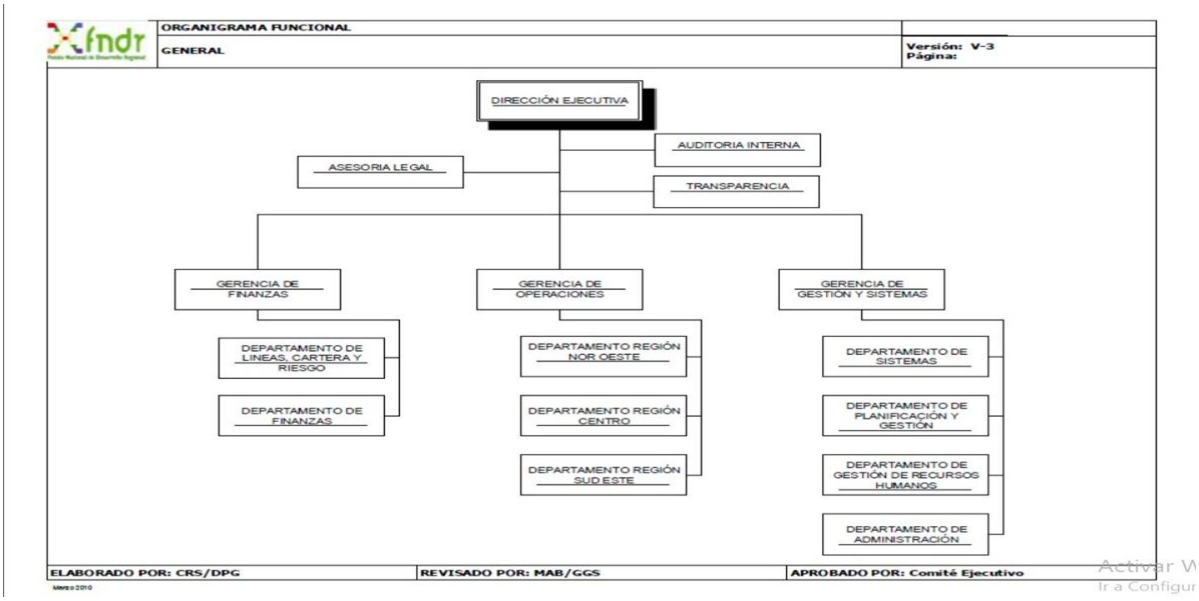
10. Medir el impacto social del financiamiento otorgado por la institución.

11. Consolidar los mecanismos de participación de los actores sociales en el proceso de financiamiento.

12. Garantizar la transparencia a través del acceso a la información, la consolidación del control social, promoción de la ética y lucha contra la corrupción.

3.7. ESTRUCTURA ORGÁNICA INSTITUCIONAL

El organigrama funcional del Fondo Nacional de Desarrollo Regional (FNDR), (ver fig. 3.1)



FUENTE: Fig. 3.1. Fondo Nacional de Desarrollo Regional (FNDR)

3.8. DEPARTAMENTO DE SISTEMAS DEL FNDR

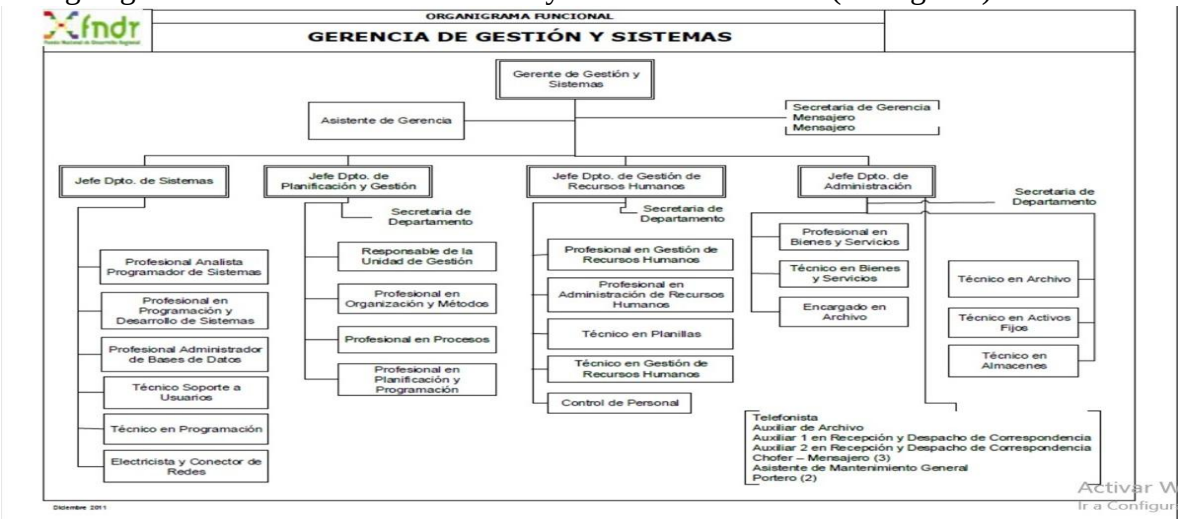
El objetivo del Departamento de Sistemas es el de Mantener a la institución tecnológicamente actualizada mediante la implementación de sistemas y equipos informáticos de alta calidad, aplicando normas vigentes y procedimientos adecuados.

Entre sus principales funciones:

- ✓ Desarrollar, administrar y actualizar los sistemas aplicativos de acuerdo a las necesidades institucionales;
- ✓ Planificar, desarrollar e implementar proyectos informáticos para coadyuvar el logro de los objetivos institucionales;
- ✓ Brindar soporte informático a todas las áreas y unidades organizacionales de la Institución, garantizar la seguridad informática de la institución;
- ✓ Administrar y realizar el mantenimiento de dispositivos informáticos de la red de datos: servidores, equipo activo, estaciones de trabajo, periféricos y otros;
- ✓ Administrar y actualizar los sistemas de comunicación interna y externa;
- ✓ Definir, implantar y velar por la seguridad informática dentro de la Institución, adoptando: políticas, planes y acciones definidas para el efecto;

- ✓ Coordinar con el Departamento de Gestión de Recursos Humanos, la programación de capacitación en sistemas desarrollados y en herramientas informáticas, para el personal de la Institución;
- ✓ Implementar la logística de la sala de servidores cumpliendo las condiciones necesarias para ello;
- ✓ Administrar precautelar el cableado estructurado, en cuanto a su mantenimiento y expansión.

El organigrama de la Gerencia de Gestión y Sistemas del FNDR (ver fig. 3.2)



FUENTE: Fig. 3.2. Fondo Nacional de Desarrollo Regional (FNDR)

CAPITULO IV.

Marco Aplicativo

4.1. Contexto

Las Normas de Auditoría de Tecnología de Información y Comunicación, emitida por la Contraloría General del Estado Plurinacional son de aplicación obligatoria en la práctica de la auditoría realizada en toda entidad pública comprendida en los artículos 3 y 4 de la Ley Nº 1178, de Administración y Control Gubernamentales, promulgada el 20 de julio de 1990, por lo que es aplicable al Fondo Nacional de Desarrollo Regional (FNDR).

Proteger al FNDR (aplicar seguridad) a cada una de las actividades, acciones y tareas de la organización (la información) mediante el conjunto de personas que cumplen distintos roles en la entidad.

Las medidas de seguridad han de ser proporcionales a los medios que queremos proteger. A grandes rasgos se entiende que mantener un sistema seguro (o fiable) consiste básicamente en garantizar tres aspectos: Confidencialidad, integridad, disponibilidad.

La norma/estándar UNE ISO/IEC 27001:2007 del "Sistema de Gestión de la Seguridad de la Información" es la solución de mejora continua más adecuada para evaluar los riesgos físicos y lógicos

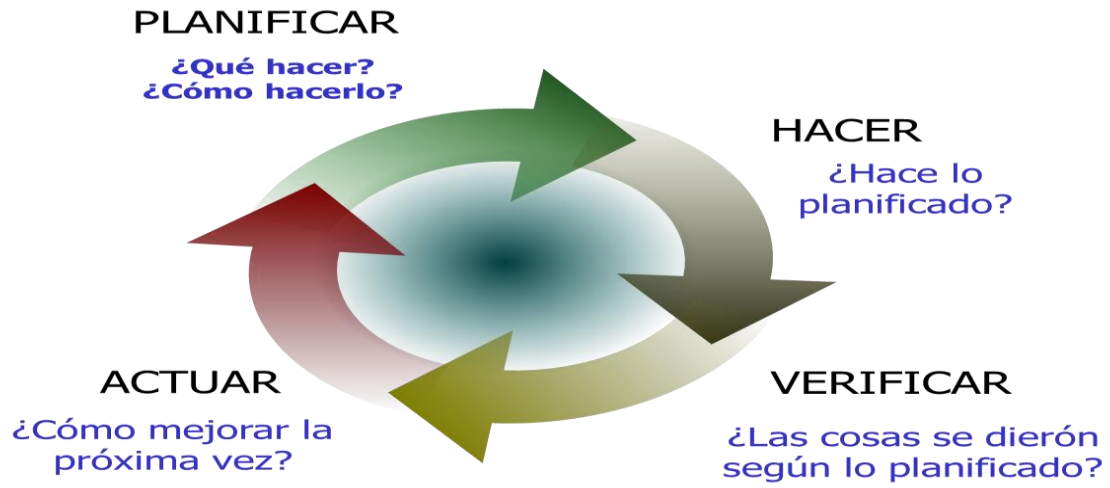
El proceso de auditoría para la seguridad de Sistemas de Información es similar al que se lleva a cabo a los de estados financieros.

