Universidad Politécnica de Madrid

Escuela Técnica Superior de Ingenieros de Telecomunicación

PLANIFICACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA SU APLICACIÓN EN LA OPERACIÓN DEL SISTEMA NACIONAL DE FINANZAS PÚBLICAS DEL ECUADOR

TRABAJO FIN DE MÁSTER

Rolando Coello Neacato

2015

Universidad Politécnica de Madrid

Escuela Técnica Superior de Ingenieros de Telecomunicación

Máster Universitario en
Ingeniería de Redes y Servicios Telemáticos

TRABAJO FIN DE MÁSTER

PLANIFICACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA SU APLICACIÓN EN LA OPERACIÓN DEL SISTEMA NACIONAL DE FINANZAS PÚBLICAS DEL ECUADOR

Autor

Rolando Coello Neacato

Director

Victor A. Villagra

Departamento de Ingeniería de Sistemas Telemáticos

2015

Resumen

El presente Trabajo de Fin de Máster plantea el estudio del Esquema Gubernamental Ecuatoriano de Gestión de Seguridad de la Información (EGSI), basado en los estándares internacionales ISO/IEC 27000, y su aplicabilidad en la operación del Sistema Nacional de Finanzas Públicas del Ecuador (SINFIP).

El estudio se enfoca en la planificación de un Sistema de Gestión de Seguridad de la Información SGSI, que incluye lo establecido en el EGSI, para su aplicación en la Dirección Nacional de Operaciones de los Sistemas de Finanzas Públicas del Ministerio de Finanzas del Ecuador.

La planificación incluye la definición del alcance del SGSI, políticas generales de seguridad, análisis y evaluación de riesgos aplicados a los activos gestionados por la Dirección en mención, y finalmente la selección de los objetivos de control y controles aplicables, tomados estos últimos del anexo A de la norma ISO/IEC 27001:2013 y del Anexo 1 del documento del EGSI.

Finalmente se propone un proceso a seguir para la implementación de objetivos de control y controles, y sus respectivos procesos específicos, al interno del Ministerio de Finanzas del Ecuador.

Abstract

This Final Master Project consists on studying the Ecuadorian Governmental Schema for Managing Information Security (EGSI), based on international standard ISO/IEC 27000, and its applicability in the operation of The National System of Public Finance of Ecuador (SINFIP).

The study focuses on planning an Information Security Management System ISMS, including the EGSI guidelines, for applying on the National Direction of Operating National System of Public Finance, belonging this Direction to the Finance Ministry of Ecuador.

The planning includes defining the ISMS scope, general security policies, risk analysis and assessment applied to the assets managed for the aforementioned Direction, and finally, selecting the control objectives and controls from the ISO/IEC 27001:2013 Annex A and EGSI Annex 1.

Finally, the study propose a process to implement control objectives, controls and their respective specific processes, inside the Finance Ministry of Ecuador.

Índice general

Índice de figuras

Índice de tablas

Siglas

EGSI	Esquema Gubernamental de Seguridad de la Información
NTE	Normas Técnicas Ecuatorianas
INEN	Servicio Ecuatoriano de Normalización
ISO	Organización Internacional de Estandarización
IEC	Comisión Electrotécnica Internacional
SINFIP	Sistema Nacional de las Finanzas Públicas del Ecuador
SGSI	Sistema de Gestión de Seguridad de la Información
SLA	Acuerdos de Nivel de Servicio
CMDB	Base de Datos de Gestión de Cambios
UPS	Sistema de alimentación ininterrumpida
IPS	Sistema de Protección de Intrusos
RAC	Cluster de Aplicación Real de Oracle
eSIGEF	Sistema de Gestión Financiera
SPRYN	Sistema Presupuestario de Remuneraciones y Nómina
eSByE	Sistema de Bienes y Existencias
TI	Tecnologías de la Información
ISMS	Sistema de Gestión de Seguridad de la Información (siglas en inglés)
PDCA	Plan, Do, Check, Act
MAGERIT	Metodología de Análisis y Gestión de Riesgos elaborada por el Consejo Superior de Administración Electrónica
CMMI	Integración de modelos de madurez de capacidades

1 Introducción

La Secretaría Nacional de la Administración Pública de la República del Ecuador, tiene como sus atribuciones el impulsar proyectos de estandarización en procesos, calidad y tecnologías de la información y comunicación, acorde a lo estipulado en el artículo 15, letra i) del Estatuto del Régimen Jurídico y Administrativo de la Función Ejecutiva.

Mediante Acuerdos Ministeriales Nos. 804 y 837 de 29 de julio y 19 de agosto de 2011, respectivamente, la Secretaría Nacional de la Administración Pública crea la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación, para que establezca lineamientos de seguridad informática, protección de infraestructura computacional y todo lo relacionado con esta, incluyendo la información contenida para las entidades de la Administración Pública Central e Institucional del Ecuador.

La Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación desarrolló el Esquema Gubernamental de Seguridad de la Información (EGSI), elaborado en base a las normas NTE INEN-ISO/IEC 27000.

Mediante Acuerdo Ministerial No. 166 del 25 de septiembre de 2013, la Secretaría Nacional de la Administración Pública dispone a las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información. En su artículo 2 se dispone la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI), que se realizará en cada institución de acuerdo al ámbito de acción, estructura orgánica, recursos y nivel de madurez en gestión de Seguridad de la Información.

El Esquema Gubernamental de Seguridad de la Información (EGSI), está basado en la norma técnica ecuatoriana INEN ISO/IEC 27002 para Gestión de la Seguridad de la Información y está dirigido a las Instituciones de la Administración Pública Central, Dependiente e Institucional.

El EGSI establece un conjunto de directrices prioritarias para Gestión de la Seguridad de la Información e inicia un proceso de mejora continua en las instituciones de las Administración Pública. El EGSI no reemplaza a la norma INEN ISO/IEC 27002 sino que marca como prioridad la implementación de algunas directrices [14].

Para cumplir con lo dispuesto, el presente trabajo propone la planificación de un Sistema de Gestión de Seguridad de la Información, que considere los requisitos establecidos en el estándar internacional ISO/IEC 27001 y las directrices estipuladas en el documento del EGSI, para su aplicación en el área encargada de la operación de los sistemas de finanzas públicas del Ecuador. A continuación se detallan los objetivos, ámbito de aplicación y estructura del presente trabajo.

1.1 Objetivos propuestos

Los objetivos propuestos son:

- Realizar el estudio de la familia de estándares internacionales ISO/IEC 27000, concretamente el estándar internacional ISO/IEC 27001:2013 y su relación con el documento de Esquema Gubernamental de Seguridad de la Información EGSI elaborado por la Secretaría Nacional de la Administración Pública del Ecuador.
- Realizar la planificación de un Sistema de Gestión de Seguridad de la Información, considerando los requisitos del estándar internacional ISO/IEC 27001:2013 y las directrices del documento del EGSI, aplicado al área encargada de la operación de los sistemas de finanzas públicas del Ecuador.
- Seleccionar objetivos de control y definir controles, de los sugeridos en el anexo A del estándar internacional ISO/IEC 27001:2013 así como en el documento del EGSI, para que formen parte del Sistema de Gestión de Seguridad de la Información.
- Proponer un proceso general de implementación de objetivos de control y controles.

1.2 Ámbito de estudio

Como se mencionó antes, la planificación del Sistema de Gestión de Seguridad de la Información se realizará tomando como escenario el área encargada de la operación de los sistemas de finanzas públicas del Ecuador. Esta área pertenece al Ministerio de Finanzas del Ecuador y se denomina Dirección Nacional de Operaciones de los Sistemas de las Finanzas Públicas.

1.3 Estructura del documento

El presente documento de trabajo de fin de máster está estructurado de la siguiente forma:

En el capítulo 2 se realiza una descripción del área de la entidad pública que sirve de escenario para la planificación del Sistema de Gestión de Seguridad de la Información. Concretamente se describen la misión, responsabilidades, productos y procesos principales de la Dirección Nacional de Operaciones de los Sistemas de Finanzas

Públicas, además del entorno que le rodea, dentro del Ministerio de Finanzas del Ecuador.

En el capítulo 3 se realiza una revisión general de la familia de estándares internacionales ISO/IEC 27000, además de exponer las definiciones y aspectos importantes acerca de seguridad de la información, sistema de gestión de seguridad de la información SGSI y del estándar internacional ISO/IEC 27001:2013.

EL capítulo 4 trata sobre una revisión del Esquema Gubernamental de Seguridad de la Información, propuesto por la Secretaría Nacional de la Administración Pública del Ecuador y que debe aplicarse en las entidades públicas ecuatorianas. Se describe sus fundamentos y relación con los estándares ISO/IEC 27000.

En el capítulo 5, que es el estudio en sí, se realiza la planificación del sistema de gestión de seguridad de la información, para su aplicación en la Dirección Nacional de Operaciones de los Sistemas de Finanzas Públicas del Ecuador, planificación que incluye un análisis y evaluación de riesgos para con esta información definir los objetivos de control y controles a ser implementados.

El capítulo 6 propone un proceso que se seguiría, dentro del ámbito del Ministerio de Finanzas del Ecuador, para iniciar la implementación de los objetivos de control y controles definidos en el capítulo 5. En este proceso propuesto, se muestran las diferentes áreas que deben participar.

En el capítulo 7 se exponen las conclusiones al presente trabajo, además de mencionar los trabajos futuros que se pueden realizar a partir de este estudio.

2 Descripción de la Entidad Pública de estudio

Mediante Acuerdo Ministerial No. 254 del 23 de noviembre de 2011, el Ministerio de Finanzas del Ecuador emite su estatuto orgánico por procesos, en donde se definen la misión, visión, objetivos y su estructura básica [10].

La misión del Ministerio de Finanzas es "Contribuir al cumplimiento de los objetivos de desarrollo del país y a una mejor calidad de vida para las y los ecuatorianos, a través de una eficaz definición, formulación y ejecución de la política fiscal de ingresos, gastos y financiamiento público, que garantice la sostenibilidad, estabilidad, equidad y transparencia de las finanzas públicas.

La visión del Ministerio de Finanzas es "Ser el ente rector de las finanzas públicas, reconocido como una entidad moderna orientada a brindar servicios públicos con calidad y oportunidad a nuestros clientes; integrado por un equipo de personas competentes y comprometidas con la ética, probidad, responsabilidad, transparencia y rendición de cuentas.

La estructura básica alineada a la misión es:

Procesos Gobernantes: Despacho ministerial de finanzas públicas, Viceministerio de finanzas públicas.

Procesos agregadores de valor relacionados con el diseño, desarrollo, operación y mantenimiento de aplicativos y servicios informáticos que soportan al Sistema Nacional de las Finanzas Públicas: Gestión de innovación de las finanzas públicas.

La Gestión de innovación de las finanzas públicas se divide en los siguientes procesos: Gestión nacional de innovación conceptual y normativa, Gestión nacional de sistema de información de las finanzas públicas, Gestión nacional de operaciones de los sistemas de las finanzas públicas y Gestión nacional del centro de servicios.

2.1 Gestión de innovación de las finanzas públicas

El Acuerdo Ministerial No. 254 del 23 de noviembre de 2011 establece como misión de la Subsecretaría de Innovación de las Finanzas Públicas el "innovar de manera permanente los conceptos, metodologías, procesos, tecnologías y servicios inherentes al Sistema Nacional de las Finanzas Públicas (SINFIP), para contribuir a una mayor eficiencia y efectividad en la gestión de las finanzas públicas" [10].

Las atribuciones y responsabilidad de la Subsecretaría de Innovación son:

- Impulsar e implantar las iniciativas de innovación y modernización del Sistema Nacional de las Finanzas Públicas.
- Promover que la innovación conceptual de las finanzas públicas vaya alineada a las nuevas tecnologías de información.
- Planificar, definir estrategias, administrar y optimizar el Sistema de Administración Financiera y todas sus aplicaciones.
- Planificar, promover, supervisar y ejecutar la entrega eficiente de los servicios que el Sistema Nacional de las Finanzas Públicas ofrece a los usuarios internos y externos.
- Establecer relaciones estratégicas con otras entidades públicas para integrar procesos comunes.
- Proveer a los funcionarios públicos capacitación y asistencia técnica, conceptual y operativa en finanzas públicas y en el uso del Sistema de Administración Financiera y todas sus aplicaciones.
- Gestionar el portafolio de proyectos de la subsecretaría y su ejecución.
- Realizar análisis y planificación de gestión de riesgos y seguridad de la información.
- Administrar el sistema oficial de la información de las finanzas públicas y su amplia difusión.
- Las demás previstas en las leyes y reglamentos que rigen la materia; y, las que le delegue la autoridad.

La Subsecretaría de Innovación está conformada por cuatro Direcciones nacionales:

- Dirección nacional de Innovación conceptual y normativa
    - Misión: Innovar, investigar, proponer e implantar conceptos, metodologías, procedimientos, soluciones y normas para todos los componentes del Sistema nacional de las Finanzas Públicas.
- Dirección nacional de sistemas de información de las finanzas públicas
    - Misión: Innovar e implementar nuevas tecnologías de información y garantizar la operación de los sistemas de información existentes para todos los componentes del Sistema nacional de las Finanzas Públicas.
- Dirección nacional de operaciones de los sistemas de las finanzas públicas
    - Misión: Garantizar la operación, seguridad y disponibilidad de la infraestructura tecnológica que soporta a las aplicaciones de software del Sistema Nacional de las Finanzas Públicas en cumplimiento a los acuerdos de niveles de servicio establecidos.
- Dirección nacional de centro de servicios
    - Misión: Proveer los servicios de asistencia técnica, conceptual y operativa en finanzas públicas a funcionarios públicos de otras instituciones y a la ciudadanía, impulsando la transformación de la

administración pública orientada al servicio y haciendo uso de las tecnologías de información.

La figura 1 muestra la estructura orgánica funcional del Ministerio de Finanzas del Ecuador, donde se puede visualizar la posición de la Subsecretaría de Innovación de la Finanzas Públicas y sus Direcciones nacionales, una de las cuales será el escenario de estudio para la planificación de un sistema de gestión de seguridad de la información.

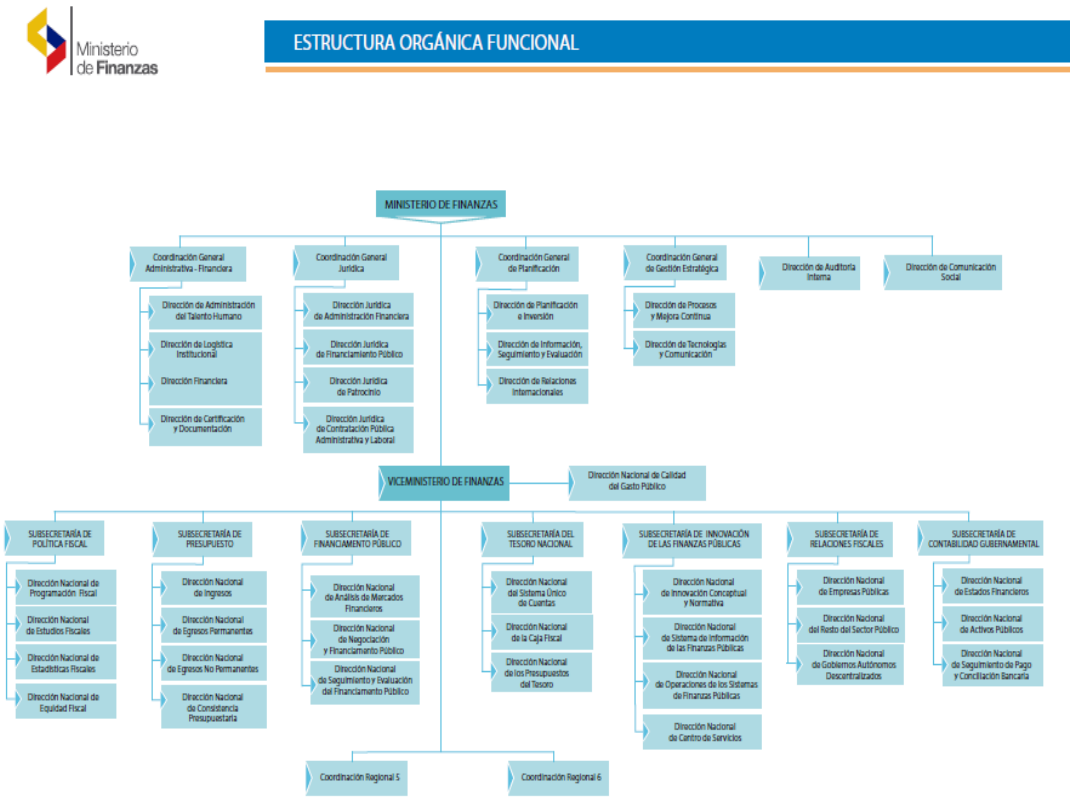

Figura 1. Estructura orgánica funcional del Ministerio de Finanzas

2.2 Escenario del caso de estudio

El estudio para la aplicación del SGSI se enfocará en el ámbito de la Dirección Nacional de Operaciones de los Sistemas de las Finanzas Públicas, dado que se establece en su misión el garantizar entre otros aspectos la seguridad de la infraestructura tecnológica que soporta a los aplicativos de software del SINFIP [10]. Por tanto, a continuación se detallan las atribuciones responsabilidades y productos de la mencionada Dirección:

- Garantizar que la infraestructura de tecnología de información satisfaga las necesidades de negocio del SINFIP y los requerimientos técnicos de las aplicaciones.