Sin embargo, la aplicación un enfoque basado en procesos para la seguridad de entornos informáticos basado en la norma UNE-ISO/IEC 27001:2007 aplicable al Fondo Nacional de Desarrollo Regional (FNDR) agrega valor.

4.2. Proceso metodológico

El método de auditoria para la seguridad de Sistemas de Información sigue un enfoque basado en procesos para la seguridad de entornos informáticos basado en la

norma UNE-ISO/IEC 27001:2007 aplicable al Fondo Nacional de Desarrollo Regional (FNDR). (ver figura 4.1).



FUENTE: Elaboración propia. Figura 4.1. Proceso metodológico

4.2.1. Planificar

En esta fase se establecen las relaciones entre auditores y colaboradores de la organización, para determinar el alcance y objetivos. Se hace un bosquejo de la situación de FNDR, acerca de su organización, sistema de información, controles internos, estrategias y demás elementos que le permitan al auditor gubernamental elaborar el programa de auditoría que se llevará a efecto.

Elementos Principales de esta Fase:

1. Conocimiento y Comprensión de la Entidad;
2. Objetivos y Alcance de la auditoría;
3. Análisis Preliminar del Control Interno;
4. Análisis de los Riesgos;
5. Planeación Específica de la auditoría;
6. Elaboración de programas de Auditoría.

4.2.2. Hacer

La ejecución de la auditoría, constituye la recopilación de la mayor cantidad de información necesaria, como son documentos y evidencias que permitan al auditor fundamentar sus comentarios, sugerencias y recomendaciones, con respecto al manejo y administración de TI.

Para la recolección de información, se pueden aplicar las siguientes técnicas:

- ✓ Entrevistas;
- ✓ Simulación;
- ✓ Cuestionarios; (ver fig. 4.1)
- ✓ Análisis de la información documental entregada por el auditado;
- ✓ Revisión y Análisis de Estándares;
- ✓ Revisión y Análisis de la información de auditorías anteriores.

ENCUESTA - SEGURIDAD FÍSICA

ÀREA:	
APELLIDOS Y NOMBRES:	
CARGO:	

Nro.	VARIABLES	SI	NO	AMENAZA		
				BAJO	MEDIO	ALTO
	PROCEDIMIENTOS GENERALES					
1	¿Existe una política de seguridad física en la institución y está actualizada?					
2	¿Existen y se difunden los planes de contingencia/emergencia?					
3	¿Existe un registro de todos los incidentes de seguridad y están clasificados según su gravedad?					
4	¿Se dan conferencias sobre Seguridad Física a todos los empleados al incorporarse al trabajo y de forma periódica?					
5	¿Se ha realizado un análisis de riesgos de la Seguridad Física?					
6	¿Tiene la institución contratados seguros generales?					
7	¿La ubicación del Área de informática está estudiada y documentada?					
8	¿Las salas de los ordenadores están alejadas y aisladas de los ruidos y vibraciones?					
9	¿El espacio es compartido? (oficina, área de informática, común)					
10	¿Está cerca de alguna puerta?					
11	¿Está cerca de algún pasillo?					
12	¿Está cerca de alguna ventana?					
13	¿Guarda la documentación impresa o magnética bajo llave propia?					

14	¿Guarda la documentación impresa o magnética bajo llave común al sector?					
15	¿Hay cables al descubierto?					

Nro.	VARIABLES	SI	NO	AMENAZA		
				BAJO	MEDIO	ALTO
	CONTROL DE ACCESO					
1	¿Se ha realizado un estudio de riesgos de intrusión en el edificio?					
2	¿Se ha realizado un análisis de riegos de acceso al área de informática?					
3	¿El área de informática está completamente aislado del resto del edificio y sus accesos controlados?					
4	¿Existe un circuito cerrado de televisión que controle el acceso al área de informática y las puertas de emergencia?					
5	¿Existe un registro escrito o impreso de todos los accesos a todas las salas de equipos informáticos?					
6	¿Todas las personas con acceso autorizado tienen una tarjeta de identificación y están controlados?					
7	¿Se utiliza un sistema de control de acceso automático para el ingreso al área de informática?					
8	¿El acceso al área de informática está auditado, tanto para la entrada como para la salida?					
9	¿Existe una vigilancia interior por medio de detectores de intrusión, conectado a un puesto permanente de vigilancia?					
10	¿Existe una vigilancia exterior por medio de detectores de intrusión, conectado a un puesto permanente de vigilancia?					
11	¿Se necesita un permiso expreso para acceder al área de informática?					
12	¿Se notifican con antelación al área de informática las visitas previstas?					

Nro.	VARIABLES	SI	NO	AMENAZA		
				BAJO	MEDIO	ALTO
	INCENDIO					
1	¿Se ha realizado un estudio de los riesgos de incendio que cubra tanto la prevención como la protección?					
2	El mobiliario del edificio del área de informática es ignífugo?					
3	¿Existe un sistema automático de detección de incendios y está conectado a una central de alarmas?					
4	¿Los conductos de aire acondicionado/ventilación están equipados con válvulas automáticas contra incendios?					
5	¿Se activa automáticamente el sistema de corte de energía eléctrica tras la detección de un incendio?					
6	¿Estas instalaciones son revisadas periódicamente, conforme a la reglamentación y tienen un mantenimiento adecuado?					
7	¿Existe una instalación de extintores portátiles en el conjunto de los locales informáticos y el equipamiento del entorno?					
8	¿La cantidad de papel almacenada en las salas de impresión es inferior a las necesidades de un día de producción?					
9	¿Está prohibido fumar en el área de informática y se respeta la prohibición?					
10	¿Se evita la acumulación de material innecesario en el área de informática?					

Nro.	VARIABLES	SI	NO	AMENAZA		
				BAJO	MEDIO	ALTO

AGUA						
1	Los problemas relacionados con el agua (lluvia, goteras, inundación). ¿Han sido tratados adecuadamente (filtración, drenaje…)?					
2	¿El techo de la sala donde se encuentran los equipos informáticos es impermeable?					
3	¿Se realiza una revisión periódica del estado de las tuberias, llaves de paso y canalizaciones?					
4	¿Todo el sistema de cableado está protegido contra inundaciones / humedad?					
Nro.	**VARIABLES**	**SI**	**NO**	**AMENAZA**		
				BAJO	**MEDIO**	**ALTO**
SUMINISTRO ELECTRICO						
1	¿Existe un sistema de vigilancia de la calidad y continuidad del suministro eléctrico?					
2	¿Existe un sistema de alimentación ininterrumpida?					
3	¿Existe un sistema autónomo de generación de energía eléctrica?					
4	¿La instalación eléctrica del edificio cumple con la normativa vigente?					
5	¿Está el personal instruido y existen carteles visibles sobre las acciones a tomar en caso de descarga eléctrica?					
6	¿Tienen los equipos informáticos placas para que el personal se descargue de la electricidad estática?					
Nro.	**VARIABLES**	**SI**	**NO**	**AMENAZA**		
				BAJO	**MEDIO**	**ALTO**
COMUNICACIONES						
1	¿Existen sistemas de comunicación alternativos en caso de avería o fallo?					
2	Se realizan pruebas periódicas para garantizar la calidad de las líneas y sistemas de comunicación?					
3	Los paneles de control de las comunicaciones. ¿Son revisados periódicamente?					
4	El cableado, ¿está protegido frente a accesos no autorizados, sabotaje, etc.?					
5	Los equipos de comunicaciónes, ¿se encuentran un lugar de acceso restringido?					
6	¿El cableado de comunicaciones está separado de la instalación eléctrica?					
Nro.	**VARIABLES**	**SI**	**NO**	**AMENAZA**		
				BAJO	**MEDIO**	**ALTO**
HARDWARE/SOFTWARE						
1	¿Existe un plan establecido para el mantenimiento y la protección del hardware y de los soportes de almacenamiento de la información?					
2	¿Existe un control de configuración del hardware y del software?					
3	¿Existe un plan de mantebnimiento del hardware?					
4	¿Existe un registro de entrada y salida del hardware?					
5	¿Se registran y documentan todos los fallos software que se detectan?					
6	¿Existen al menos 2 copias de software de aplicación y de base, almacenadas en lugares distintos al de su utilización?					

Por favor, si desea, usted puede adicionar algunas variables relevantes para el dominio del problema:

1.-……..
2.-……..
3.-……..
4.-……..
5.-……..
6.-……..

La Paz, 25 de abril del 2015

FUENTE: Elaboración propia, fig. 4.1 Formulario encuesta para el Centro de Cómputo

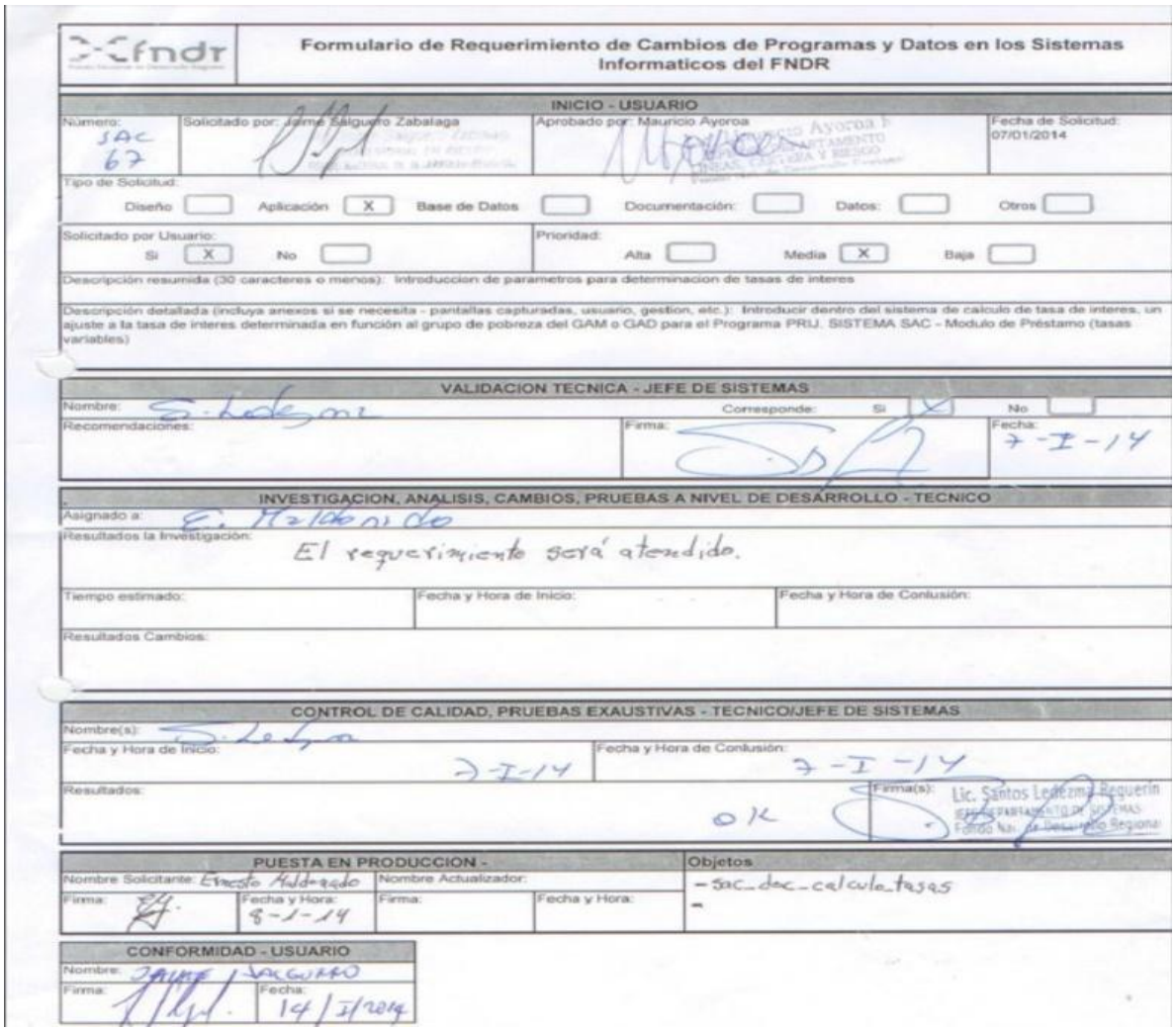
La evidencia se clasifica de la siguiente manera:

a) Evidencia documental. (ver fig. 4.2)

b) Evidencia física.

c) Evidencia analítica.

d) Evidencia testimonial.



Formulario de Requerimiento de Cambios de Programas y Datos en los Sistemas Informaticos del FNDR

INICIO - USUARIO

Numero: SAC 67 | Solicitado por: Jaime Salguero Zabalaga | Aprobado por: Mauricio Ayoroa | Fecha de Solicitud: 07/01/2014

Tipo de Solicitud: Diseño [ ] Aplicación [X] Base de Datos [ ] Documentación: [ ] Datos: [ ] Otros [ ]

Solicitado por Usuario: Si [X] No [ ] | Prioridad: Alta [ ] Media [X] Baja [ ]

Descripción resumida (30 caracteres o menos): Introduccion de parametros para determinacion de tasas de interes

Descripción detallada (incluya anexos si se necesita - pantallas capturadas, usuario, gestion, etc.): Introducir dentro del sistema de calculo de tasa de interes, un ajuste a la tasa de interes determinada en función al grupo de pobreza del GAM o GAD para el Programa PRIJ. SISTEMA SAC - Modulo de Préstamo (tasas variables)

VALIDACION TECNICA - JEFE DE SISTEMAS

Nombre: E. Ledesma | Corresponde: Si [X] No [ ] | Recomendaciones: | Firma: | Fecha: 7-I-14

INVESTIGACION, ANALISIS, CAMBIOS, PRUEBAS A NIVEL DE DESARROLLO - TECNICO

Asignado a: E. Heldenido

Resultados la Investigación: El requerimiento será atendido.

Tiempo estimado: | Fecha y Hora de Inicio: | Fecha y Hora de Conlusión:

Resultados Cambios:

CONTROL DE CALIDAD, PRUEBAS EXAUSTIVAS - TECNICO/JEFE DE SISTEMAS

Nombre(s): E. Ledesma

Fecha y Hora de Inicio: 7-I-14 | Fecha y Hora de Conlusión: 7-I-14

Resultados: OK | Firma(s): Lic. Santos Ledezma Requerin

PUESTA EN PRODUCCION - | Objetos: -SAC_dec_calculo_tasas

Nombre Solicitante: Ernesto Heldenido | Nombre Actualizador: | Firma: | Fecha y Hora: 8-I-14

CONFORMIDAD - USUARIO

Nombre: Jaime Salguero | Firma: | Fecha: 14/I/2014

FUENTE: FNDR. fig. 4.2 Formulario cambios a programa

Una vez que tenemos información real y confiable, procedemos a evaluar y probar la manera en la que han sido diseñados los controles en la organización, para el mejoramiento continuo de la misma, para esto el equipo de Auditoría utilizara medios informáticos y electrónicos que permitan obtener resultados reales.

El equipo de auditores, para poder dar una opinión sobre un sistema o proceso informático, debe comprobar el funcionamiento de los sistemas de información y efectuar una revisión completa de los equipos de cómputo a través del siguiente proceso en forma sistemática y disciplinada:

4.2.2.1 Política de seguridad

El Fondo Nacional de Desarrollo Regional (FNDR), requiere una política que refleje las expectativas de la organización en materia de seguridad, a fin de establecer una administración con dirección y soporte. La política también se puede utilizar como base para el estudio y evaluación en curso.

La política de seguridad requiere ejecutar 2 controles:

A.5 Política de seguridad

A.5.1 Política de seguridad de la información *Objetivo de control:* Dirigir y dar soporte a la gestión de la seguridad de la información en concordancia con los requisitos del negocio, las leyes y las regulaciones.		
A.5.1.1	*Documentos de política de seguridad de la información*	Control La gerencia deberá aprobar, publicar y comunicar a todos los empleados y terceras partes que lo requieran.
A.5.1.2	*Revisión de la política de seguridad de información*	Control La política será revisada en intervalos planificados, y en caso de cambios que la afecten, asegurar que siga siendo apropiada, conveniente y efectiva.

4.2.2.2 Estructura organizativa

Sugiere diseñar una estructura de administración dentro la organización, que establezca la responsabilidad de los grupos en ciertas áreas de la seguridad y un proceso para el manejo de respuesta a incidentes.