- Promover y garantizar el uso del marco de referencia para el diseño y operación de los servicios para reducir el riesgo, mejorar la calidad y asegurar la exactitud de las cargas de trabajo estimadas.
- Gestionar la disponibilidad, capacidad, continuidad de operaciones, seguridad e instalaciones de tecnología de información y de los sistemas del SINFIP.
- Participar en la definición de SLAs.
- Administrar la plataforma de hardware y software base.
- Administrar la base de datos de gestión de la configuración (CMDB).
- Gestionar los problemas, cambios, configuraciones y versionado de plataforma.
- Monitorear las operaciones y la producción de los sistemas.
- Gestionar riegos y seguridad de infraestructura tecnológica de información y de los sistemas del SINFIP.
- Coordinar la entrega de servicios con las otras direcciones.
- Las demás previstas en las leyes y reglamentos que rigen la materia y, las que le delegue la autoridad.

Los productos de la Dirección nacional de operaciones de los sistemas de las finanzas públicas son:

- Portafolio de servicios de tecnología de la información.
- Plan, políticas y reportes de seguridad de infraestructura.
- Plan, líneas de base, umbrales, alarmas y base de datos de la capacidad de infraestructura.
- Planes de continuidad y recuperaciones de operaciones/tecnología de información.
- Plan de reducción del riesgo.
- Plan, diseño y calendarios de la disponibilidad/recuperación.
- Plan de mantenimiento de las instalaciones.
- Base de datos de gestión de la configuración actualizada.
- Informe de administración técnica de los contratos.

La figura 2 muestra la estructura funcional de la Dirección Nacional de Operaciones de los Sistemas de Finanzas Públicas, en donde está enfocado el presente estudio de planificación del SGSI.

Figura 2. Estructura funcional de la Dirección Nacional de Operaciones de los Sistemas de Finanzas Públicas

Tomando como referencia las atribuciones de la Dirección, esta se encarga de la gestión de la plataforma de hardware y software base, que soporta la provisión de los servicios y aplicativos web del SINFIP. En base a esta premisa se crea su estructura funcional actual, expuesta en la figura 2.

2.2.1 Infraestructura de TI

El área de Infraestructura de TI tiene como responsabilidad la gestión de la infraestructura tecnológica, que soporta a los aplicativos y servicios web del SINFIP, compuesta de las siguientes plataformas e instalaciones:

- Instalaciones de Centro de Datos
  - Sistema de alimentación eléctrica
  - Sistemas UPS redundantes
  - Generadores eléctricos redundantes
  - Sistema de Aires Acondicionados de precisión redundantes
  - Sistema de Detección y Extinción de incendios
  - Sistema de control de acceso biométrico
  - Sistema de video vigilancia IP
- Plataforma de Aprovisionamiento de Recursos
  - Servidores Blade
  - Almacenamiento Externo
  - Hipervisor Hyper-V de Microsoft
  - Sistemas Operativos: Microsoft Windows 2012 Server, Linux Red Hat
  - Antivirus
- Plataforma de Respaldos
  - Librería Virtual
  - Librería Física (cintas de respaldo)

La figura 3 muestra de forma general la infraestructura tecnológica gestionada por el área en mención:

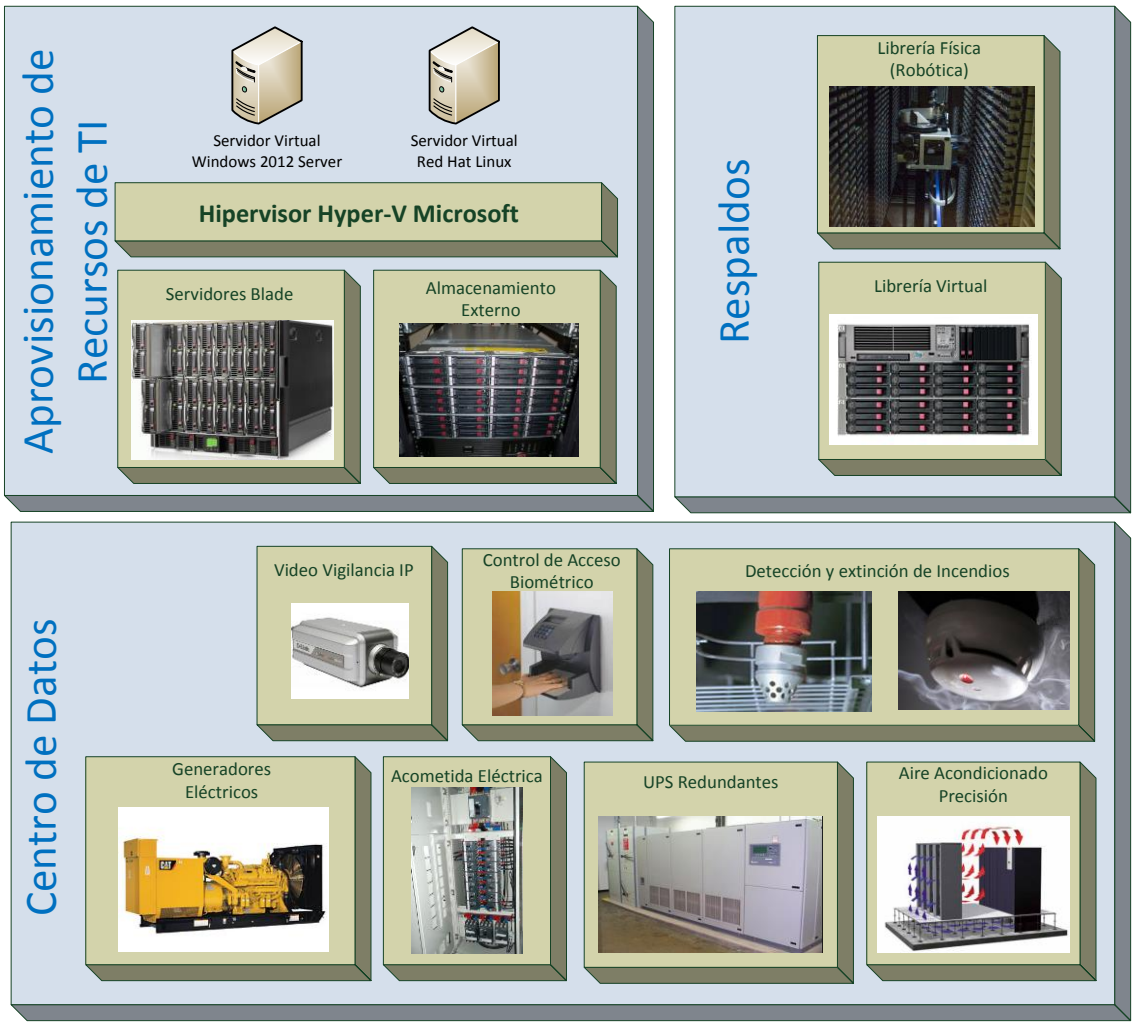

Figura 3. Infraestructura tecnológica de centro de datos, aprovisionamiento de recursos de TI y respaldos

2.2.2 Redes, Comunicaciones y Seguridades

El área de Redes, Comunicaciones y Seguridades tiene como responsabilidad la gestión de la infraestructura tecnológica de comunicaciones y seguridades de red, que proporciona el servicio de conectividad y acceso para los aplicativos y servicios web del SINFIP. Esta infraestructura está formada por:

- Plataforma de Switching
- Plataforma de Routing
- Plataforma de Firewall e IPS
- Plataforma de Balanceo de Carga
- Plataforma de Balanceo de IPS

La figura 4 muestra de forma general la infraestructura tecnológica de redes, comunicaciones y seguridad de red, gestionada por el área en mención:

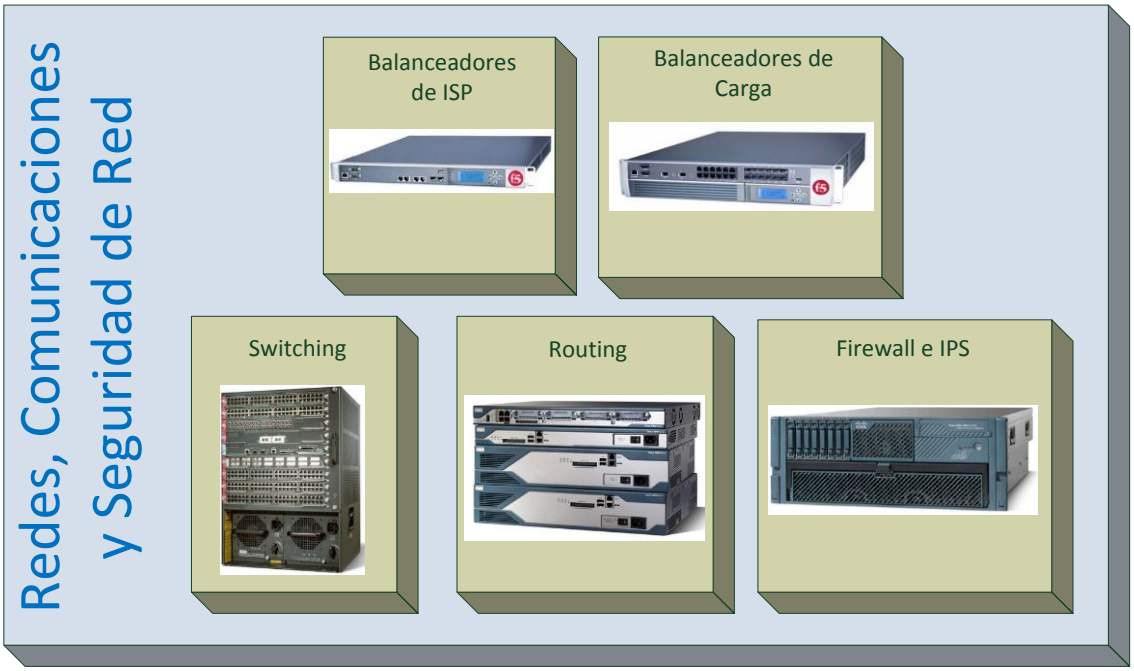

Figura 4. Infraestructura tecnológica de redes, comunicaciones y seguridades de red

2.2.3 Bases de Datos

El área de bases de datos tiene la responsabilidad de gestionar el sistema de Bases de Datos, que constituye una capa transversal para el funcionamiento de todos los aplicativos y servicios web del SINFIP. Este sistema lo conforma una Configuración de Oracle RAC (Oracle Real Application Cluster).

La figura 5 muestra el esquema de configuración del sistema de bases de datos.

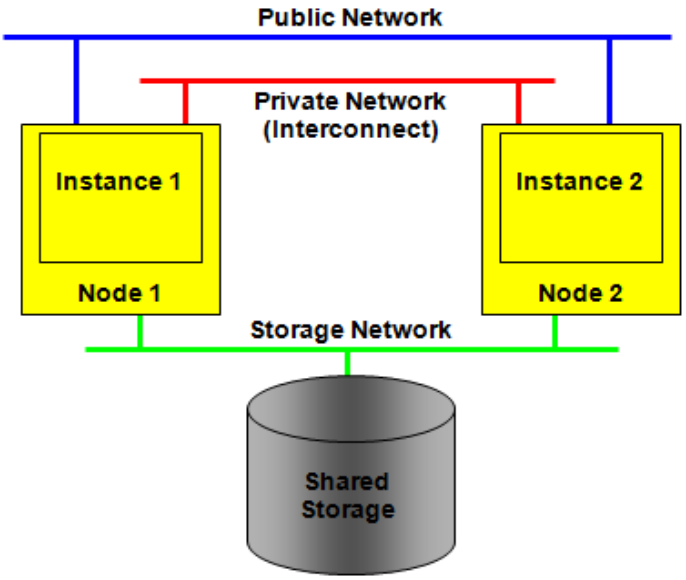

Figura 5. Sistema de Bases de Datos (Cluster)

2.3 Sistema Nacional de Finanzas Públicas del Ecuador (SINFIP)

El SINFIP comprende el conjunto de normas, políticas, instrumentos, procesos, actividades, registros y operaciones que las entidades y organismos del Sector Público del Ecuador, deben realizar con el objeto de gestionar en forma programada los ingresos, gastos y financiamiento públicos, con sujeción al Plan Nacional de Desarrollo y a las políticas públicas establecidas en la Ley [11].

La rectoría del SINFIP corresponde al Presidente de la República de Ecuador, a través del Ministerio de Finanzas, como ente rector. Para cumplir las atribuciones asignadas al Ministerio de Finanzas, como ente rector de las Finanzas Públicas, como son las de dictar las normas, manuales, instructivos, directrices, clasificadores, catálogos, glosarios y otros instrumentos de cumplimiento obligatorio por parte de las entidades del sector público para el diseño, implantación y funcionamiento del SINFIP y sus componentes, realizó el despliegue de los aplicativos web eSIGEF, SPRYN, eSByE, disponibles en Internet, a través de los cuales todas las entidades del sector público gestionan sus ingresos, gastos y financiamiento públicos.

El aplicativo web eSigef proporciona el servicio de programación presupuestaria y evaluación de ejecución a las entidades del sector público. Su interfaz web se muestra en la figura 6.

Figura 6. Interfaz web aplicativo web eSigef

El aplicativo web SPRYN proporciona el servicio de programación presupuestaria de gastos en personal, y la respectiva evaluación de su ejecución a través de la gestión desconcentrada de la nómina y su posterior afectación financiera en el eSigef. La figura 7 muestra la interfaz web respectiva.

Figura 7. Interfaz web aplicativo web SPRYN

El aplicativo web eByE proporciona el servicio de gestión de bienes y existencias para las entidades públicas. Su interfaz web se muestra en la figura 8.

Figura 8. Interfaz web aplicativo web eByE

3 Estándar Internacional ISO/IEC 27000

ISO/IEC 27000 es la raíz para un amplio número de series numeradas de estándares internacionales para la gestión de seguridad de la información [1]. Estos estándares proveen una plataforma ampliamente reconocida de mejores prácticas para gestión de seguridad de la información.

EL estándar ISO/IEC 27001:2013 es la versión actual de la especificación del estándar internacional para un Sistema de Gestión de Seguridad de la Información. Es independiente de tecnologías y proveedores. Está diseñado para ser aplicable a todas las organizaciones, sin importar el tipo, tamaño o naturaleza. Es un sistema de gestión y no una especificación de tecnología, con el título formal "Tecnología de Información – Técnicas de Seguridad – Sistemas de gestión de seguridad de la información – Requerimientos".

El estándar ISO/IEC 27002:2013 es titulado "Tecnología de Información – Técnicas de Seguridad – Código de práctica para gestión de seguridad de la información". La primera edición fue publicada en Julio de 2005, habiendo sido numerada inicialmente como ISO/IEC 17799. La última edición fue publicada en Octubre de 2013.

El estándar ISO/IEC 27003:2010 es titulado "Tecnología de Información – Técnicas de seguridad – Guía de implementación de un sistema de gestión de seguridad de información". Fue publicado en Enero de 2010.

El estándar ISO/IEC 27004 es titulado "Tecnología de Información – Técnicas de seguridad – Gestión de seguridad de la información – Medición". Diseñado para ayudar a las organizaciones a ser más eficientes con los requerimientos para medir la efectividad de los controles. Fue publicado en Diciembre de 2009.

El estándar ISO/IEC 27005:2011 tiene que ver con la administración de riesgos de seguridad de la información, fue publicada en Junio de 2008, con una versión nueva publicada en el 2011.

El estándar ISO/IEC 27006:2011 establece los requerimientos para entidades que proveen la auditoría y certificación de sistemas de gestión de seguridad de la información.