Los aspectos organizativos para la seguridad requieren ejecutar 11 controles:

A.6 Seguridad organizacional

A.6.1 Organización interna *Objetivo de control:* Gestionar la seguridad de la información dentro de la organización.		
A.6.1.1	*Comité de Gestión de seguridad de la información*	Control La gerencia debe respaldar activamente la seguridad dentro de la organización a través de una dirección clara, un compromiso apropiado, recursos adecuados y conocimiento de responsabilidades de la seguridad de información.
A.6.1.2	*Coordinación de la seguridad de la información*	Control Las actividades en la seguridad de información deben ser coordinados por representantes de diferentes partes de la organización que tengan roles relevantes y funciones de trabajo.
A.6.1.3	*Asignación de responsabilidades sobre seguridad de la información*	Control Todas las responsabilidades sobre la seguridad de información deben ser claramente definidas.
A.6.1.4	*Proceso de autorización para las nuevas instalaciones de procesamiento de información*	Control Debe establecerse y definirse un proceso de gestión de autorización para facilitar los nuevos procesamientos información.
A.6.1.5	*Acuerdos de confidencialidad*	Control Se debe identificar y revisar regularmente los requisitos de confidencialidad o acuerdos de no divulgación que reflejen las necesidades de la organización para la protección de información.
A.6.1.6	*Contacto con autoridades*	Control Se debe mantener contactos apropiados con las autorizaciones relevantes.
A.6.1.7	*Contacto con grupos de interés especial*	Control Se debe mantener contactos con grupos de interés especial u otros foros de especialistas en seguridad así como de asociaciones profesionales.
A.6.1.8	*Revisión independiente de seguridad de la información*	Control El alcance de la organización para manejar la seguridad de información, así como su implementación (como por ejemplo: los objetivos de control, los controles, las políticas, procesos y procedimientos) deben ser revisados independientemente durante intervalos planificados o cuando ocurran cambios significativos en la implementación.

A.6.2 Seguridad del acceso a terceras partes *Objetivo de control:* Mantener la seguridad de las instalaciones de procesamiento de la información organizacional que acceden, procesan, comunican o gestionan terceros.		
A.6.2.1	*Identificación de riesgos por el acceso de terceros*	Control Se evaluará los riesgos asociados con el acceso a las instalaciones de procesamiento de la información organizacional por parte de terceros, y se implementarán controles de seguridad adecuados antes de permitir su acceso.
A.6.2.2	*Requisitos de seguridad cuando se trata con clientes*	Control Se deben identificar todos los requisitos de seguridad antes de dar acceso a clientes a los activos o a la información de la organización.
A.6.2.3	*Requisitos de seguridad en contratos con terceros*	Control Los acuerdos que involucran el acceso, procesamiento, comunicación o manejo de terceros de las instalaciones de procesamiento de información organizacional o la adición de productos o servicios a dichas instalaciones deben cubrir todos los requisitos de seguridad necesarios.

4.2.2.3. Clasificación y Control de Activos

Inventario de los recursos de información de la organización y con base en este conocimiento, debe asegurar que se brinde un nivel adecuado de protección.

La clasificación y control de activos requiere ejecutar 5 controles:

A.7 Gestión de activos

A.7.1 Responsabilidad por los activos *Objetivo de control:* Mantener la protección apropiada de los activos de la organización.		
A.7.1.1	*Inventario de activos*	Control Se elaborará y mantendrá un inventario de todos los activos importantes que sean claramente identificados.
A.7.1.2	*Propiedad de los activos*	Control Toda la información y los activos asociados con las instalaciones de procesamiento de información deben ser propiedad[3] de una parte designada de la organización.
A.7.1.3	*Uso aceptable de los activos*	Control Se deben de identificar, documentar e implementar las reglas para el uso aceptable de los activos de información asociados con las instalaciones de procesamiento de información.

A.7.2 Clasificación de la información *Objetivo de control:* Asegurar que los activos de información reciban un nivel de protección adecuado.		
A.7.2.1	*Guías de clasificación*	Control La información debe ser clasificada en términos de su valor, requisitos legales, sensibilidad y criticidad para la organización.
A.7.2.2	*Etiquetado y tratamiento de la información*	Control Se definirá e implementará un conjunto de procedimientos apropiados para etiquetar y manejar información de conformidad con el esquema de clasificación adoptado por la organización.

4.2.2.4. Seguridad ligada al personal

Necesidad de educar e informar a los empleados actuales y potenciales sobre lo que se espera de ellos en materia de seguridad y asuntos de confidencialidad. Implementa un plan para reportar los incidentes.

La seguridad de Recursos Humanos requiere ejecutar 9 controles:

A.8 Seguridad en recursos humanos

A.8.1 Previo al empleo[4] *Objetivo de control:* Asegurar que los empleados, contratistas y usuarios externos entiendan sus responsabilidades y que estos sean adecuados a los roles para los cuales han sido considerados y reducir así el riesgo de estafa, fraude o mal uso de las instalaciones.		
A.8.1.1	*Roles y responsabilidades*	Control Se definirán y documentarán los roles de seguridad y las responsabilidades de los empleados, contratistas y usuarios externos en concordancia con la política de seguridad de la información de la organización.
A.8.1.2	*Investigación*	Control Se debe hacer un chequeo y verificación de informaciones anteriores de todos los candidatos para empleos, contratistas y personal externo, en concordancia con las leyes, regulaciones y ética; y proporcional a los requisitos del negocio, la clasificación de la información a ser accedida y a los riesgos percibidos.
A.8.1.3	*Términos y condiciones de la relación laboral*	Control Los empleados, contratistas y terceros suscribirán un acuerdo de confidencialidad como parte de los términos y condiciones iniciales de su empleo en donde se señalará la responsabilidad del empleado en cuanto a la seguridad de la información.

A.8.2 Durante el empleo *Objetivo de control:* Asegurar que todos los empleados, contratistas y usuarios externos sean conscientes de las amenazas y riesgos en el ámbito de la seguridad de la información, y que estén preparados para aplicar la política de seguridad de la organización en el curso de trabajo normal y reducir el riesgo de error humano.		
A.8.2.1	*Gestión de responsabilidades*	Control La gerencia debe requerir a los empleados, contratistas y a los usuarios externos aplicar la seguridad en concordancia con las políticas y procedimientos de la organización.
A.8.2.2	*Concientización, educación y entrenamiento en la seguridad de información*	Control Todos los empleados de la organización y, donde sea relevante, contratistas y usuarios externos deben recibir una adecuada concientización, entrenamiento y actualizaciones regulares en los procesos y políticas organizacionales, como acciones relevantes de su función laboral.
A.8.2.3	*Proceso disciplinario*	Control Debe existir un proceso disciplinario para los empleados que hayan cometido una violación de seguridad.

A.8.3 Finalización o cambio de empleo *Objetivo de control:* Asegurar que los empleados, contratistas y usuarios externos dejen o cambien de organización de una forma ordenada.		
A.8.3.1	*Responsabilidades de finalización*	Control Debe informarse sobre los incidentes de seguridad a través de canales administrativos adecuados tan pronto como sea posible.
A.8.3.2	*Devolución de activos*	Control Todos los empleados, contratistas y usuarios externos deben realizar la devolución de los activos de la organización que están en su posesión cuando termine su empleo, contrato o acuerdo.
A.8.3.3	*Retiro de los derechos de acceso*	Control El derecho de acceso a la información y a las instalaciones de procesamiento de información, que se le otorga a los empleados, contratistas y usuarios externos, debe ser removido cuando termine su empleo, contrato o acuerdo; o modificado ante cambios.

4.2.2.5. Seguridad física y del Entorno

La seguridad física y del entorno, responde a la necesidad de proteger las áreas, el equipo y los controles generales. La seguridad física y del entorno requiere ejecutar 13 controles:

A.9 Seguridad física y del entorno

A.9.1 Áreas seguras *Objetivo de control:* Prevenir accesos no autorizados, daños e interferencias contra los locales y la información de la organización.		
A.9.1.1	*Seguridad física perimetral*	Control Las organizaciones usarán perímetros de seguridad (barreras como paredes, puertas con control de entrada por tarjeta o recepciones) para proteger áreas que contienen información e instalaciones de procesamiento de información.
A.9.1.2	*Controles físicos de entradas*	Control Las áreas seguras estarán protegidas mediante controles de acceso adecuados para garantizar que únicamente personal autorizado pueda ingresar.
A.9.1.3	*Seguridad de oficinas, despachos y recursos*	Control Se deben designar y mantener áreas seguras con el fin de proteger las oficinas, despachos e instalaciones.
A.9.1.4	*Protección contra amenazas externas y ambientales*	Control Se deben designar y mantener protección física contra daños por fuego, inundación, terremoto, explosión, manifestación civil y otras formas de desastre natural o realizado por el hombre.
A.9.1.5	*El trabajo en las áreas seguras*	Control Se debe designar y mantener protección física y pautas para trabajar en áreas seguras.
A.9.1.6	*Áreas de carga, descarga y acceso público*	Control Las áreas de carga, descarga y acceso público y otras áreas donde las personas tengan acceso deben controlarse y, cuando sea posible, aislarse de las instalaciones de procesamiento de información para evitar un acceso no autorizado.