3.1 Sistema de Gestión de Seguridad de la Información

La Información es considerada como la posesión más valiosa de una organización, incluso si esta información no ha sido sujeta a una valoración formal y comprehensiva [1]. La Gobernanza de TI es la disciplina que trata con las estructuras, estándares y procesos para gestionar efectivamente, proteger y aprovechar los activos de información de una organización.

La Gestión de Seguridad de la Información es un subconjunto de la Gobernanza de TI que se enfoca en proteger y asegurar los activos de información de una organización.

Los activos de información están sujetos a varios tipos de amenazas, internas o externas, que van desde lo aleatorio a lo específico. Los riesgos incluyen actos de la naturaleza, fraude y otras actividades criminales, errores de usuarios y fallas de los sistemas.

El Sistema de Gestión de Seguridad de la Información (ISMS) es definido en la ISO/IEC 27000 como "parte de un sistema de gestión global, basado en un enfoque de riesgo del negocio, para establecer, implementar, operar, monitorear, revisar mantener y mejorar la seguridad de la información [1]. El sistema de gestión incluye estructura organizacional, políticas, actividades de planificación, responsabilidades, prácticas, procedimientos, procesos y recursos.

3.1.1 Definición de Seguridad de la Información

La ISO 27000 define a la seguridad de la información como la "preservación de la confidencialidad, integridad y disponibilidad de la información; adicionalmente, otras propiedades tales como autenticidad, responsabilidad, no repudio y confiabilidad pueden ser incluidas" [1].

Los riesgos de la información pueden afectar uno o varios de los tres atributos fundamentales de un activo de información, que son: disponibilidad, confidencialidad e integridad.

- Disponibilidad: La propiedad de ser accesible y utilizable bajo demanda, por una entidad autorizada, lo cual posibilita que la información sea accedida por programas de software y por usuarios humanos.
- Confidencialidad: La propiedad que hace que la información no esté disponible o sea divulgada para personas no autorizadas, entidades o procesos.
- Integridad: La propiedad de proteger la exactitud e integridad de los activos.

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

3.1.2 Sistema de Gestión de Seguridad de la Información

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización [1]. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de

conformidad legal e imagen institucional necesarios para lograr los objetivos de la entidad pública.

Las entidades públicas y sus sistemas de información están expuestas a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el "cracking" o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia entidad o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.

El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de la entidad para asegurar el máximo beneficio, son algunos de los aspectos fundamentales en los que un SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de las entidades.

EL nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la entidad, con las autoridades al frente, tomando en consideración también a usuarios y proveedores de bienes y servicios. El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

El SGSI ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la entidad, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia entidad ha decidido asumir.

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

Un SGSI, que dentro del estándar incluye la estructura organizacional, políticas, actividades de planificación, responsabilidades, prácticas, procedimientos, procesos y recursos, es un enfoque de gestión estructurado, coherente para la seguridad de la información, el cual es diseñado para garantizar la interacción efectiva de los tres componentes claves para la implementación de un política de seguridad de la información:

- Proceso (procedimiento)

- Tecnología
- Comportamiento del usuario

El requerimiento del estándar es que el diseño e implementación de un SGSI debería ser directamente influenciado por las necesidades y objetivos de cada entidad, requerimientos de seguridad, los procesos organizacionales usados, además del tamaño y estructura de la entidad.

3.2 ISO/IEC 27001:2013, Aspectos fundamentales

Este estándar internacional ha sido preparado para proporcionar requerimientos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de seguridad de la información [12].

3.2.1 Alcance

Este estándar internacional especifica los requerimientos para el establecimiento, implementación, mantenimiento y mejoramiento continuo de un sistema de gestión de seguridad de la información dentro del contexto de la entidad u organización. Este estándar internacional también incluye requerimientos para la valoración y tratamiento de riesgos de seguridad de la información adaptados a las necesidades de la organización. Los requerimientos expuestos en este estándar internacional son genéricos y pueden ser aplicados a todas las organizaciones, sin importar el tipo, tamaño o naturaleza.

3.2.2 Contexto de la organización

Se debe tener un entendimiento de la organización y su contexto; es decir, la organización debe determinar los problemas internos y externos que son relevantes para su propósito y que afecta la capacidad de su sistema de gestión de seguridad de la información para alcanzar los resultados esperados.

Se debe tener un entendimiento de las necesidades y expectativas de las partes interesadas; es decir, la organización debe determinar las partes interesadas que son relevantes para el sistema de gestión de seguridad de la información, y los requerimientos de estas partes interesadas que son relevantes para la seguridad de la información.

Se debe determinar el alcance del sistema de gestión de seguridad de la información; es decir, la organización debe determinar los límites y aplicabilidad del sistema de gestión de seguridad de la información para establecer su alcance. Cuando se determina el alcance, la organización debe considerar: los problemas internos y externos referidos en el primer párrafo de este apartado, los requerimientos referidos en el segundo párrafo de este apartado, y, las interfaces y dependencias entre las actividades realizadas por la organización y las realizadas por otras organizaciones.

La organización debe establecer, implementar, mantener y mejorar de forma continua un sistema de gestión de seguridad de la información, de acuerdo a los requerimientos de este estándar internacional.

3.2.3 Liderazgo

La alta gerencia o dirección debe demostrar liderazgo y compromiso respecto al sistema de gestión de seguridad de la información mediante el:

- Asegurar que la política y objetivos de seguridad de la información estén establecidos y sean compatibles con la dirección estratégica de la organización.
- Asegurar la integración de los requerimientos del sistema de gestión de seguridad de la información dentro de los procesos de la organización.
- Asegurar que los recursos necesarios para el sistema de gestión de seguridad de la información estén disponibles.
- Comunicar la importancia de una gestión efectiva de seguridad de la información y que esté acorde a los requerimientos del sistema de gestión de seguridad de la información.
- Asegurar que el sistema de gestión de seguridad de la información logre los resultados esperados.
- Dirigir y apoyar a las personas para contribuir a la efectividad del sistema de gestión de seguridad de la información.
- Promover el mejoramiento continuo.
- Apoyar otros roles relevantes de gestión para demostrar su liderazgo y su aplicación en sus áreas de responsabilidad.

La alta gerencia o dirección debe establecer una política de seguridad de la información que:

- Sea apropiada para el propósito de la organización.
- Incluya los objetivos de seguridad de la información o provea la plataforma para establecer los objetivos de seguridad de la información.
- Incluya un compromiso para satisfacer los requerimientos aplicables relacionados a la seguridad de la información.
- Incluya un compromiso para el mejoramiento continuo del sistema de gestión de seguridad de la información.

La alta gerencia o dirección debe asegurar que las responsabilidades y autoridades sean asignadas y comunicadas para los roles relevantes de la seguridad de la información. La asignación de responsabilidad y autoridad permitirá:

- Asegurar que el sistema de gestión de seguridad de la información esté acorde a los requerimientos de este estándar internacional.
- Reportar a la alta gerencia o dirección acerca del desempeño del sistema de gestión de seguridad de la información.

3.2.4 Planificación

La planificación tiene que ver con las acciones para manejar los riesgos y las oportunidades. Cuando se está planificando el sistema de gestión de seguridad de la información, la organización debe considerar los problemas y los requerimientos referidos en el apartado 3.2.2 sobre contexto de la información, y determinar los riesgos y oportunidades que necesitan ser manejados para:

- Asegurar que el sistema de gestión de seguridad de la información pueda lograr los resultados esperados.
- Prevenir o reducir los efectos no deseados.
- Lograr el mejoramiento continuo.

La organización debe planificar acciones para manejar los riesgos y oportunidades, buscar la forma de integrar e implementar estas acciones en los procesos del sistema de gestión de seguridad de la información, además de evaluar la efectividad de estas acciones.

En lo que respecta a la valoración de riesgos de seguridad de la información, la organización debe definir y aplicar un proceso de valoración de riesgos de seguridad de la información que:

- Establezca y mantenga un criterio de riegos de seguridad de la información que incluya un criterio de aceptación del riesgo; y, un criterio para realizar la valoración de riesgos de seguridad de la información.
- Asegure que las valoraciones de riesgos de seguridad de la información produzcan resultados consistentes, válidos y comparables.
- Identifique riesgos asociados con la pérdida de confidencialidad, integridad y disponibilidad de la información, dentro del alcance del sistema de gestión de seguridad de la información; además de identificar a los poseedores de los riesgos.
- Analice los riesgos de seguridad de la información; es decir, que valore las potenciales consecuencias que podrían resultar si los riesgos identificados se materialicen, que valore la probabilidad real de ocurrencia de los riesgos identificados y que determine los niveles de riesgos.

- Evalúe los riesgos de seguridad de la información; es decir, que compare los resultados del análisis de riesgos con el criterio de riesgo establecido, y que priorice los riesgos analizados para su tratamiento.

Para el tratamiento de los riesgos de seguridad de la información, la organización debe definir y aplicar un proceso de tratamiento de riesgos para:

- Seleccionar las opciones apropiadas de tratamiento de riesgos de seguridad de la información, tomando en cuenta los resultados de la valoración de riesgos.
- Determinar todos los controles que son necesarios de implementar las opciones seleccionadas de tratamiento de riesgos de seguridad de la información.
- Comparar los controles determinados con los descritos en el Anexo A del estándar ISO/IEC 27001 y verificar que no hayan sido omitidos controles necesarios.
- Generar una Declaración de Aplicabilidad que contenga los controles necesarios y las justificaciones de su inclusión, si estos están implementados o no, y la justificación de exclusiones de controles del referido Anexo A del estándar.
- Formular un plan de tratamiento de riesgos de seguridad de la información.
- Obtener la aprobación del plan de tratamiento de riesgos de seguridad de la información, por parte de los poseedores o dueños de los riesgos, y la aceptación de los riesgos residuales de seguridad de la información.

En lo relacionado a objetivos de seguridad de la información y la planificación para su consecución, la organización debe establecer estos objetivos en funciones y niveles relevantes. Estos objetivos deben:

- Ser consistentes con la política de seguridad de la información.
- Ser medibles.
- Considerar los requerimientos aplicables de seguridad de la información, y resultados de la valoración y tratamiento de riesgos.
- Ser comunicados.
- Ser actualizados cuando en caso lo amerite.

En la planificación para lograr los objetivos de seguridad de la información, la organización debe determinar:

- Lo que será realizado
- Los recursos requeridos

- Los responsables
- Los plazos de ejecución
- La forma de evaluación de los resultados.

La figura 9 muestra la estructura del estándar internacional ISO/IEC 27000, basado en la clasificación de los objetivos de control y controles, que están detallados en el Anexo A del estándar referido.

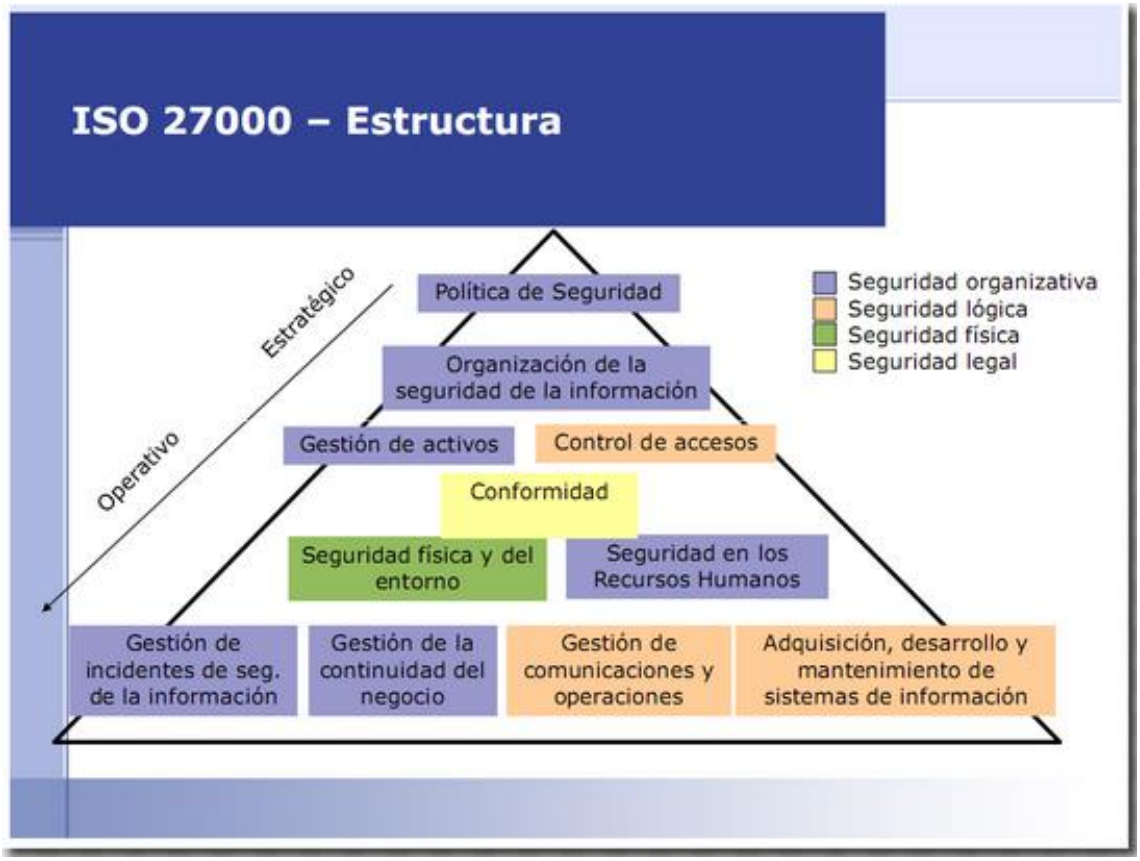

Figura 9. Estructura de la norma ISO/IEC 27000

4 Esquema Gubernamental de Seguridad de la Información EGSI

La Secretaría Nacional de la Administración Pública del Ecuador, considerando que las TIC son herramientas imprescindibles para el desempeño institucional e interinstitucional, y como respuesta a la necesidad de gestionar de forma eficiente y eficaz la seguridad de la información en las entidades públicas, creó la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación [14].

La comisión realizó un análisis de la situación respecto de la gestión de la seguridad de la información en las Instituciones de la Administración Pública Central, Dependiente e Institucional, llegando a determinar la necesidad de aplicar normas y procedimientos para seguridad de la información, e incorporar a la cultura y procesos institucionales la gestión permanente de la misma.

Se genera entonces el documento denominado Esquema Gubernamental de Seguridad de la Información (EGSI), que está basado en la norma técnica ecuatoriana INEN ISO/IEC27002 para Gestión de la Seguridad de la Información y está dirigido a las Instituciones de la Administración Pública Central.

El EGSI establece un conjunto de directrices prioritarias para Gestión de la Seguridad de la Información e inicia un proceso de mejora continua en las instituciones de la Administración Pública. El EGSI no reemplaza a la norma INEN ISO/IEC 27002 sino que marca como prioridad la implementación de algunas directrices. La implementación del EGSI tiene como propósito incrementar la seguridad de la información en las entidades públicas así como la confianza de los ciudadanos en la Administración Pública.

El contenido del EGSI, se basa en lo indicado en el Anexo A del estándar internacional ISO/IEC 27001 y en el estándar ISO/IEC 27002, relacionado a mejores prácticas, y lo ordena de la siguiente forma:

- Política de Seguridad de la Información
- Organización de la Seguridad de la Información
- Gestión de activos
- Seguridad de los Recursos Humanos
- Seguridad física y del entorno
- Gestión de Comunicaciones y Operaciones
- Control de Acceso
- Adquisición, desarrollo y mantenimiento de Sistemas de Información
- Gestión de los Incidentes de la Seguridad de la Información
- Gestión de la Continuidad del Negocio
- Cumplimiento

Del estudio realizado al EGSI, su implementación se la debe realizar a través de la planificación, implementación, control y mejora continua de un sistema de gestión de seguridad de la información SGSI.

La propuesta de planificación del SGSI se la detalla en el capítulo 5 del presente documento; sin embargo, es importante señalar aspectos generales que constan en el EGSI, relacionados con la política y organización de la seguridad de la información.

EL ESGI, en lo referente a Política de Seguridad de la Información, establece que:

- La máxima autoridad de la institución dispondrá la implementación del EGSI.
- Se debe aplicar el EGSI para definir procesos, procedimientos y tecnologías a fin de garantizar la confidencialidad, integridad y disponibilidad de la Información, en los medios y el tiempo que su legitimidad lo requiera.