A.9.2 Seguridad de los equipos *Objetivo de control:* Prevenir pérdidas, daños o comprometer los activos así como la interrupción de las actividades de la organización.		
A.9.2.1	*Ubicación y protección de equipos*	Control El equipamiento será ubicado o protegido para reducir los riesgos de amenazas, peligros ambientales y oportunidades de acceso no autorizado.
A.9.2.2	*Suministro eléctrico*	Control El equipamiento se protegerá de fallas de energía y otras anomalías eléctricas causadas por fallo en el suministro eléctrico.
A.9.2.3	*Seguridad del cableado*	Control Se protegerá el cableado de energía y telecomunicaciones que transportan datos o respaldan servicios de información frente a interceptaciones o daños.
A.9.2.4	*Mantenimiento de equipos*	Control El equipamiento recibirá un adecuado mantenimiento para garantizar su continua disponibilidad e integridad.
A.9.2.5	*Seguridad de equipos fuera de los locales de la organización*	Control Se debe aplicar seguridad al utilizar equipamiento para procesar información fuera de los locales de la organización tomando en cuenta los diferentes riesgos en los que se incurre.
A.9.2.6	*Seguridad en el re-uso o eliminación de equipos*	Control Todos los equipos que contienen almacenamiento de datos deben ser revisados con el fin de asegurar que los datos sensibles y los software con licencia han sido removidos o sobrescritos antes de desecharlos o reutilizarlos.
A.9.2.7	*Retiro de propiedad*	Control Los equipos, información y software no deben ser retirados fuera de la organización sin una autorización previa.

4.2.2.6. Gestión de Comunicaciones y Operaciones

- ✓ Asegurar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información.
- ✓ Minimizar el riesgo de falla de los sistemas.
- ✓ Proteger la integridad del software y la información.
- ✓ Conservar la integridad y disponibilidad del procesamiento y la comunicación de la información.
- ✓ Garantizar la protección de la información en las redes y de la infraestructura de soporte.
- ✓ Evitar daños a los recursos de información e interrupciones en las actividades de la institución.
- ✓ Evitar la pérdida, modificación o uso indebido de la información que intercambian las organizaciones

La gestión de operaciones y comunicaciones requiere ejecutar 32 controles:

A.10 Gestión de comunicaciones y operaciones

A.10.1 Procedimientos y responsabilidades de operación *Objetivo de control:* Asegurar la operación correcta y segura de los recursos de procesamiento de información.		
A.10.1.1	*Documentación de procedimientos operativos*	Control Los procedimientos operativos deberán estar documentados, mantenidos y estar disponibles a todos los usuarios que lo requieran.
A.10.1.2	*Gestión de cambios*	Control Se controlarán los cambios en las instalaciones y sistemas de procesamiento de la información.
A.10.1.3	*Segregación de tareas*	Control Se segregarán las obligaciones y las áreas de responsabilidad con el fin de reducir las oportunidades de modificaciones no autorizadas o mal uso de los activos de la organización.

A.10.1.4	*Separación de las instalaciones de desarrollo, prueba y operación*	Control Se separarán las instalaciones de desarrollo, prueba y operación con el fin de reducir el riesgo de acceso no autorizado o cambios en el sistema operacional.

A.10.2 Gestión de entrega de servicios externos *Objetivo de control:* Implementar y mantener un nivel apropiado de seguridad de información y servicios de entrega en concordancia con los acuerdos de servicios de entrega por parte de terceros.		
A.10.2.1	*Entrega de servicios*	Control Debemos asegurarnos que los controles de seguridad, las definiciones de servicio y los niveles de entrega incluidos en el acuerdo de servicios externos sean implementados, estén operativos y sean mantenidos por el personal externo.
A.10.2.2	*Monitoreo y revisión de los servicios externos*	Control Los servicios, reportes, y registros provistos por terceras partes deben ser monitoreados y revisados regularmente. Igualmente, se deben de llevar a cabo auditorías con regularidad.

A.10.2.3	*Gestión de cambios de los servicios externos*	Control Se debe manejar los cambios en la provisión de servicios, incluyendo el mantenimiento y mejora de la política de seguridad de información, procedimientos y controles, tomando en cuenta la criticidad de los sistemas de negocio y procesos envueltos en la reevaluación de riesgos.

A.10.3 Planificación y aceptación del sistema *Objetivo de control:* Minimizar el riesgo de fallas de los sistemas.		
A.10.3.1	*Gestión de la capacidad*	Control Se monitorearán las demandas de capacidad y se harán las proyecciones de futuros requisitos de capacidad para asegurar el desarrollo requerido por el sistema.
A.10.3.2	*Aceptación del sistema*	Control Se establecerán los criterios de aceptación para nuevos sistemas de información, actualizaciones y nuevas versiones y se llevarán a cabo pruebas adecuadas del sistema antes de la aceptación.

A.10.4 Protección contra software malicioso *Objetivo de control:* Proteger la integridad del software y de la información.		
A.10.4.1	*Controles contra software malicioso*	Control Para ofrecer protección frente a software malicioso, se implementarán controles de detección, prevención y procedimientos adecuados de toma de conciencia con los usuarios.
A.10.4.2	*Controles contra software móvil*	Control Donde sea autorizado el uso de software móvil, la configuración debe asegurar que este opere de acuerdo a una política de seguridad clara y definida. Igualmente, se debe prevenir la ejecución de código móvil no autorizado.

A.10.5 Gestión interna de respaldo y recuperación *Objetivo de control:* Mantener la integridad y disponibilidad del procesamiento de información y servicios de comunicación.		
A.10.5.1	*Recuperación de la información*	Control Se obtendrán y probarán las copias de recuperación y respaldo de información y software regularmente en concordancia con la política acordada.

A.10.6 Gestión de seguridad de redes *Objetivo de control:* Asegurar la salvaguarda de información en las redes y la protección de la infraestructura de soporte.		
A.10.6.1	*Controles de red*	Control Se implementará un conjunto de controles para lograr y mantener la seguridad en las redes, y mantener la seguridad de los sistemas y aplicaciones usuarios de la red, incluyendo la información en tránsito.
A.10.6.2	*Seguridad de los servicios de red*	Control Se deben identificar e incluir en cualquier acuerdo de servicio de red los aspectos de seguridad, niveles de servicio y requisitos de gestión, así estos servicios sean provistos interna o externamente.

A.10.7 Utilización y seguridad de los medios de información *Objetivo de control:* Prevenir daños, modificaciones o destrucciones a los activos e interrupciones de las actividades del negocio.		
A.10.7.1	*Gestión de medios removibles*	Control Deben de existir procedimientos para la gestión de medios removibles.
A.10.7.2	*Eliminación de medios*	Control Se eliminarán los medios de forma segura cuando ya no se necesiten, utilizando procedimientos formales.
A.10.7.3	*Procedimientos de manipulación de la información*	Control Se establecerán procedimientos para el manejo y almacenamiento de la información con el fin de proteger dicha información de divulgaciones no autorizadas o su mal uso.
A.10.7.4	*Seguridad de la documentación de sistemas*	Control La documentación de los sistemas se protegerá de accesos no autorizados.

A.10.8 Intercambio de información *Objetivo de control:* Mantener la seguridad de información y el intercambio de software dentro de la organización y con entidades externas.		
A.10.8.1	*Políticas y procedimientos para el intercambio de información*	Control Se deben establecer políticas, procedimientos y controles para proteger el intercambio de información durante el uso de todo tipo de recursos de comunicación.
A.10.8.2	*Acuerdos de intercambio*	Control Se deben de establecer acuerdos para el intercambio de información y software entre la organización y entidades externas.
A.10.8.3	*Seguridad de medios físicos en tránsito*	Control Los medios a ser transportados deberán ser protegidos de acceso no autorizado, mal uso o corrupción durante su transporte fuera de los límites físicos de la organización.
A.10.8.4	*Seguridad del correo electrónico*	Control La información contenida en correos electrónicos debe ser protegida apropiadamente.
A.10.8.5	*Seguridad en los sistemas de información de negocio*	Control Se deben desarrollar e implementar políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información del negocio.

A.10.9 Servicios de comercio electrónico *Objetivo de control:* Mantener la seguridad en los servicios de comercio electrónico y la seguridad en su uso.		
A.10.9.1	*Seguridad en comercio electrónico*	Control El comercio electrónico será protegido frente a actividades fraudulentas, controversias contractuales y divulgación o modificación de información.
A.10.9.2	*Seguridad en las transacciones en línea*	Control La información contenida en las transacciones en línea debe ser protegida para prevenir transmisiones incompletas, rutas incorrectas, alteración no autorizada de mensajes, o duplicación no autorizada de mensajes.
A.10.9.3	*Información disponible públicamente*	Control Se protegerá la integridad de la información públicamente disponible para prevenir modificaciones no autorizadas.