EL ESGI, en lo referente a Organización de la Seguridad de la Información, establece que:

- Se debe realizar el seguimiento de la puesta en marcha de las normas del EGSI.
- Se debe disponer la difusión, capacitación y sensibilización del contenido del EGSI.
- Se debe conformar de forma oficial el Comité de Gestión de la Seguridad de la Información, al interno de la institución, y designar a los integrantes.
- La coordinación de la Gestión de la Seguridad de la Información estará a cargo del Comité, que tendrá las siguientes funciones:
    - Definir y mantener la política y normas institucionales particulares en materia de seguridad de la información y gestionar la aprobación por parte de la máxima autoridad de la institución.
    - Monitorear cambios significativos de los riesgos que afectan a los recursos de información frente a las amenazas.
    - Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.
    - Aprobar las principales iniciativas para incrementar la seguridad de la información.
    - Acordar y aprobar metodologías y procesos específicos, en base al EGSI.
    - Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios, en base al EGSI.

- Coordinar el proceso de gestión de la continuidad de la operación de los servicios y sistemas de información de la institución frente a incidentes de seguridad imprevistos.
- Designar a los custodios o responsables de la información.
- Gestionar la provisión permanente de recursos económicos, tecnológicos y humanos para la gestión de la seguridad de la información.
- Velar por la aplicación de la familia de normas técnicas ecuatorianas INEN ISO/IEC 27000.
- Designar formalmente a un funcionario como Oficial de Seguridad de la Información quien actuará como coordinador del Comité.

5 Planificación del SGSI

Dado que el SGSI es básicamente un conjunto de procesos y procedimientos enfocados en gestionar la seguridad de la información, dentro de una organización, se utiliza el ciclo continuo PDCA (Plan, Do, Check, Act) por sus siglas en inglés, que es tradicional en los sistemas de gestión de calidad [5].

EL presente trabajo final de máster se enfoca en el Plan, es decir, en la planificación de un SGSI, para lo cual se consideran los requisitos más sobresalientes del estándar internacional ISO/IEC 27001 y se siguen los pasos indicados en el estándar internacional ISO/IEC 27003 [3], [13].

5.1 Alcance del SGSI

El Ministro de Finanzas de Ecuador, por medio del Acuerdo Ministerial No. 209 del 23 de julio de 2014, dispone la implementación del Esquema Gubernamental de la Seguridad de la Información en el Ministerio de Finanzas, basado en el Acuerdo Ministerial No. 166, denominado "Esquema Gubernamental de Seguridad de la Información EGSI", emitido por la Secretaría Nacional de la Administración Pública, que a su vez se basa en la norma ISO 27000.

El Acuerdo Ministerial No. 209 dispone la implementación del EGSI en el ámbito de sus competencias, entre otras, a la Subsecretaría de Innovación de las Finanzas Públicas, de la que la Dirección Nacional de Operaciones de los Sistemas de las Finanzas Públicas forma parte.

El presente documento define como alcance el diseñar (Plan) un sistema de gestión de seguridad de la información, para su implementación al interno de la Dirección citada.

El alcance del SGSI cubre a la infraestructura tecnológica (servidores, almacenamiento, comunicaciones) sobre la cual operan los sistemas de finanzas públicas, aplicaciones informáticas e información almacenada.

Los activos involucrados se localizan en el Centro de Datos del Ministerio de Finanzas del Ecuador, en la ciudad de Quito.

5.2 Definición de la política de seguridad

El Acuerdo Ministerial No. 209 dispone la aprobación y elevación a rango de normativa interna el documento denominado Política General de Seguridad de la Información, que es de cumplimiento obligatorio para todo el personal del Ministerio de Finanzas en el marco de la implantación del EGSI y del Sistema de Gestión de Seguridad de la Información [8]. El Ministerio de Finanzas del Ecuador, reconoce la importancia de identificar y proteger los activos de información de la Institución; para ello, evitará la

destrucción, divulgación, modificación, indisponibilidad y utilización no autorizada de toda información, comprometiéndose a planificar, desarrollar, implantar, mantener, mejorar y evaluar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI) y del uso del Esquema Gubernamental de Seguridad de la Información (EGSI).

Es Política de Seguridad de la Información del Ministerio de Finanzas del Ecuador [9]:

- Establecer objetivos anuales con relación a la Seguridad de la Información.
- Establecer la gestión de riesgos de seguridad de la información, evaluación y tratamiento de riesgos, de acuerdo a su resultado implementar las acciones correctivas y preventivas correspondientes al tratamiento y gestión de riesgos, así como elaborar y actualizar los planes de acción y manuales de seguridad de la información correspondientes.
- Clasificar y proteger la información de acuerdo a los criterios de valoración en relación a la importancia que posee para la Institución y a la normativa vigente.
- Cumplir con los requerimientos legales o reglamentarios de seguridad de la información en concordancia con la Constitución y las Leyes aplicables vigentes.
- Realizar campañas de concientización y formación al personal de la Institución en materia de seguridad de la información.
- Contar con una política de gestión de incidentes de seguridad de la información.
- Contar con un Plan de Continuidad de Negocio con el fin de garantizar las operaciones críticas y necesarias de la Institución.

5.3 Metodología de Evaluación de Riesgos

Se hará uso de un metodología concreta de Análisis de Riesgos que considere los riesgos lógicos, de los cuales nos ocuparemos en este estudio. La metodología a usar cumple con los estándares ISO 27001.

La metodología a usarse se basa en MAGERIT II, que es una metodología desarrollada con el Consejo Superior de Administración Electrónica [4]. La figura 10 muestra un diagrama de los fundamentos de la metodología.

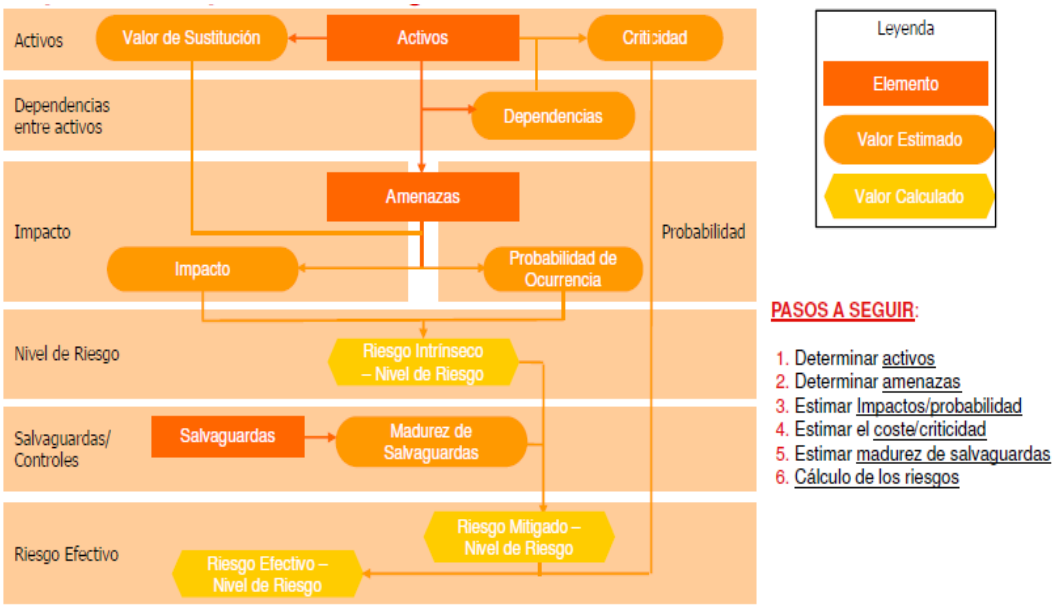

Figura 10. Fundamentos de la metodología de evaluación de riesgos

La metodología propuesta, basada en MAGERIR II, da cumplimiento a lo establecido en:

- ISO 27005, "Identificar Riesgos"
- ISO 27005, " Analizar y Evaluar Riesgos"
- ISO 27001, "Sistemas de Gestión de Seguridad de la Información"
- ISO 27002, "Manual de Buenas Prácticas de Gestión de Seguridad de la Información"
- ISO 27005, "Gestión de Riesgos de Seguridad de Información"

Para simplificar la metodología a usar, se definen etapas para una correcta gestión de los riesgos y su relación para un continuo proceso de mejora. La figura 11 muestra las etapas definidas.

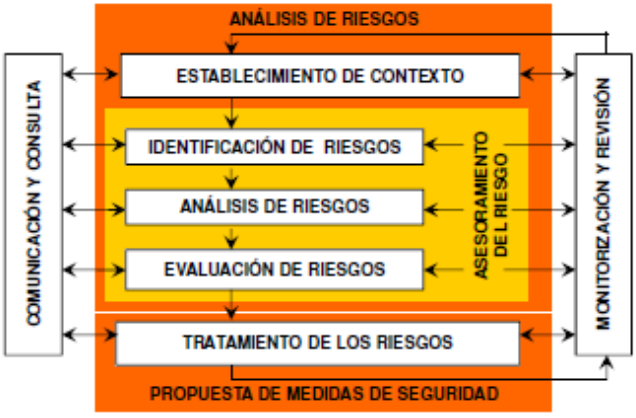

Figura 11. Etapas de la metodología de evaluación de riesgos

El resumen de las etapas es el siguiente:

- Establecimiento del contexto
    - Activos
    - Amenazas
- Identificación de riesgos
    - Situaciones de riesgo
- Análisis de riesgos
    - Impacto
    - Probabilidad
    - Criticidad
    - Nivel de necesidad de salvaguardas
- Evaluación de riesgos

5.4 Establecimiento del contexto

En esta etapa, para la determinación de activos y amenazas, primero se expone las definiciones de activos, tipos de activos, amenazas y tipos de amenazas.

Activo: son todos aquellos bienes, espacios, procesos y cualquier otro elemento de consideración que sea susceptible de sufrir las consecuencias de una amenaza.

Los tipos de activos físicos y lógicos considerados en este estudio son:

- Servicios
- Aplicaciones (Software)
- Redes de comunicaciones
- Plataforma tecnológica de almacenamiento
- Plataforma tecnológica de procesamiento
- Plataforma tecnológica de respaldo
- Plataforma tecnológica de seguridad
- Plataforma tecnológica de Bases de Datos
- Datos/información

Amenazas: Contingencias o riesgos específicos de los activos analizados, dependientes del entorno y circunstancias, cuya potencial materialización debe ser mermada.

Los tipos de amenazas consideradas en este estudio son:

- Desastres Naturales
- Ataques Intencionados
- Errores y fallos no intencionados

La figura 12 muestra la arquitectura tecnológica sobre la cual operan los diferentes servicios y aplicativos web proporcionados por el Ministerio de Finanzas del Ecuador, cuya gestión está a cargo de la Dirección Nacional de Operaciones de los Sistemas de Finanzas Públicas.

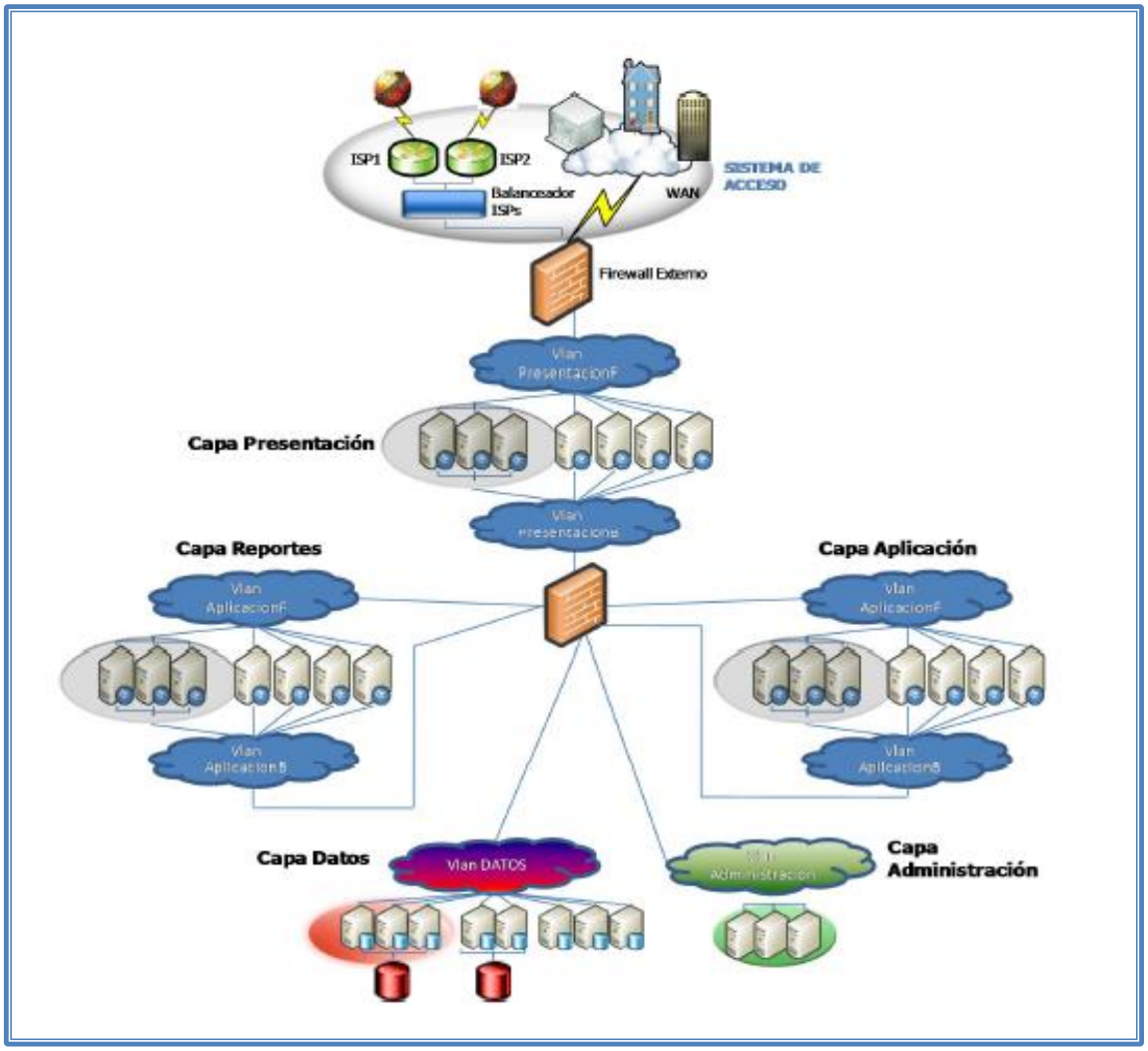

Figura 12. Arquitectura tecnológica de los servicios y aplicativos web del Ministerio de Finanzas

5.4.1 Determinación de activos y amenazas

Las tablas, desde la 1 hasta la 9, detallan los activos y amenazas incluidos en el estudio, dentro del campo de acción de la Dirección Nacional de Operaciones de los Sistemas de Finanzas Públicas, y que guardan relación con la arquitectura tecnológica mostrada en la figura 12. [2], [6], [7].

Tabla 1. Activos del grupo Almacenamiento vs amenazas

	Grupo	Almacenamiento		
	Activo	Arreglo de Discos	Controladora	SAN
Tipo Amenaza	**Amenaza**			
Ataques Intencionados	Malware			
Ataques Intencionados	Denegación de Servicio			
Ataques Intencionados	Alteración de Información			
Ataques Intencionados	Destrucción de Información			
Ataques Intencionados	Fugas de Información			
Ataques Intencionados	Acceso no autorizado a la Información			
Ataques Intencionados	Suplantación de Identidad			
Ataques Intencionados	Abuso de privilegios de acceso			
Ataques Intencionados	Interceptación de información			
Ataques Intencionados	Manipulación de programas			
Ataques Intencionados	Ingeniería Social			
Ataques Intencionados	Manipulación de configuraciones	X	X	X
Ataques Intencionados	Repudio			
Ataques Intencionados	Ocupación no autorizada (huelgas)	X	X	X
Desastres Naturales	Terremotos	X	X	X
Desastres Naturales	Erupción Volcánica	X	X	X
Errores y Fallos No Intencionados	Corte de Suministro eléctrico	X	X	X
Errores y Fallos No Intencionados	Condiciones inadecuadas de temperatura o humedad	X	X	X
Errores y Fallos No Intencionados	Errores de mantenimiento/actualización	X	X	X
Errores y Fallos No Intencionados	Agotamiento de recursos			
Errores y Fallos No Intencionados	Indisponibilidad del personal			
Errores y Fallos No Intencionados	Fallo de servicios de comunicaciones			
Errores y Fallos No Intencionados	Interrupción de servicios de soporte	X	X	X
Errores y Fallos No Intencionados	Errores de usuarios			
Errores y Fallos No Intencionados	Errores de administrador	X	X	X
Errores y Fallos No Intencionados	Errores de configuración	X	X	X
Errores y Fallos No Intencionados	Incendios	X	X	X

Tabla 2. Activos del grupo Procesamiento vs amenazas

	Grupo	Procesamiento	
	Activo	Servidores Blade	Chasis Blade
Tipo Amenaza	**Amenaza**		
Ataques Intencionados	Malware		
Ataques Intencionados	Denegación de Servicio	X	
Ataques Intencionados	Alteración de Información		
Ataques Intencionados	Destrucción de Información		
Ataques Intencionados	Fugas de Información		
Ataques Intencionados	Acceso no autorizado a la Información		
Ataques Intencionados	Suplantación de Identidad		
Ataques Intencionados	Abuso de privilegios de acceso		
Ataques Intencionados	Interceptación de información		
Ataques Intencionados	Manipulación de programas		
Ataques Intencionados	Ingeniería Social		
Ataques Intencionados	Manipulación de configuraciones	X	X
Ataques Intencionados	Repudio		
Ataques Intencionados	Ocupación no autorizada (huelgas)	X	X
Desastres Naturales	Terremotos	X	X
Desastres Naturales	Erupción Volcánica	X	X
Errores y Fallos No Intencionados	Corte de Suministro eléctrico	X	X
Errores y Fallos No Intencionados	Condiciones inadecuadas de temperatura o humedad	X	X
Errores y Fallos No Intencionados	Errores de mantenimiento/actualización	X	X
Errores y Fallos No Intencionados	Agotamiento de recursos		
Errores y Fallos No Intencionados	Indisponibilidad del personal		
Errores y Fallos No Intencionados	Fallo de servicios de comunicaciones		
Errores y Fallos No Intencionados	Interrupción de servicios de soporte	X	X
Errores y Fallos No Intencionados	Errores de usuarios		
Errores y Fallos No Intencionados	Errores de administrador	X	X
Errores y Fallos No Intencionados	Errores de configuración	X	X
Errores y Fallos No Intencionados	Incendios	X	X

Tabla 3. Activos del grupo Comunicaciones vs amenazas

	Grupo	Comunicaciones				
	Activo	Switch Core	Switch Distribución	Switch Acceso	Balanceadores de carga	Balanceadores ISP
Tipo Amenaza	**Amenaza**					
Ataques Intencionados	Malware					
Ataques Intencionados	Denegación de Servicio				X	X
Ataques Intencionados	Alteración de Información					
Ataques Intencionados	Destrucción de Información					
Ataques Intencionados	Fugas de Información					
Ataques Intencionados	Acceso no autorizado a la Información					
Ataques Intencionados	Suplantación de Identidad					
Ataques Intencionados	Abuso de privilegios de acceso					
Ataques Intencionados	Interceptación de información					
Ataques Intencionados	Manipulación de programas					
Ataques Intencionados	Ingeniería Social					
Ataques Intencionados	Manipulación de configuraciones	X	X	X	X	X
Ataques Intencionados	Repudio					
Ataques Intencionados	Ocupación no autorizada (huelgas)	X	X	X	X	X
Desastres Naturales	Terremotos	X	X	X	X	X
Desastres Naturales	Erupción Volcánica	X	X	X	X	X
Errores y Fallos No Intencionados	Corte de Suministro eléctrico	X	X	X	X	X
Errores y Fallos No Intencionados	Condiciones inadecuadas de temperatura o humedad	X	X	X	X	X
Errores y Fallos No Intencionados	Errores de mantenimiento/actualización	X	X	X	X	X
Errores y Fallos No Intencionados	Agotamiento de recursos					
Errores y Fallos No Intencionados	Indisponibilidad del personal					
Errores y Fallos No Intencionados	Fallo de servicios de comunicaciones					
Errores y Fallos No Intencionados	Interrupción de servicios de soporte	X	X	X	X	X
Errores y Fallos No Intencionados	Errores de usuarios					
Errores y Fallos No Intencionados	Errores de administrador	X	X	X	X	X
Errores y Fallos No Intencionados	Errores de configuración	X	X	X	X	X
Errores y Fallos No Intencionados	Incendios	X	X	X	X	X

Tabla 4. Activos del grupo Seguridad vs amenazas

	Grupo	Seguridad		
	Activo	Firewall	IPS	Antivirus
Tipo Amenaza	**Amenaza**			
Ataques Intencionados	Malware			
Ataques Intencionados	Denegación de Servicio			
Ataques Intencionados	Alteración de Información			
Ataques Intencionados	Destrucción de Información			
Ataques Intencionados	Fugas de Información			
Ataques Intencionados	Acceso no autorizado a la Información			
Ataques Intencionados	Suplantación de Identidad			
Ataques Intencionados	Abuso de privilegios de acceso			
Ataques Intencionados	Interceptación de información			
Ataques Intencionados	Manipulación de programas			
Ataques Intencionados	Ingeniería Social			
Ataques Intencionados	Manipulación de configuraciones	X	X	X
Ataques Intencionados	Repudio			
Ataques Intencionados	Ocupación no autorizada (huelgas)	X	X	X
Desastres Naturales	Terremotos	X	X	X
Desastres Naturales	Erupción Volcánica	X	X	X
Errores y Fallos No Intencionados	Corte de Suministro eléctrico	X	X	
Errores y Fallos No Intencionados	Condiciones inadecuadas de temperatura o humedad	X	X	
Errores y Fallos No Intencionados	Errores de mantenimiento/actualización	X	X	X
Errores y Fallos No Intencionados	Agotamiento de recursos			
Errores y Fallos No Intencionados	Indisponibilidad del personal			
Errores y Fallos No Intencionados	Fallo de servicios de comunicaciones			
Errores y Fallos No Intencionados	Interrupción de servicios de soporte	X	X	X
Errores y Fallos No Intencionados	Errores de usuarios			
Errores y Fallos No Intencionados	Errores de administrador	X	X	X
Errores y Fallos No Intencionados	Errores de configuración	X	X	X
Errores y Fallos No Intencionados	Incendios	X	X	X

Tabla 5. Activos del grupo Respaldos vs amenazas

	Grupo	Respaldos	
	Activo	Librería virtual	Controlador
Tipo Amenaza	**Amenaza**		
Ataques Intencionados	Malware		
Ataques Intencionados	Denegación de Servicio		
Ataques Intencionados	Alteración de Información		
Ataques Intencionados	Destrucción de Información		
Ataques Intencionados	Fugas de Información		
Ataques Intencionados	Acceso no autorizado a la Información		
Ataques Intencionados	Suplantación de Identidad		
Ataques Intencionados	Abuso de privilegios de acceso		
Ataques Intencionados	Interceptación de información		
Ataques Intencionados	Manipulación de programas		
Ataques Intencionados	Ingeniería Social		
Ataques Intencionados	Manipulación de configuraciones	X	X
Ataques Intencionados	Repudio		
Ataques Intencionados	Ocupación no autorizada (huelgas)	X	X
Desastres Naturales	Terremotos	X	X
Desastres Naturales	Erupción Volcánica	X	X
Errores y Fallos No Intencionados	Corte de Suministro eléctrico	X	X
Errores y Fallos No Intencionados	Condiciones inadecuadas de temperatura o humedad	X	X
Errores y Fallos No Intencionados	Errores de mantenimiento/actualización	X	X
Errores y Fallos No Intencionados	Agotamiento de recursos		
Errores y Fallos No Intencionados	Indisponibilidad del personal		
Errores y Fallos No Intencionados	Fallo de servicios de comunicaciones		
Errores y Fallos No Intencionados	Interrupción de servicios de soporte	X	X
Errores y Fallos No Intencionados	Errores de usuarios		
Errores y Fallos No Intencionados	Errores de administrador	X	X
Errores y Fallos No Intencionados	Errores de configuración	X	X
Errores y Fallos No Intencionados	Incendios	X	X

Tabla 6. Activos del grupo Bases de Datos vs amenazas

	Grupo	Bases de Datos
	Activo	Sistema de Bases de Datos
Tipo Amenaza	**Amenaza**	
Ataques Intencionados	Malware	X
Ataques Intencionados	Denegación de Servicio	
Ataques Intencionados	Alteración de Información	
Ataques Intencionados	Destrucción de Información	
Ataques Intencionados	Fugas de Información	
Ataques Intencionados	Acceso no autorizado a la Información	
Ataques Intencionados	Suplantación de Identidad	
Ataques Intencionados	Abuso de privilegios de acceso	
Ataques Intencionados	Interceptación de información	
Ataques Intencionados	Manipulación de programas	
Ataques Intencionados	Ingeniería Social	
Ataques Intencionados	Manipulación de configuraciones	X
Ataques Intencionados	Repudio	
Ataques Intencionados	Ocupación no autorizada (huelgas)	X
Desastres Naturales	Terremotos	X
Desastres Naturales	Erupción Volcánica	X
Errores y Fallos No Intencionados	Corte de Suministro eléctrico	X
Errores y Fallos No Intencionados	Condiciones inadecuadas de temperatura o humedad	X
Errores y Fallos No Intencionados	Errores de mantenimiento/actualización	X
Errores y Fallos No Intencionados	Agotamiento de recursos	
Errores y Fallos No Intencionados	Indisponibilidad del personal	
Errores y Fallos No Intencionados	Fallo de servicios de comunicaciones	
Errores y Fallos No Intencionados	Interrupción de servicios de soporte	X
Errores y Fallos No Intencionados	Errores de usuarios	
Errores y Fallos No Intencionados	Errores de administrador	X
Errores y Fallos No Intencionados	Errores de configuración	X
Errores y Fallos No Intencionados	Incendios	X

Tabla 7. Activos del grupo Sistemas Operativos vs amenazas

	Grupo	Sistemas Operativos	
	Activo	Microsof Windows Server 2012	Linux Red Hat
Tipo Amenaza	**Amenaza**		
Ataques Intencionados	Malware	X	X
Ataques Intencionados	Denegación de Servicio		
Ataques Intencionados	Alteración de Información		
Ataques Intencionados	Destrucción de Información		
Ataques Intencionados	Fugas de Información		
Ataques Intencionados	Acceso no autorizado a la Información		
Ataques Intencionados	Suplantación de Identidad		
Ataques Intencionados	Abuso de privilegios de acceso		
Ataques Intencionados	Interceptación de información		
Ataques Intencionados	Manipulación de programas		
Ataques Intencionados	Ingeniería Social		
Ataques Intencionados	Manipulación de configuraciones	X	X
Ataques Intencionados	Repudio		
Ataques Intencionados	Ocupación no autorizada (huelgas)	X	X
Desastres Naturales	Terremotos	X	X
Desastres Naturales	Erupción Volcánica	X	X
Errores y Fallos No Intencionados	Corte de Suministro eléctrico		
Errores y Fallos No Intencionados	Condiciones inadecuadas de temperatura o humedad		
Errores y Fallos No Intencionados	Errores de mantenimiento/actualización	X	X
Errores y Fallos No Intencionados	Agotamiento de recursos		
Errores y Fallos No Intencionados	Indisponibilidad del personal		
Errores y Fallos No Intencionados	Fallo de servicios de comunicaciones		
Errores y Fallos No Intencionados	Interrupción de servicios de soporte	X	X
Errores y Fallos No Intencionados	Errores de usuarios		
Errores y Fallos No Intencionados	Errores de administrador	X	X
Errores y Fallos No Intencionados	Errores de configuración	X	X
Errores y Fallos No Intencionados	Incendios	X	X

Tabla 8. Activos del grupo Aplicativos vs amenazas

	Grupo	Aplicativos				
	Activo	eSigef	eSipren	eSByE	SPRYN	Servicios WEB
Tipo Amenaza	**Amenaza**					
Ataques Intencionados	Malware	X	X	X	X	
Ataques Intencionados	Denegación de Servicio	X	X	X	X	X
Ataques Intencionados	Alteración de Información	X	X	X	X	X
Ataques Intencionados	Destrucción de Información	X	X	X	X	X
Ataques Intencionados	Fugas de Información	X	X	X	X	X
Ataques Intencionados	Acceso no autorizado a la Información					
Ataques Intencionados	Suplantación de Identidad	X	X	X	X	X
Ataques Intencionados	Abuso de privilegios de acceso	X	X	X	X	X
Ataques Intencionados	Interceptación de información	X	X	X	X	X
Ataques Intencionados	Manipulación de programas	X	X	X	X	X
Ataques Intencionados	Ingeniería Social					
Ataques Intencionados	Manipulación de configuraciones	X	X	X	X	X
Ataques Intencionados	Repudio					
Ataques Intencionados	Ocupación no autorizada (huelgas)	X	X	X	X	X
Desastres Naturales	Terremotos	X	X	X	X	X
Desastres Naturales	Erupción Volcánica	X	X	X	X	X
Errores y Fallos No Intencionados	Corte de Suministro eléctrico					
Errores y Fallos No Intencionados	Condiciones inadecuadas de temperatura o humedad					
Errores y Fallos No Intencionados	Errores de mantenimiento/actualización					
Errores y Fallos No Intencionados	Agotamiento de recursos	X	X	X	X	X
Errores y Fallos No Intencionados	Indisponibilidad del personal	X	X	X	X	X
Errores y Fallos No Intencionados	Fallo de servicios de comunicaciones	X	X	X	X	X
Errores y Fallos No Intencionados	Interrupción de servicios de soporte					
Errores y Fallos No Intencionados	Errores de usuarios					
Errores y Fallos No Intencionados	Errores de administrador	X	X	X	X	X
Errores y Fallos No Intencionados	Errores de configuración	X	X	X	X	X
Errores y Fallos No Intencionados	Incendios	X	X	X	X	X

Tabla 9. Activos del grupo Información vs amenazas

	Grupo	Información	
	Activo	Almacenada	En tránsito
Tipo Amenaza	**Amenaza**		
Ataques Intencionados	Malware	X	
Ataques Intencionados	Denegación de Servicio		
Ataques Intencionados	Alteración de Información	X	X
Ataques Intencionados	Destrucción de Información	X	
Ataques Intencionados	Fugas de Información		
Ataques Intencionados	Acceso no autorizado a la Información	X	X
Ataques Intencionados	Suplantación de Identidad	X	X
Ataques Intencionados	Abuso de privilegios de acceso	X	
Ataques Intencionados	Interceptación de información		X
Ataques Intencionados	Manipulación de programas	X	
Ataques Intencionados	Ingeniería Social	X	
Ataques Intencionados	Manipulación de configuraciones		
Ataques Intencionados	Repudio		X
Ataques Intencionados	Ocupación no autorizada (huelgas)	X	
Desastres Naturales	Terremotos	X	
Desastres Naturales	Erupción Volcánica	X	
Errores y Fallos No Intencionados	Corte de Suministro eléctrico		
Errores y Fallos No Intencionados	Condiciones inadecuadas de temperatura o humedad		
Errores y Fallos No Intencionados	Errores de mantenimiento/actualización		
Errores y Fallos No Intencionados	Agotamiento de recursos		
Errores y Fallos No Intencionados	Indisponibilidad del personal		
Errores y Fallos No Intencionados	Fallo de servicios de comunicaciones		X
Errores y Fallos No Intencionados	Interrupción de servicios de soporte		
Errores y Fallos No Intencionados	Errores de usuarios	X	
Errores y Fallos No Intencionados	Errores de administrador		
Errores y Fallos No Intencionados	Errores de configuración		
Errores y Fallos No Intencionados	Incendios	X	

5.5 Identificación de riesgos

En esta etapa las combinaciones aplicables de activos-amenazas son consideradas. Cada posible combinación de activo-amenaza se denomina Situación de Riesgo [4]. El conjunto de estos genera el Mapa de Riesgos [2], [6], [7].

Las tablas 1 hasta la 9 muestran el mapa de riesgos con las situaciones de riesgo encontradas.

5.6 Análisis de riesgos

Para el análisis de riesgos se utilizarán escalas cualitativas para los parámetros considerados [4]. Los parámetros a analizarse y estimarse son:

- Parámetros a considerar para cada situación de riesgo
  - Impacto
  - Probabilidad
  - Nivel de necesidad de salvaguardas
- Parámetros a considerar para cada activo
  - Criticidad

El impacto es la medida de las consecuencias que puede sufrir un activo, en caso de materialización de una amenaza en un tiempo determinando. Se valora para cada situación de riesgo considerada, asumiendo uno de los valores indicados en la tabla 10.