A.10.10 Monitoreo *Objetivo de control:* Detectar actividades de procesamiento de información no autorizadas.		
A.10.10.1	*Registro de auditoría*	Control Se deben producir y guardar, por un periodo acordado, los registros de auditoría que registran las actividades de los usuarios, excepciones y eventos de seguridad, con el fin de asistir a investigaciones futuras y al monitoreo del control de acceso.
A.10.10.2	*Uso del sistema de monitoreo*	Control Se deben establecer procedimientos para monitorear las instalaciones de procesamiento de información y los resultados del monitoreo de actividades deben ser revisados regularmente.
A.10.10.3	*Protección de la información de registro*	Control Las instalaciones e información de registro debe ser protegido contra acceso forzado y no autorizado.
A.10.10.4	*Registros de administrador y operador*	Control Las actividades del administrador y operadores deben ser registradas.
A.10.10.5	*Registros con faltas*	Control Las faltas deben ser registradas, analizadas y se deben tomar acciones apropiadas.
A.10.10.6	*Sincronización de reloj*	Control Los relojes de todos los sistemas relevantes de procesamiento de información dentro de la organización deben estar sincronizados con una fuente de tiempo actual acordado.

4.2.2.7. Control de accesos

Establece la importancia de monitorear y controlar el acceso a la red y los recursos de aplicación como protección contra los abusos internos e intrusos externos.

El control de accesos requiere ejecutar 25 controles:

A.11 Control de accesos

A.11.1 Requisitos de negocio para el control de accesos *Objetivo de control:* Controlar los accesos a la información.		
A.11.1.1	*Política de control de accesos*	Control Se debe establecer, documentar y revisar una política de control de accesos, basado en requisitos de acceso de seguridad y del negocio.

A.11.2 Gestión de acceso de usuarios *Objetivo de control:* Asegurar que el acceso de usuarios es autorizado y prevenir el acceso no autorizado a los sistemas de información.		
A.11.2.1	*Registro de usuarios*	Control Habrá un procedimiento de registro y anulación formal de usuarios para otorgar y eliminar el acceso a todos los servicios y sistemas de información.
A.11.2.2	*Gestión de privilegios*	Control Se restringirá y controlará la asignación y uso de privilegios.
A.11.2.3	*Gestión de contraseñas de usuario*	Control Se controlará la asignación de contraseñas a través de un proceso de gestión formal.
A.11.2.4	*Revisión de los derechos de acceso de los usuarios*	Control La gerencia conducirá un proceso formal y de manera periódica para revisar los derechos de acceso del usuario.

A.11.3 Responsabilidades de los usuarios *Objetivo de control:* Prevenir el acceso no autorizado de usuarios y el compromiso o robo de la información o de las instalaciones de procesamiento.		
A.11.3.1	*Uso de contraseñas*	Control Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas.
A.11.3.2	*Equipo informático de usuario desatendido*	Control Se exige al usuario que asegure protección adecuada a un equipo desatendido.
A.11.3.3	*Política de pantalla y escritorio limpio*	Control Se debe adoptar una política de escritorio limpio para papeles y dispositivos de almacenamiento removibles. Igualmente, se debe adoptar una política para las instalaciones de procesamiento de información.

A.11.4 Control de acceso a la red *Objetivo de control:* Prevenir el acceso no autorizado a los servicios de red.		
A.11.4.1	*Política de uso de los servicios de la red*	Control Los usuarios deben tener acceso directo únicamente a los servicios cuyo uso está específicamente autorizado.
A.11.4.2	*Autenticación de usuarios para conexiones externas*	Control Deben usarse apropiados métodos de autenticación para controlar el acceso de usuarios remotos.
A.11.4.3	*Autenticación de equipos en la red*	Control Se debería considerar equipos con identificación automática para autentificar conexiones desde ubicaciones y equipos específicos.
A.11.4.4	*Protección para la configuración de puertos y diagnóstico remoto*	Control Debe controlarse la seguridad en el acceso lógico y físico para el diagnóstico y configuración de puertos.
A.11.4.5	*Segregación en las redes*	Control Los grupos de servicios, usuarios y sistemas de información deben ser segregados en las redes.
A.11.4.6	*Control de conexión a las redes*	Control La capacidad de conexión de los usuarios de redes compartidas, especialmente aquellas que se extienden fuera de las fronteras de la organización, debe restringirse de conformidad con la política de control de acceso y los requisitos de las aplicaciones de negocio (véase 11.1).
A.11.4.7	*Control de enrutamiento en la red*	Control Se deben implementar controles de ruteo para asegurar que las conexiones de computadora y los flujos de información no violen la política de control de acceso de las aplicaciones de negocios.

A.11.5 Control de acceso al sistema operativo *Objetivo de control:* Prevenir accesos no autorizados a los sistemas operativos.		
A.11.5.1	*Procedimientos seguros de conexión*	Control Se usará un proceso de registro de conexión (login) seguro para acceder a los servicios de información.
A.11.5.2	*Identificación y autenticación del usuario*	Control Todos los usuarios tienen un identificador único para su uso propio y exclusivo para sus actividades y debe elegirse una técnica de autenticación adecuada para sustentar la identidad del usuario.
A.11.5.3	*Sistema de gestión de contraseñas*	Control Sistemas de gestión de contraseñas proveerán medios efectivos e interactivos, cuyo objetivo es asegurar contraseñas de calidad.
A.11.5.4	*Uso de los programas utilitarios del sistema*	Control Se debe registrar y controlar firmemente el uso de programas utilitarios que puedan ser capaces de forzar el sistema y los controles de aplicación.
A.11.5.5	*Desconexión automática de terminales*	Control Las sesiones inactivas deben cerrarse luego de un periodo definido de inactividad.
A.11.5.6	*Limitación del tiempo de conexión*	Control Se usará restricciones de tiempos de conexión para ofrecer seguridad adicional para las aplicaciones de alto riesgo.
A.11.6 Control de acceso a las aplicaciones e información *Objetivo de control:* Evitar el acceso no autorizado a la información contenida en los sistemas.		
A.11.6.1	*Restricción de acceso a la información*	Control El acceso a las funciones de información y de aplicación por usuarios y personal de soporte serán restringidos con la política de control de acceso.
A.11.6.2	*Aislamiento de sistemas sensibles*	Control Los sistemas sensibles tendrán un ambiente de computo dedicado (aislado).

A.11.7 Informática móvil y teletrabajo *Objetivo de control:* Garantizar la seguridad de la información cuando se usan dispositivos de informática móvil y facilidades de teletrabajo.		
A.11.7.1	*Informática y comunicaciones móviles*	Control Se pondrá en práctica una política formal y se adoptarán los controles adecuados para protegerse frente a los riesgos de trabajar con puntos de computadores móviles y medios de comunicación.
A.11.7.2	*Teletrabajo*	Control Se desarrollarán e implementaran políticas, procedimientos y estándares para las actividades de teletrabajo.

4.2.2.8. Desarrollo y Mantenimiento de los Sistemas

Recuerda que en toda labor de la tecnología de la información, se debe implementar y mantener la seguridad mediante el uso de controles de seguridad en todas las etapas del proceso.

La adquisición, desarrollo y mantenimiento de sistemas requiere ejecutar 16 controles:

A.12 Adquisición de sistemas de información, desarrollo y mantenimiento

***A.12.1 Requisitos de seguridad de los sistemas* de información** *Objetivo de seguridad:* Garantizar que la seguridad esté incluida dentro de los sistemas de información.		
A.12.1.1	*Análisis y especificación de los requisitos de seguridad*	Control Los requisitos de negocios para nuevos sistemas, o ampliaciones de los sistemas existentes, especificarán los requisitos de control.

A.12.2 Proceso correcto en aplicaciones *Objetivo de control:* Prevenir errores, pérdidas, modificaciones no autorizadas o mal uso de los datos del usuario en las aplicaciones.		
A.12.2.1	*Validación de los datos de entrada*	Control Se validará el ingreso de datos a los sistemas de aplicación para asegurar que sean correctos y adecuados.
A.12.2.2	*Control del proceso interno*	Control Se incorporarán verificaciones y validaciones para detectar cualquier corrupción de los datos procesados.
A.12.2.3	*Integridad de mensajes*	Control Se deben identificar requisitos para la autenticación y protección de la integridad de mensajes. Igualmente, se deben implementar e identificar controles apropiados.
A.12.2.4	*Validación de los datos de salida*	Control Los datos de salida de una aplicación se validarán para garantizar que el procesamiento de la información almacenada sea correcto y adecuado a las circunstancias.

A.12.3 Controles criptográficos *Objetivo de control:* Proteger la confidencialidad, autenticidad o integridad a través de medios criptográficos.		
A.12.3.1	*Política de uso de los controles criptográficos*	Control Debe desarrollarse e implementarse una política sobre el uso de controles criptográficos para proteger la información.
A.12.3.2	*Gestión de claves*	Control Se usará un sistema de gestión de claves con el fin de apoyar el uso de técnica criptográficas dentro de la organización.