Tabla 10. Valoración del Impacto a la materialización de una amenaza

IMPACTO	
MA	Impacto muy alto, muy grave o severo para la Organización
A	Impacto alto, grave para la Organización
M	Impacto medio, moderado, importante para la Organización
B	Impacto bajo, menor para la Organización
MB	Impacto muy bajo, irrelevante para la Organización

La probabilidad de ocurrencia de riesgos suele basarse en estudios estadísticos sobre la materialización de sucesos, averías o amenazas, sin embargo, se puede tener una valoración para indicar el grado de materialización de una amenaza, considerando dos indicadores como son el atractivo y la vulnerabilidad. EL atractivo se refiere al nivel de interés del agente de la amenaza para llevarla a cabo. La vulnerabilidad es la medida de cuan sencillo es llevar a cabo una amenaza sobre un activo, considerando que no existen salvaguardas.

La probabilidad puede tomar uno de los valores indicados en la tabla 11:

Tabla 11. Valoración de Probabilidad de Ocurrencia de Amenazas

PROBABILIDAD	
MA	Probabilidad muy alta de ocurrencia del evento, evento probablemente ocurra
A	Probabilidad alta de ocurrencia del evento, evento posible
M	Probabilidad moderada de ocurrencia del evento, evento improbable
B	Probabilidad baja de ocurrencia del evento, evento raro
MB	Probabilidad muy baja de ocurrencia del evento, evento muy raro

Las salvaguardas reducen ciertos riesgos mediante dos vías: reduciendo el impacto de las amenazas o reduciendo la probabilidad o frecuencia de ocurrencia. La necesidad de salvaguardas es inversamente proporcional al nivel de salvaguardas que afectan a un activo. Su valoración se define basándose en el modelo CMMI, obteniendo valores cuantitativos, conforme se indica en la tabla 12:

Tabla 12. Niveles CMMI y Necesidades de Salvaguardas

Grado de Madurez y Necesidad de Salvaguardas para Riesgos Lógicos			
Grado de Madurez	**Necesidad de Salvaguardas**	**Nivel CMMI**	**Prácticas de Gestión de Seguridad Lógica**
5	MB	OPTIMIZADO	Los procesos han sido revisados hasta un nivel de "best practice", sobre la base de una mejora continua
4	M	GESTIONADO	Los procesos están en mejora continua y proporcionan mejores prácticas. Se usan herramientas automatizadas de manera aislada o fragmentada
3	A	DEFINIDO	La organización asegura que el control se planifica, documenta, ejecuta, monitoriza y controla
2	MA	REPETIBLE	Los procesos han evolucionado de forma de que se siguen procedimientos similares para realizar la misma tarea. No existe formación ni comunicación de procedimientos estándar y la responsabilidad recae en el individuo
1	MA	INICIAL	No existen procesos estándar aunque existen planteamientos "ad hoc" que se utilizan en cada situación
0	MA	NO EXISTENTE	Ausencia total de procesos reconocibles

La criticidad mide las consecuencias que se estiman o asignan a cada dimensión de seguridad en los activos considerados, independiente de amenazas.

Dado que la Dirección Nacional de Operaciones de los Sistemas de Finanzas Públicas gestiona toda la infraestructura tecnológica que soporta los servicios relacionados con los sistemas de finanzas públicas, este estudio considera que los diferentes activos que conforman dicha infraestructura son considerados críticos.

La tabla 13 muestra en el análisis de riesgos realizado:

Tabla 13. Análisis de Riesgos

Situación de Riesgo			Impacto	Probabilidad	Necesidad de salvaguardas	Nivel CMMI
Grupo Activo	Activo	Amenaza				
Almacenamiento	Arreglo de discos	Manipulación de configuraciones	MA	B	A	DEFINIDO
Almacenamiento	Arreglo de discos	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
Almacenamiento	Arreglo de discos	Terremotos	MA	B	MA	REPETIBLE
Almacenamiento	Arreglo de discos	Erupción Volcánica	A	B	MA	REPETIBLE
Almacenamiento	Arreglo de discos	Corte de Suministro eléctrico	A	B	M	GESTIONADO
Almacenamiento	Arreglo de discos	Condiciones inadecuadas de temperatura o humedad	A	B	M	GESTIONADO
Almacenamiento	Arreglo de discos	Errores de mantenimiento/actualización	M	B	M	GESTIONADO
Almacenamiento	Arreglo de discos	Interrupción de servicios de soporte	A	B	A	DEFINIDO
Almacenamiento	Arreglo de discos	Errores de administrador	A	B	A	DEFINIDO
Almacenamiento	Arreglo de discos	Errores de configuración	A	B	A	DEFINIDO
Almacenamiento	Arreglo de discos	Incendios	MA	B	M	GESTIONADO
Almacenamiento	Controladora	Manipulación de configuraciones	MA	B	A	DEFINIDO
Almacenamiento	Controladora	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
Almacenamiento	Controladora	Terremotos	MA	B	MA	REPETIBLE
Almacenamiento	Controladora	Erupción Volcánica	A	B	MA	REPETIBLE
Almacenamiento	Controladora	Corte de Suministro eléctrico	A	B	M	GESTIONADO
Almacenamiento	Controladora	Condiciones inadecuadas de temperatura o humedad	A	B	M	GESTIONADO
Almacenamiento	Controladora	Errores de mantenimiento/actualización	M	B	M	GESTIONADO

Almacenamiento	Controladora	Interrupción de servicios de soporte	A	B	A	DEFINIDO
Almacenamiento	Controladora	Errores de administrador	A	B	A	DEFINIDO
Almacenamiento	Controladora	Errores de configuración	A	B	A	DEFINIDO
Almacenamiento	Controladora	Incendios	MA	B	M	GESTIONADO
Almacenamiento	SAN	Manipulación de configuraciones	MA	B	A	DEFINIDO
Almacenamiento	SAN	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
Almacenamiento	SAN	Terremotos	MA	B	MA	REPETIBLE
Almacenamiento	SAN	Erupción Volcánica	A	B	MA	REPETIBLE
Almacenamiento	SAN	Corte de Suministro eléctrico	A	B	M	GESTIONADO
Almacenamiento	SAN	Condiciones inadecuadas de temperatura o humedad	A	B	M	GESTIONADO
Almacenamiento	SAN	Errores de mantenimiento/actualización	M	B	M	GESTIONADO
Almacenamiento	SAN	Interrupción de servicios de soporte	A	B	A	DEFINIDO
Almacenamiento	SAN	Errores de administrador	A	B	A	DEFINIDO
Almacenamiento	SAN	Errores de configuración	A	B	A	DEFINIDO
Almacenamiento	SAN	Incendios	MA	B	M	GESTIONADO
Procesamiento	Servidores Blade	Denegación de Servicio	A	M	A	DEFINIDO
Procesamiento	Servidores Blade	Manipulación de configuraciones	MA	B	A	DEFINIDO
Procesamiento	Servidores Blade	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
Procesamiento	Servidores Blade	Terremotos	MA	B	MA	REPETIBLE
Procesamiento	Servidores Blade	Erupción Volcánica	A	B	MA	REPETIBLE
Procesamiento	Servidores Blade	Corte de Suministro eléctrico	A	B	M	GESTIONADO
Procesamiento	Servidores Blade	Condiciones inadecuadas de temperatura o humedad	A	B	M	GESTIONADO
Procesamiento	Servidores Blade	Errores de mantenimiento/actualización	M	B	M	GESTIONADO
Procesamiento	Servidores Blade	Interrupción de servicios de soporte	A	B	A	DEFINIDO
Procesamiento	Servidores Blade	Errores de administrador	A	B	A	DEFINIDO
Procesamiento	Servidores Blade	Errores de configuración	A	B	A	DEFINIDO
Procesamiento	Servidores Blade	Incendios	MA	B	M	GESTIONADO
Procesamiento	Chasis Blade	Manipulación de configuraciones	MA	B	A	DEFINIDO

Procesamiento	Chasis Blade	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
Procesamiento	Chasis Blade	Terremotos	MA	B	MA	REPETIBLE
Procesamiento	Chasis Blade	Erupción Volcánica	A	B	MA	REPETIBLE
Procesamiento	Chasis Blade	Corte de Suministro eléctrico	A	B	M	GESTIONADO
Procesamiento	Chasis Blade	Condiciones inadecuadas de temperatura o humedad	A	B	M	GESTIONADO
Procesamiento	Chasis Blade	Errores de mantenimiento/actualización	M	B	M	GESTIONADO
Procesamiento	Chasis Blade	Interrupción de servicios de soporte	A	B	A	DEFINIDO
Procesamiento	Chasis Blade	Errores de administrador	A	B	A	DEFINIDO
Procesamiento	Chasis Blade	Errores de configuración	A	B	A	DEFINIDO
Procesamiento	Chasis Blade	Incendios	MA	B	M	GESTIONADO
Comunicaciones	Switch Core	Manipulación de configuraciones	MA	B	A	DEFINIDO
Comunicaciones	Switch Core	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
Comunicaciones	Switch Core	Terremotos	MA	B	MA	REPETIBLE
Comunicaciones	Switch Core	Erupción Volcánica	A	B	MA	REPETIBLE
Comunicaciones	Switch Core	Corte de Suministro eléctrico	A	B	M	GESTIONADO
Comunicaciones	Switch Core	Condiciones inadecuadas de temperatura o humedad	A	B	M	GESTIONADO
Comunicaciones	Switch Core	Errores de mantenimiento/actualización	M	B	M	GESTIONADO
Comunicaciones	Switch Core	Interrupción de servicios de soporte	A	B	A	DEFINIDO
Comunicaciones	Switch Core	Errores de administrador	A	B	A	DEFINIDO
Comunicaciones	Switch Core	Errores de configuración	A	B	A	DEFINIDO
Comunicaciones	Switch Core	Incendios	MA	B	M	GESTIONADO
Comunicaciones	Switch Distribución	Manipulación de configuraciones	MA	B	A	DEFINIDO
Comunicaciones	Switch Distribución	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
Comunicaciones	Switch Distribución	Terremotos	MA	B	MA	REPETIBLE
Comunicaciones	Switch Distribución	Erupción Volcánica	A	B	MA	REPETIBLE
Comunicaciones	Switch Distribución	Corte de Suministro eléctrico	A	B	M	GESTIONADO
Comunicaciones	Switch Distribución	Condiciones inadecuadas de temperatura o humedad	A	B	M	GESTIONADO

Comunicaciones	Switch Distribución	Errores de mantenimiento/actualización	M	B	M	GESTIONADO
Comunicaciones	Switch Distribución	Interrupción de servicios de soporte	A	B	A	DEFINIDO
Comunicaciones	Switch Distribución	Errores de administrador	A	B	A	DEFINIDO
Comunicaciones	Switch Distribución	Errores de configuración	A	B	A	DEFINIDO
Comunicaciones	Switch Distribución	Incendios	MA	B	M	GESTIONADO
Comunicaciones	Switch Acceso	Manipulación de configuraciones	MA	B	A	DEFINIDO
Comunicaciones	Switch Acceso	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
Comunicaciones	Switch Acceso	Terremotos	MA	B	MA	REPETIBLE
Comunicaciones	Switch Acceso	Erupción Volcánica	A	B	MA	REPETIBLE
Comunicaciones	Switch Acceso	Corte de Suministro eléctrico	A	B	M	GESTIONADO
Comunicaciones	Switch Acceso	Condiciones inadecuadas de temperatura o humedad	A	B	M	GESTIONADO
Comunicaciones	Switch Acceso	Errores de mantenimiento/actualización	M	B	M	GESTIONADO
Comunicaciones	Switch Acceso	Interrupción de servicios de soporte	A	B	A	DEFINIDO
Comunicaciones	Switch Acceso	Errores de administrador	A	B	A	DEFINIDO
Comunicaciones	Switch Acceso	Errores de configuración	A	B	A	DEFINIDO
Comunicaciones	Switch Acceso	Incendios	MA	B	M	GESTIONADO
Comunicaciones	Balanceadores de carga	Denegación de Servicio	A	M	A	DEFINIDO
Comunicaciones	Balanceadores de carga	Manipulación de configuraciones	MA	B	A	DEFINIDO
Comunicaciones	Balanceadores de carga	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
Comunicaciones	Balanceadores de carga	Terremotos	MA	B	MA	REPETIBLE
Comunicaciones	Balanceadores de carga	Erupción Volcánica	A	B	MA	REPETIBLE
Comunicaciones	Balanceadores de carga	Corte de Suministro eléctrico	A	B	M	GESTIONADO
Comunicaciones	Balanceadores de carga	Condiciones inadecuadas de temperatura o humedad	A	B	M	GESTIONADO
Comunicaciones	Balanceadores de carga	Errores de mantenimiento/actualización	M	B	M	GESTIONADO
Comunicaciones	Balanceadores de carga	Interrupción de servicios de soporte	A	B	A	DEFINIDO
Comunicaciones	Balanceadores de carga	Errores de administrador	A	B	A	DEFINIDO
Comunicaciones	Balanceadores de carga	Errores de configuración	A	B	A	DEFINIDO
Comunicaciones	Balanceadores de carga	Incendios	MA	B	M	GESTIONADO

Comunicaciones	Balanceadores ISP	Denegación de Servicio	A	M	A	DEFINIDO
Comunicaciones	Balanceadores ISP	Manipulación de configuraciones	MA	B	A	DEFINIDO
Comunicaciones	Balanceadores ISP	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
Comunicaciones	Balanceadores ISP	Terremotos	MA	B	MA	REPETIBLE
Comunicaciones	Balanceadores ISP	Erupción Volcánica	A	B	MA	REPETIBLE
Comunicaciones	Balanceadores ISP	Corte de Suministro eléctrico	A	B	M	GESTIONADO
Comunicaciones	Balanceadores ISP	Condiciones inadecuadas de temperatura o humedad	A	B	M	GESTIONADO
Comunicaciones	Balanceadores ISP	Errores de mantenimiento/actualización	M	B	M	GESTIONADO
Comunicaciones	Balanceadores ISP	Interrupción de servicios de soporte	A	B	A	DEFINIDO
Comunicaciones	Balanceadores ISP	Errores de administrador	A	B	A	DEFINIDO
Comunicaciones	Balanceadores ISP	Errores de configuración	A	B	A	DEFINIDO
Comunicaciones	Balanceadores ISP	Incendios	MA	B	M	GESTIONADO
Seguridad	Firewall	Manipulación de configuraciones	MA	B	A	DEFINIDO
Seguridad	Firewall	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
Seguridad	Firewall	Terremotos	MA	B	MA	REPETIBLE
Seguridad	Firewall	Erupción Volcánica	A	B	MA	REPETIBLE
Seguridad	Firewall	Corte de Suministro eléctrico	A	B	M	GESTIONADO
Seguridad	Firewall	Condiciones inadecuadas de temperatura o humedad	A	B	M	GESTIONADO
Seguridad	Firewall	Errores de mantenimiento/actualización	M	B	M	GESTIONADO
Seguridad	Firewall	Interrupción de servicios de soporte	A	B	A	DEFINIDO
Seguridad	Firewall	Errores de administrador	A	B	A	DEFINIDO
Seguridad	Firewall	Errores de configuración	A	B	A	DEFINIDO
Seguridad	Firewall	Incendios	MA	B	M	GESTIONADO
Seguridad	IPS	Manipulación de configuraciones	MA	B	A	DEFINIDO
Seguridad	IPS	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
Seguridad	IPS	Terremotos	MA	B	MA	REPETIBLE
Seguridad	IPS	Erupción Volcánica	A	B	MA	REPETIBLE
Seguridad	IPS	Corte de Suministro eléctrico	A	B	M	GESTIONADO

Seguridad	IPS	Condiciones inadecuadas de temperatura o humedad	A	B	M	GESTIONADO
Seguridad	IPS	Errores de mantenimiento/actualización	M	B	M	GESTIONADO
Seguridad	IPS	Interrupción de servicios de soporte	A	B	A	DEFINIDO
Seguridad	IPS	Errores de administrador	A	B	A	DEFINIDO
Seguridad	IPS	Errores de configuración	A	B	A	DEFINIDO
Seguridad	IPS	Incendios	MA	B	M	GESTIONADO
Seguridad	Antivirus	Manipulación de configuraciones	MA	B	A	DEFINIDO
Seguridad	Antivirus	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
Seguridad	Antivirus	Terremotos	MA	B	MA	REPETIBLE
Seguridad	Antivirus	Erupción Volcánica	A	B	MA	REPETIBLE
Seguridad	Antivirus	Errores de mantenimiento/actualización	A	M	M	GESTIONADO
Seguridad	Antivirus	Interrupción de servicios de soporte	A	B	A	DEFINIDO
Seguridad	Antivirus	Errores de administrador	A	B	A	DEFINIDO
Seguridad	Antivirus	Errores de configuración	A	B	A	DEFINIDO
Seguridad	Antivirus	Incendios	MA	B	M	GESTIONADO
Respaldos	Librería Virtual	Manipulación de configuraciones	MA	B	A	DEFINIDO
Respaldos	Librería Virtual	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
Respaldos	Librería Virtual	Terremotos	MA	B	MA	REPETIBLE
Respaldos	Librería Virtual	Erupción Volcánica	A	B	MA	REPETIBLE
Respaldos	Librería Virtual	Corte de Suministro eléctrico	A	B	M	GESTIONADO
Respaldos	Librería Virtual	Condiciones inadecuadas de temperatura o humedad	A	B	M	GESTIONADO
Respaldos	Librería Virtual	Errores de mantenimiento/actualización	A	B	M	GESTIONADO
Respaldos	Librería Virtual	Interrupción de servicios de soporte	A	B	A	DEFINIDO
Respaldos	Librería Virtual	Errores de administrador	A	B	A	DEFINIDO
Respaldos	Librería Virtual	Errores de configuración	A	B	A	DEFINIDO
Respaldos	Librería Virtual	Incendios	MA	B	M	GESTIONADO
Respaldos	Controladora	Manipulación de configuraciones	MA	B	A	DEFINIDO
Respaldos	Controladora	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE

Respaldos	Controladora	Terremotos	MA	B	MA	REPETIBLE
Respaldos	Controladora	Erupción Volcánica	A	B	MA	REPETIBLE
Respaldos	Controladora	Corte de Suministro eléctrico	A	B	M	GESTIONADO
Respaldos	Controladora	Condiciones inadecuadas de temperatura o humedad	A	B	M	GESTIONADO
Respaldos	Controladora	Errores de mantenimiento/actualización	A	B	M	GESTIONADO
Respaldos	Controladora	Interrupción de servicios de soporte	A	B	A	DEFINIDO
Respaldos	Controladora	Errores de administrador	A	B	A	DEFINIDO
Respaldos	Controladora	Errores de configuración	A	B	A	DEFINIDO
Respaldos	Controladora	Incendios	MA	B	M	GESTIONADO
Bases de Datos	Sistema de Bases de Datos	Malware	A	M	M	GESTIONADO
Bases de Datos	Sistema de Bases de Datos	Manipulación de configuraciones	A	B	M	GESTIONADO
Bases de Datos	Sistema de Bases de Datos	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
Bases de Datos	Sistema de Bases de Datos	Terremotos	MA	B	MA	REPETIBLE
Bases de Datos	Sistema de Bases de Datos	Erupción Volcánica	A	B	MA	REPETIBLE
Bases de Datos	Sistema de Bases de Datos	Errores de mantenimiento/actualización	A	B	M	GESTIONADO
Bases de Datos	Sistema de Bases de Datos	Interrupción de servicios de soporte	A	B	A	DEFINIDO
Bases de Datos	Sistema de Bases de Datos	Errores de administrador	A	B	M	GESTIONADO
Bases de Datos	Sistema de Bases de Datos	Errores de configuración	A	B	M	GESTIONADO
Bases de Datos	Sistema de Bases de Datos	Incendios	MA	B	M	GESTIONADO
Sistemas Operativos	Microsoft Windows Server 2012	Malware	A	M	M	GESTIONADO
Sistemas Operativos	Microsoft Windows Server 2012	Manipulación de configuraciones	A	B	A	DEFINIDO
Sistemas Operativos	Microsoft Windows Server 2012	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
Sistemas Operativos	Microsoft Windows Server 2012	Terremotos	MA	B	MA	REPETIBLE
Sistemas Operativos	Microsoft Windows Server 2012	Erupción Volcánica	A	B	MA	REPETIBLE

Sistemas Operativos	Microsoft Windows Server 2012	Errores de mantenimiento/actualización	A	B	MA	REPETIBLE
Sistemas Operativos	Microsoft Windows Server 2012	Interrupción de servicios de soporte	A	B	A	DEFINIDO
Sistemas Operativos	Microsoft Windows Server 2012	Errores de administrador	A	B	A	DEFINIDO
Sistemas Operativos	Microsoft Windows Server 2012	Errores de configuración	A	B	A	DEFINIDO
Sistemas Operativos	Microsoft Windows Server 2012	Incendios	MA	B	M	GESTIONADO
Sistemas Operativos	Linux Red Hat	Malware	A	M	M	GESTIONADO
Sistemas Operativos	Linux Red Hat	Manipulación de configuraciones	A	B	A	DEFINIDO
Sistemas Operativos	Linux Red Hat	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
Sistemas Operativos	Linux Red Hat	Terremotos	MA	B	MA	REPETIBLE
Sistemas Operativos	Linux Red Hat	Erupción Volcánica	A	B	MA	REPETIBLE
Sistemas Operativos	Linux Red Hat	Errores de mantenimiento/actualización	A	B	MA	REPETIBLE
Sistemas Operativos	Linux Red Hat	Interrupción de servicios de soporte	A	B	A	DEFINIDO
Sistemas Operativos	Linux Red Hat	Errores de administrador	A	B	A	DEFINIDO
Sistemas Operativos	Linux Red Hat	Errores de configuración	A	B	A	DEFINIDO
Sistemas Operativos	Linux Red Hat	Incendios	MA	B	M	GESTIONADO
Aplicativos	eSigef	Malware	A	M	M	GESTIONADO
Aplicativos	eSigef	Denegación de Servicio	A	M	A	DEFINIDO
Aplicativos	eSigef	Alteración de Información	MA	M	A	DEFINIDO
Aplicativos	eSigef	Destrucción de Información	MA	B	M	GESTIONADO
Aplicativos	eSigef	Fugas de Información	M	M	A	DEFINIDO
Aplicativos	eSigef	Suplantación de Identidad	M	M	M	GESTIONADO
Aplicativos	eSigef	Abuso de privilegios de acceso	MA	M	A	DEFINIDO
Aplicativos	eSigef	Interceptación de información	A	M	M	GESTIONADO
Aplicativos	eSigef	Manipulación de programas	M	B	M	GESTIONADO
Aplicativos	eSigef	Manipulación de configuraciones	A	M	M	GESTIONADO
Aplicativos	eSigef	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
Aplicativos	eSigef	Terremotos	MA	B	MA	REPETIBLE
Aplicativos	eSigef	Erupción Volcánica	A	B	MA	REPETIBLE
Aplicativos	eSigef	Agotamiento de recursos	A	M	M	GESTIONADO
Aplicativos	eSigef	Indisponibilidad del personal	A	M	MA	REPETIBLE

Aplicativos	eSigef	Fallo de servicios de comunicaciones	MA	B	M	GESTIONADO
Aplicativos	eSigef	Errores de administrador	A	B	M	GESTIONADO
Aplicativos	eSigef	Errores de configuración	A	B	M	GESTIONADO
Aplicativos	eSigef	Incendios	MA	B	M	GESTIONADO
Aplicativos	eSipren	Malware	A	M	M	GESTIONADO
Aplicativos	eSipren	Denegación de Servicio	A	M	A	DEFINIDO
Aplicativos	eSipren	Alteración de Información	MA	M	A	DEFINIDO
Aplicativos	eSipren	Destrucción de Información	MA	B	M	GESTIONADO
Aplicativos	eSipren	Fugas de Información	M	M	A	DEFINIDO
Aplicativos	eSipren	Suplantación de Identidad	M	M	M	GESTIONADO
Aplicativos	eSipren	Abuso de privilegios de acceso	MA	M	A	DEFINIDO
Aplicativos	eSipren	Interceptación de información	A	M	M	GESTIONADO
Aplicativos	eSipren	Manipulación de programas	M	B	M	GESTIONADO
Aplicativos	eSipren	Manipulación de configuraciones	A	M	M	GESTIONADO
Aplicativos	eSipren	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
Aplicativos	eSipren	Terremotos	MA	B	MA	REPETIBLE
Aplicativos	eSipren	Erupción Volcánica	A	B	MA	REPETIBLE
Aplicativos	eSipren	Agotamiento de recursos	A	M	M	GESTIONADO
Aplicativos	eSipren	Indisponibilidad del personal	A	M	MA	REPETIBLE
Aplicativos	eSipren	Fallo de servicios de comunicaciones	MA	B	M	GESTIONADO
Aplicativos	eSipren	Errores de administrador	A	B	M	GESTIONADO
Aplicativos	eSipren	Errores de configuración	A	B	M	GESTIONADO
Aplicativos	eSipren	Incendios	MA	B	M	GESTIONADO
Aplicativos	eSByE	Malware	A	M	M	GESTIONADO
Aplicativos	eSByE	Denegación de Servicio	A	M	A	DEFINIDO
Aplicativos	eSByE	Alteración de Información	MA	M	A	DEFINIDO
Aplicativos	eSByE	Destrucción de Información	MA	B	M	GESTIONADO
Aplicativos	eSByE	Fugas de Información	M	M	A	DEFINIDO
Aplicativos	eSByE	Suplantación de Identidad	M	A	A	DEFINIDO
Aplicativos	eSByE	Abuso de privilegios de acceso	MA	M	A	DEFINIDO
Aplicativos	eSByE	Interceptación de información	A	A	A	DEFINIDO
Aplicativos	eSByE	Manipulación de programas	M	B	M	GESTIONADO
Aplicativos	eSByE	Manipulación de configuraciones	A	M	M	GESTIONADO

Aplicativos	eSByE	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
Aplicativos	eSByE	Terremotos	MA	B	MA	REPETIBLE
Aplicativos	eSByE	Erupción Volcánica	A	B	MA	REPETIBLE
Aplicativos	eSByE	Agotamiento de recursos	A	M	M	GESTIONADO
Aplicativos	eSByE	Indisponibilidad del personal	A	M	MA	REPETIBLE
Aplicativos	eSByE	Fallo de servicios de comunicaciones	MA	B	M	GESTIONADO
Aplicativos	eSByE	Errores de administrador	A	B	M	GESTIONADO
Aplicativos	eSByE	Errores de configuración	A	B	M	GESTIONADO
Aplicativos	eSByE	Incendios	MA	B	M	GESTIONADO
Aplicativos	SPRYN	Malware	A	M	M	GESTIONADO
Aplicativos	SPRYN	Denegación de Servicio	A	M	A	DEFINIDO
Aplicativos	SPRYN	Alteración de Información	MA	M	A	DEFINIDO
Aplicativos	SPRYN	Destrucción de Información	MA	B	M	GESTIONADO
Aplicativos	SPRYN	Fugas de Información	M	M	A	DEFINIDO
Aplicativos	SPRYN	Suplantación de Identidad	M	M	M	GESTIONADO
Aplicativos	SPRYN	Abuso de privilegios de acceso	MA	M	A	DEFINIDO
Aplicativos	SPRYN	Interceptación de información	A	M	M	GESTIONADO
Aplicativos	SPRYN	Manipulación de programas	M	B	M	GESTIONADO
Aplicativos	SPRYN	Manipulación de configuraciones	A	M	M	GESTIONADO
Aplicativos	SPRYN	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
Aplicativos	SPRYN	Terremotos	MA	B	MA	REPETIBLE
Aplicativos	SPRYN	Erupción Volcánica	A	B	MA	REPETIBLE
Aplicativos	SPRYN	Agotamiento de recursos	A	M	M	GESTIONADO
Aplicativos	SPRYN	Indisponibilidad del personal	A	M	MA	REPETIBLE
Aplicativos	SPRYN	Fallo de servicios de comunicaciones	MA	B	M	GESTIONADO
Aplicativos	SPRYN	Errores de administrador	A	B	M	GESTIONADO
Aplicativos	SPRYN	Errores de configuración	A	B	M	GESTIONADO
Aplicativos	SPRYN	Incendios	MA	B	M	GESTIONADO
Aplicativos	Servicios Web	Denegación de Servicio	A	M	A	DEFINIDO
Aplicativos	Servicios Web	Alteración de Información	MA	A	A	DEFINIDO
Aplicativos	Servicios Web	Destrucción de Información	MA	B	M	GESTIONADO
Aplicativos	Servicios Web	Fugas de Información	M	M	A	DEFINIDO
Aplicativos	Servicios Web	Suplantación de Identidad	A	M	A	DEFINIDO
Aplicativos	Servicios Web	Abuso de privilegios de acceso	A	M	A	DEFINIDO

Aplicativos	Servicios Web	Interceptación de información	A	M	A	DEFINIDO
Aplicativos	Servicios Web	Manipulación de programas	M	B	M	GESTIONADO
Aplicativos	Servicios Web	Manipulación de configuraciones	A	M	M	GESTIONADO
Aplicativos	Servicios Web	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
Aplicativos	Servicios Web	Terremotos	MA	B	MA	REPETIBLE
Aplicativos	Servicios Web	Erupción Volcánica	A	B	MA	REPETIBLE
Aplicativos	Servicios Web	Agotamiento de recursos	A	M	M	GESTIONADO
Aplicativos	Servicios Web	Indisponibilidad del personal	A	M	MA	REPETIBLE
Aplicativos	Servicios Web	Fallo de servicios de comunicaciones	MA	B	M	GESTIONADO
Aplicativos	Servicios Web	Errores de administrador	A	B	M	GESTIONADO
Aplicativos	Servicios Web	Errores de configuración	A	B	M	GESTIONADO
Aplicativos	Servicios Web	Incendios	MA	B	M	GESTIONADO
Información	Almacenada	Malware	A	M	A	DEFINIDO
Información	Almacenada	Alteración de Información	MA	M	M	GESTIONADO
Información	Almacenada	Destrucción de Información	MA	B	M	GESTIONADO
Información	Almacenada	Acceso no autorizado a la Información	A	M	M	GESTIONADO
Información	Almacenada	Suplantación de Identidad	A	M	M	GESTIONADO
Información	Almacenada	Abuso de privilegios de acceso	A	M	A	DEFINIDO
Información	Almacenada	Manipulación de programas	A	M	A	DEFINIDO
Información	Almacenada	Ingeniería Social	A	M	A	DEFINIDO
Información	Almacenada	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
Información	Almacenada	Terremotos	MA	B	MA	REPETIBLE
Información	Almacenada	Erupción Volcánica	A	B	MA	REPETIBLE
Información	Almacenada	Errores de usuarios	A	M	M	GESTIONADO
Información	Almacenada	Incendios	MA	B	M	GESTIONADO
Información	En tránsito	Alteración de Información	MA	M	A	DEFINIDO
Información	En tránsito	Acceso no autorizado a la Información	MA	M	A	DEFINIDO
Información	En tránsito	Suplantación de Identidad	MA	M	A	DEFINIDO
Información	En tránsito	Interceptación de información	MA	M	A	DEFINIDO
Información	En tránsito	Repudio	A	M	A	DEFINIDO
Información	En tránsito	Fallo de servicios de comunicaciones	MA	B	M	GESTIONADO

5.7 Evaluación de riesgos

Una vez establecidos los niveles de riesgo para los diferentes activos definidos, se procede a definir las medidas de protección, controles, salvaguardas o contramedidas que se deben implementar para cada uno de los activos en función del impacto que pueda representar la materialización de la amenaza [4].

La tabla 14 muestra el resultado de la evaluación de riesgos, priorizando aquellos que reúnen las siguientes características:

- Impacto: alto, muy alto.
- Probabilidad de ocurrencia: media, alta.
- Necesidad de salvaguardas: alta, muy alta.
- Nivel CMMI: definido, repetible.

Con la finalidad de relacionar las situaciones de riegos con los objetivos de control y controles a ser definidos en el subcapítulo 5.8 para su mitigación, se ha procedido a asignar un identificador a cada situación de riego, mismo que se puede observar en la primera columna de la tabla 14.