A.12.4 Seguridad de los archivos del sistema *Objetivo de control:* Asegurar la seguridad de los archivos del sistema.		
A.12.4.1	*Control del software en producción*	Control Se pondrá en práctica procedimientos para controlar la implementación del software en sistemas operacionales.
A.12.4.2	*Protección de los datos de prueba del sistema*	Control Se protegerán y controlarán los datos de prueba los cuales deben ser seleccionados cuidadosamente.

A.12.4.3	*Control de acceso a la librería de programas fuente*	Control El acceso a las librerías de programas fuente debe ser restringido.

A.12.5 Seguridad en los procesos de desarrollo y soporte *Objetivo de control:* Mantener la seguridad del software de aplicación y la información.		
A.12.5.1	*Procedimientos de control de cambios*	Control La implementación de cambios se controlará estrictamente mediante el uso de procedimientos formales de control de cambios.
A.12.5.2	*Revisión técnica de los cambios en el sistema operativo*	Control Cuando los sistemas operativos son cambiados, se deben de revisar y probar las aplicaciones criticas de negocio con el fin de asegurar que no existan impactos adversos en las operaciones o seguridad de la organización.
A.12.5.3	*Restricciones en los cambios a los paquetes de software*	Control No se debe fomentar las modificaciones en los paquetes. Se debe limitar a cambios necesarios y todos estos cambios deben ser estrictamente controlados.
A.12.5.4	*Fuga de información*	Control Se deben de prevenir las oportunidades de fuga de información.
A.12.5.5	*Desarrollo externo del software*	Control La organización debe supervisar y monitorear el desarrollo externo de software.

A.12.6 Gestión de vulnerabilidades técnicas *Objetivo de control:* Reducir los riesgos que son el resultado de la explotación de vulnerabilidades técnicas publicadas.		
A.12.6.1	*Control de vulnerabilidades técnicas*	Control Se debe obtener información a tiempo sobre las vulnerabilidades técnicas de los sistemas de información que se utilizan. La exposición de la organización a tales vulnerabilidades debe ser evaluada y se debe tomar medidas apropiadas asociadas al riesgo.

4.2.2.9 Gestión de Incidentes de Seguridad

Asegurar que los eventos y debilidades en la seguridad de la información sean comunicados de manera que permitan una acción correctiva a tiempo. La gestión de incidentes de la seguridad de la información requiere ejecutar 5 controles:

A.13 Gestión de incidentes en la seguridad de información

A.13.1 Reportando eventos y debilidades en la seguridad de información *Objetivo de control:* Asegurar que los eventos y debilidades en la seguridad de información asociados con los sistemas de información sean comunicados de manera tal que permitan tomar una acción correctiva a tiempo.		
A.13.1.1	*Reportando eventos de la seguridad de información*	Control Los eventos en la seguridad de información deben ser reportados lo mas rápido posible a través de canales apropiados.
A.13.1.2	*Reportando debilidades de seguridad*	Control Todos los empleados, contratistas o personal externo usuario de los sistemas y servicios de información, deben estar obligados de notar y reportar cualquier debilidad en la seguridad de los sistemas y servicios.

A.13.2 Gestión de los incidentes y mejoras en la seguridad de información *Objetivo de control:* Asegurar que un alcance consistente y efectivo sea aplicado en la gestión de incidentes de la seguridad de información.		
A.13.2.1	*Responsabilidades y procedimientos*	Control. Se deben de establecer procedimientos y responsabilidades de gestión con el fin de asegurar una respuesta rápida, efectiva y ordenada ante incidentes en la seguridad de información.
A.13.2.2	*Aprendiendo de los incidentes en la seguridad de información*	Control Deben existir mecanismos que habiliten que los tipos, volúmenes y costos de los incidentes en la seguridad de información sean cuantificados y monitoreados.
A.13.2.3	*Recolección de evidencia*	Control Cuando exista una acción de seguimiento contra una persona u organización, luego de que un incidente en el sistema de información involucre una acción legal (civil o criminal), se debe de recolectar, retener y presentar evidencia conforme con las reglas dentro de la jurisdicción.

4.2.2.10. Gestión de Continuidad del Negocio

Aconseja estar preparado para contrarrestar las interrupciones en las actividades de la organización y para proteger los procesos importantes de la organización en caso de una falla grave o desastre.

La gestión continuidad del negocio requiere ejecutar 5 controles:

A.14 Gestión de la continuidad del negocio

A.14.1 Aspectos de la gestión de continuidad del negocio en la seguridad de información *Objetivo de control:* Neutralizar las interrupciones a las actividades del negocio y proteger los procesos críticos del negocio de los efectos de fallas mayores o desastres en los sistemas de información y asegurar su reanudación oportuna.		
A.14.1.1	*Incluyendo la seguridad de la información en la gestión de la continuidad del negocio*	Control Se deben de establecer procedimientos y responsabilidades de gestión con el fin de asegurar una respuesta rápida, efectiva y ordenada ante incidentes en la seguridad de la información.
A.14.1.2	*Continuidad del negocio y evaluación de riesgos*	Control Los eventos que pueden causar interrupciones en los procesos del negocio deben ser identificados así como las probabilidades e impacto de dichas interrupciones y sus consecuencias para la seguridad de la información.
A.14.1.3	*Desarrollando e implementando planes de continuidad que incluyen la seguridad de la información*	Control Se deben desarrollar e implementar planes para mantener o reparar operaciones y asegurar la disponibilidad de información al nivel y tiempo requerido, siguiendo las interrupciones o fallas a los procesos críticos del negocio.
A.14.1.4	*Marco de planificación de la continuidad del negocio*	Control Un simple marco de los planes de continuidad del negocio debe ser mantenido para asegurar que todos los planes sean consistentes, que anexen consistentemente los requisitos de seguridad de la información, para identificar prioridades de prueba y mantenimiento.
A.14.1.5	*Probando, manteniendo y reevaluando los planes de continuidad del negocio*	Control Los planes de continuidad del negocio deben ser probados y actualizados regularmente con el fin de asegurar que se encuentren actuales y que sean efectivos.

4.2.2.11. Conformidad y Cumplimiento

Evitar brechas de cualquier ley civil o penal, estatutos, obligaciones regulatorias o contractuales y de cualquier requerimiento de seguridad.

La conformidad y cumplimiento legislación requiere ejecutar 10 controles:

A.15 Cumplimiento

A.15.1 Cumplimiento de los requisitos legales *Objetivo de control:* Evitar los incumplimientos de cualquier ley civil o penal, requisito reglamentario, regulación u obligación contractual, y de cualquier requisito de seguridad.		
A.15.1.1	*Identificación de la legislación aplicable*	Control Se definirán y documentarán explícitamente todos los requisitos legales, regulatorios y contractuales relevantes y se deben mantener actualizados cada sistema de información y la organización.
A.15.1.2	*Derechos de propiedad intelectual (DPI)*	Control Se implementarán procedimientos adecuados para garantizar el cumplimiento de las restricciones legales en el uso de material con respecto a derechos de propiedad intelectual y uso de productos de software propietario.

A.15.1.3	*Salvaguarda de los registros de la organización*	Control Se protegerán los registros importantes de la organización frente a pérdidas, destrucción y falsificación en concordancia con los requisitos regulatorios, contractuales y de negocio.
A.15.1.4	*Protección de los datos y privacidad de la información personal*	Control Se aplicarán controles para proteger información personal en conformidad con la legislación correspondiente y si es aplicable, con las cláusulas contractuales.
A.15.1.5	*Prevención en el mal uso de las instalaciones de procesamiento de la información*	Control Los usuarios deben ser disuadidos de utilizar las instalaciones del procesamiento de información para propósitos no autorizados.
A.15.1.6	*Regulación de los controles criptográficos*	Control Se implementarán controles para permitir el cumplimiento de los acuerdos nacionales, leyes y reglamentos.

A.15.2 Cumplimiento con las políticas y estándares de seguridad y del cumplimiento técnico *Objetivo de control:* Asegurar el cumplimiento de los sistemas con las políticas y normas de seguridad organizacionales.		
A.15.2.1	*Cumplimiento con los estándares y la política de seguridad*	Control Los gerentes deben tomar acciones para garantizar que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se lleven a cabo correctamente con el fin de garantizar el cumplimiento de las políticas y estándares de seguridad.
A.15.2.2	*Comprobación del cumplimiento técnico*	Control Debe verificarse regularmente el cumplimiento de la implementación de normas de seguridad en los sistemas de información.

A.15.3 Consideraciones sobre la auditoría de sistemas *Objetivo de control:* Maximizar la efectividad y minimizar las interferencias en el proceso de auditoría del sistema.		
A.15.3.1	*Controles de auditoría de sistemas*	Control Se planificarán cuidadosamente las auditorías de los sistemas operacionales a fin de minimizar el riesgo de interrupciones a los procesos de negocio.
A.15.3.2	*Protección de las herramientas de auditoría de sistemas*	Control Se protegerá el acceso a las herramientas de auditoría del sistema para prevenir cualquier posible mal uso o daño.

4.2.3. Verificar

Con el fin de gestionar los riesgos de una manera segura, FNDR puede ver su perfil cibernético a través de los componentes del control interno del Marco Integrado de COSO.

El uso de un lente de qué datos es más importante para una organización, la gerencia debe invertir en los controles de seguridad, costo justificado para proteger sus activos más importantes.

La evaluación del riesgo conduce a la asignación de recursos de la entidad en contra de las actividades de control que previenen, detectan y gestionan los riesgos informáticos.

Las evaluaciones de riesgo deben actualizarse de forma continua para proteger sus SI más críticos.

Se deben verificar la efectividad de los controles: preventivos, detectivos y correctivos.

4.2.4. Actuar

Para finalizar un proceso de Auditoría para la seguridad de Sistemas de Información bajo el modelo ISO 27000, se debe presentar un informe que contenga conclusiones y recomendaciones, necesarias para que el FNDR este en mejoramiento

continuo, esta documentación debe ser redactada por el equipo de Auditoría y entregarse a la Alta Dirección de la empresa para su evaluación y análisis.

A manera de ejemplo, el informe de auditoría, bajo la NAG 270, en base a la cuarta norma que es EVIDENCIA utilizando los atributos: condición, criterio, causa y efecto, se propone la siguiente recomendación

RECOMENDACIONES PARA LA SEGURIDAD FÍSICA DEL CENTRO DE CÓMPUTO

Condición

Como resultado de la evaluación de seguridad física realizada al Centro de Cómputo de la Entidad, se observó que el Data Center al ser un activo informático, no se ubica en un lugar adecuado para garantizar la seguridad de los equipos donde residen los sistemas del Programa.

Criterio

De acuerdo con la metodología propuesta, en el punto **4.2.2.5. Seguridad física y del Entorno,** hace referencia que la seguridad física y del entorno, responde a la necesidad de proteger las áreas, el equipo y los controles generales.

La seguridad física y del entorno requiere ejecutar controles, en su apartado **A.9.1 Áreas seguras**, tiene como objetivo de control: prevenir accesos no autorizados, daños e interferencias contra los locales y la información de la organización. En **A.9.1.1. y A.9.1.2**. se ejecutan controles de seguridad física perimetral y controles físicos respectivamente.

De acuerdo con la ISO 27002, en su apartado 9.2.1 "Ubicación y protección del equipamiento", los equipos deben ser ubicados y protegidos para reducir los riegos ocasionados por amenazas y peligros ambientales y oportunidades de accesos no autorizados.

Asimismo, el Estándar TIA-914 se encarga de brindar los requerimientos y lineamientos necesarios para el diseño e instalación del Data Center.

La aplicación de infraestructura con componentes redundantes (TIER II), infraestructura con mantenimiento simultaneo (TIER III) e infraestructura tolerante a fallos (TIER IV) deben ser considerados a la hora de implementar un Data Center.

Causa

Este aspecto no fue considerado con anterioridad.

Efecto

El no contar con infraestructura adecuada reduce las medidas de seguridad básicas de protección del equipamiento, incrementa el riesgo de que se generen

accesos no autorizados a la información y que los equipos puedan sufrir amenazas físicas y ambientales las cuales deriven en la interrupción de las operaciones del programa por falta de los sistemas de información.

Recomendación

Debería considerarse que el ambiente de procesamiento de datos cuente con las siguientes medidas como ser:

- Compañías que dan soporte 24/7;
- Servicios 24x365;
- Manejo térmico;
- Software de administración de infraestructura física diseñada como solución integral;
- Detección y supresión de incendios;
- Generadores de energía
- Cajas ignifugas, para el resguardo de los medios de almacenamiento removibles (tales como cintas, discos ópticos, etc.)
- Armarios especiales con algún tipo de dispositivo de cierre;
- Monitoreo y personal de seguridad 7x24;
- Acceso restringido a través de tarjetas de proximidad y sensores biométricos de huella, temperatura corporal y de iris;
- Resguardo físico por vidrios anti-balas nivel 7 y puertas de acero;
- Sistemas de detección de intrusos;
- Sistemas de análisis de seguridad de activos.

Comentario de la Entidad:

CAPITULO V.

Conclusiones y Recomendaciones

5.1. Conclusiones

Cada día se escuchan incidentes de inseguridad relacionadas a Tecnología de Información, a falta de un referente metodológico. El trabajo de Proyecto de Grado está orientado al desarrollo de un método de Auditoria para la seguridad de Sistemas de Información bajo el modelo ISO 27000 aplicable al Fondo Nacional de Desarrollo Regional (FNDR) cumpliendo normas y procedimientos generalmente aceptados.

Este método está dirigida a ejecutar controles efectivos, que luego, permita emitir una opinión profesional sobre el estado de TI y tomar las acciones preventivas, detectivas y correctivas adecuadas con el fin de minimizar errores. Este método esta adecuado a la realidad de nuestro país. Prueba de ello es la aplicación de la NAG 270 y los componentes de control Interno del Marco Integrado de COSO

Es importante resaltar que cada vez que se incorpora una nueva herramienta o negocio de TIC a la entidad se debe actualizar el análisis de riesgos para poder mitigar de forma responsable los riesgos y, por supuesto, considerando la regla básica de Riesgo de TI *vs.* Control *vs.* Coste, es decir, minimizar los riesgos con medidas de control ajustadas y considerando los costes del control.

La metodología propuesta, contribuye a fomentar las actividades de protección de la información en el Fondo Nacional de Desarrollo Regional (FNDR), mejorando su seguridad de la información, su imagen y generando confianza frente a terceros.

- ✓ La metodología propuesta, cumple con los objetivos planteados;
- ✓ La seguridad de la información se basa en las personas;
- ✓ Las personas responsables de seguridad de la información del FNDR, al utilizar la metodología, podrán evaluar el contenido de las diferentes actividades y aplicar los controles que considere necesario en forma sistemática y disciplinada.

5.2. Recomendaciones

El hecho de que hasta hoy, no se aplique métodos de auditoría para la seguridad de los SI bajo el paraguas de la ISO 27000, no significa que con la aplicación de este método, se garantice la gobernabilidad efectiva de la información. Todo dependerá del cambio de actitud cultural de los diferentes actores de la institución.

La auditoría a Sistemas de Información, bajo estándares internacionales, es relativamente nueva. Por lo que se sugiere las siguientes recomendaciones:

- ✓ La primera que debo recomendar es la de actualización del trabajo. Parece obvio que en poco tiempo los sistemas y dispositivos de los que se habla en este trabajo quedarán desfasados, ya que debido a la alta demanda, la tecnología informática y de seguridad avanza a pasos agigantados.
- ✓ Las organizaciones deben definir una estrategia de seguridad basada en el negocio y no en la tecnología.
- ✓ El enfoque de la Seguridad debe ser integral, si no puede conducir a una falsa sensación de seguridad y al fracaso.
- ✓ También se podría profundizar en cualquiera de los puntos tratados en este trabajo, como las copias de seguridad, los incendios, la energía eléctrica, etc., ya que todos los aspectos se tratan de una manera general.
- ✓ Se recomienda que a la metodología propuesta, se pueda insertar en futuros estudios la parte legal, como el derecho informático.
- ✓ En futuros trabajos se recomienda implementar la ISO 30000 e ISO 31000
- ✓ Se debe profundizar en la investigación de temas relativos a la seguridad, aplicando criptografía, cableado estructurado;
- ✓ Se debe tomar conciencia de parte de las autoridades, que los ambientes donde se procesa información cuente con un plan de contingencias, que este contemplado como objetivos generales de la institución.

Referencias bibliográficas

AENOR *Sistemas de gestión de la calidad*. ISO 9001-2000. Madrid: AENOR, 2000.

[Hernández 2005] Hernández, R., 2005: Metodología de la Investigación, 505 pp. Editorial McGraw-Hill.

IBNORCA Norma boliviana NB-ISO-IEC 27001-07 “Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de seguridad.

IRAM/ISO/IEC Julio 2005. Proyecto 1 de norma Argentina. Código de práctica para la gestión de la seguridad de la información. Basada en ISO/IEC Estándar 17799: Information Technology – Code of Practice for Information Security.

ISO Information technology - Code of practice for information security management. ISO-IEC 17799-2000. Switzerland: ISO, 2005.

En línea:

http://ciberconta.unizar.es/LECCION/SEGURO/inicio.html

[Acceso, Agosto 2015] Riesgos y seguridad en los sistemas de información. Auditoría informática.

[Acceso, Mayo 2015] El portal de ISO 27000 en español

http://www.iso27000.es/