Tabla 14. Evaluación de Riesgos

Situación de Riesgo				Impacto	Probabilidad	Necesidad de salvaguardas	Nivel CMMI
ID	Grupo Activo	Activo	Amenaza				
A1	Almacenamiento	Arreglo de discos	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
A2	Almacenamiento	Controladora	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
A3	Almacenamiento	SAN	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
P1	Procesamiento	Servidores Blade	Denegación de Servicio	A	M	A	DEFINIDO
P2	Procesamiento	Servidores Blade	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
P3	Procesamiento	Chasis Blade	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
C1	Comunicaciones	Switch Core	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
C2	Comunicaciones	Switch Distribución	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
C3	Comunicaciones	Switch Acceso	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
C4	Comunicaciones	Balanceadores de carga	Denegación de Servicio	A	M	A	DEFINIDO
C5	Comunicaciones	Balanceadores de carga	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
C6	Comunicaciones	Balanceadores ISP	Denegación de Servicio	A	M	A	DEFINIDO
C7	Comunicaciones	Balanceadores ISP	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
S1	Seguridad	Firewall	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
S2	Seguridad	IPS	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
S3	Seguridad	Antivirus	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE

R1	Respaldos	Librería Virtual	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
R2	Respaldos	Controladora	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
B1	Bases de Datos	Sistema de Bases de Datos	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
SO1	Sistemas Operativos	Microsoft Windows Server 2012	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
SO2	Sistemas Operativos	Linux Red Hat	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
A1	Aplicativos	eSigef	Denegación de Servicio	A	M	A	DEFINIDO
A2	Aplicativos	eSigef	Alteración de Información	MA	M	A	DEFINIDO
A3	Aplicativos	eSigef	Fugas de Información	M	M	A	DEFINIDO
A4	Aplicativos	eSigef	Abuso de privilegios de acceso	MA	M	A	DEFINIDO
A5	Aplicativos	eSigef	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
A6	Aplicativos	eSigef	Indisponibilidad del personal	A	M	MA	REPETIBLE
A7	Aplicativos	eSipren	Denegación de Servicio	A	M	A	DEFINIDO
A8	Aplicativos	eSipren	Alteración de Información	MA	M	A	DEFINIDO
A9	Aplicativos	eSipren	Fugas de Información	M	M	A	DEFINIDO
A10	Aplicativos	eSipren	Abuso de privilegios de acceso	MA	M	A	DEFINIDO
A11	Aplicativos	eSipren	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
A12	Aplicativos	eSipren	Indisponibilidad del personal	A	M	MA	REPETIBLE
A13	Aplicativos	eSByE	Denegación de Servicio	A	M	A	DEFINIDO
A14	Aplicativos	eSByE	Alteración de Información	MA	M	A	DEFINIDO
A15	Aplicativos	eSByE	Fugas de Información	M	M	A	DEFINIDO
A16	Aplicativos	eSByE	Suplantación de Identidad	M	A	A	DEFINIDO
A17	Aplicativos	eSByE	Abuso de privilegios de acceso	MA	M	A	DEFINIDO
A18	Aplicativos	eSByE	Interceptación de información	A	A	A	DEFINIDO
A19	Aplicativos	eSByE	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
A20	Aplicativos	eSByE	Indisponibilidad del personal	A	M	MA	REPETIBLE
A21	Aplicativos	SPRYN	Denegación de Servicio	A	M	A	DEFINIDO
A22	Aplicativos	SPRYN	Alteración de Información	MA	M	A	DEFINIDO
A23	Aplicativos	SPRYN	Fugas de Información	M	M	A	DEFINIDO
A24	Aplicativos	SPRYN	Abuso de privilegios de acceso	MA	M	A	DEFINIDO
A25	Aplicativos	SPRYN	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
A26	Aplicativos	SPRYN	Indisponibilidad del personal	A	M	MA	REPETIBLE
A27	Aplicativos	Servicios Web	Denegación de Servicio	A	M	A	DEFINIDO
A28	Aplicativos	Servicios Web	Alteración de Información	MA	A	A	DEFINIDO
A29	Aplicativos	Servicios Web	Fugas de Información	M	M	A	DEFINIDO
A30	Aplicativos	Servicios Web	Suplantación de Identidad	A	M	A	DEFINIDO

A31	Aplicativos	Servicios Web	Abuso de privilegios de acceso	A	M	A	DEFINIDO
A32	Aplicativos	Servicios Web	Interceptación de información	A	M	A	DEFINIDO
A33	Aplicativos	Servicios Web	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
A34	Aplicativos	Servicios Web	Indisponibilidad del personal	A	M	MA	REPETIBLE
I1	Información	Almacenada	Malware	A	M	A	DEFINIDO
I2	Información	Almacenada	Abuso de privilegios de acceso	A	M	A	DEFINIDO
I3	Información	Almacenada	Manipulación de programas	A	M	A	DEFINIDO
I4	Información	Almacenada	Ingeniería Social	A	M	A	DEFINIDO
I5	Información	Almacenada	Ocupación no autorizada (huelgas)	MA	M	MA	REPETIBLE
I6	Información	En tránsito	Alteración de Información	MA	M	A	DEFINIDO
I7	Información	En tránsito	Acceso no autorizado a la Información	MA	M	A	DEFINIDO
I8	Información	En tránsito	Suplantación de Identidad	MA	M	A	DEFINIDO
I9	Información	En tránsito	Interceptación de información	MA	M	A	DEFINIDO
I10	Información	En tránsito	Repudio	A	M	A	DEFINIDO

5.8 Selección de los objetivos de control y controles

El EGSI establece un conjunto de directrices prioritarias para la Gestión de la Seguridad de la Información, que son generales para su aplicación en las entidades públicas ecuatorianas; sin embargo, en el presente estudio, se pretende limitar el alcance a su aplicación dentro del área o departamento que tiene como responsabilidad principal la operación de los aplicativos web que forman parte del Sistema Nacional de Finanzas Públicas (SINFIP).

El acuerdo ministerial que dispone la implementación del EGSI, cuenta con el anexo 1, que es una recopilación del Anexo A de la norma ISO/IEC 27001:2013, relacionado con los objetivos de control y controles a ser aplicados; por tanto, se tomará como referencia el anexo 1 del EGSI para la selección de los objetivos de control y controles [14].

Del análisis y evaluación de riesgos realizados, los objetivos de control y controles seleccionados están relacionados con:

- Gestión de comunicaciones y operaciones
- Control de Acceso
- Gestión de la continuidad del negocio

5.8.1 Gestión de Comunicaciones y Operaciones

Los objetivos, procedimiento y actividades seleccionados, relacionados con la gestión de comunicaciones y operaciones son:

Gestión del Cambio:

Objetivo: Controlar cambios sobre los servicios y sistemas de procesamiento de información, procesos del negocio, que afecten la seguridad de la información. En particular se pretende controlar y registrar cambios significativos sobre las configuraciones de hardware y software base. El detalle de los controles, procedimientos y actividades se muestran en la figura 13.

Situaciones de riesgos a mitigar: A4, A10, A17, A24, A31, I2.

Responsable: Área de Infraestructura de TI

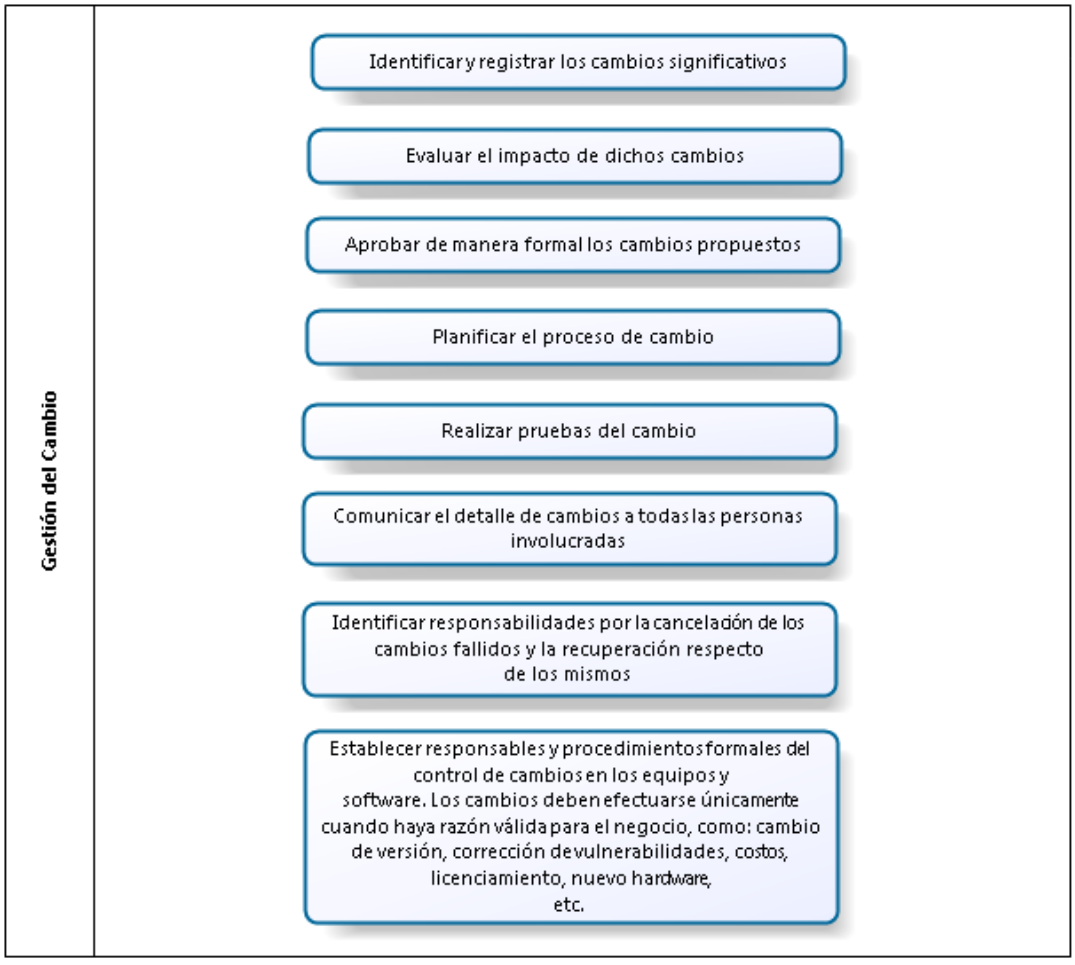

Figura 13. Gestión del Cambio

Distribución de Funciones:

Objetivo: Establecer de forma clara las funciones y responsabilidades entre las diferentes áreas que conforman la Dirección de estudio, para evitar el cruce de funciones y accesos no autorizados a las configuraciones de las diferentes plataformas. El detalle de los controles, procedimientos y actividades se muestran en la figura 14.

Situaciones de riesgos a mitigar: A4, A10, A17, A24, A31, I2.

Responsable: Director de Operaciones, en coordinación con responsables de áreas.

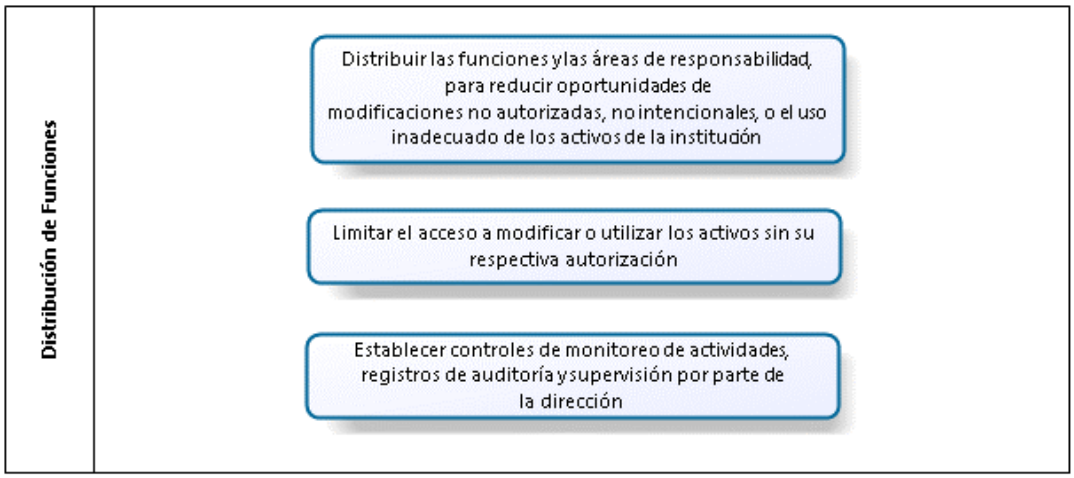

Figura 14. Distribución de Funciones

Separación de las instancias de Desarrollo, Pruebas, Capacitación y Producción:

Objetivo: Separar desde el nivel más bajo posible los ambientes de Desarrollo, Pruebas, Capacitación y Producción, para evitar accesos no autorizados a datos sensibles. Disponer de ambientes similares en capacidad, en la medida de lo posible, a los ambientes de producción. El detalle de los controles, procedimientos y actividades se muestran en la figura 15.

Situaciones de riesgos a mitigar: A2, A4, A8, A10, A14, A17, A22, A24, A28, A31, I2.

Responsable: Todas las áreas de TI.

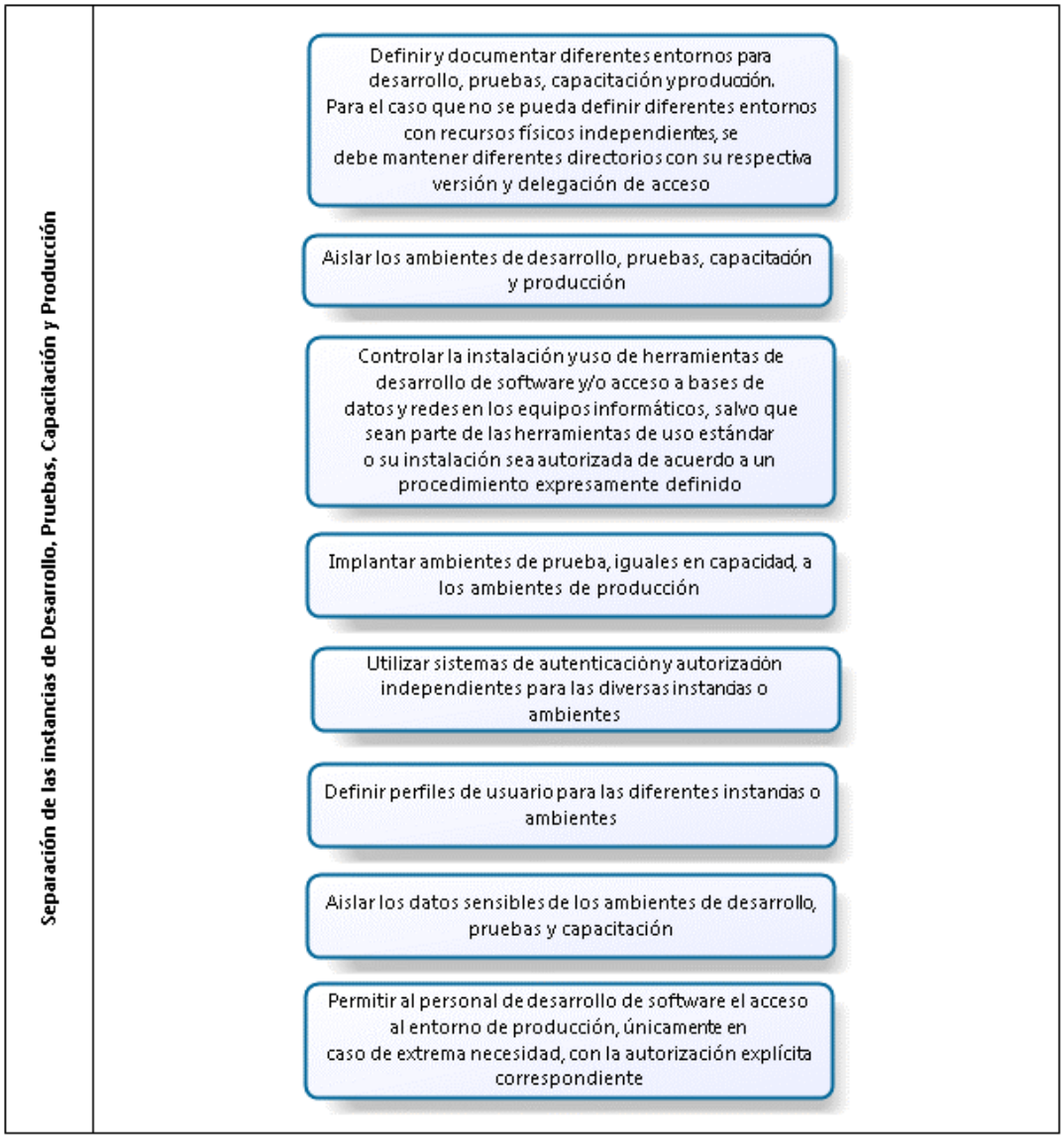

Figura 15. Separación de las instancias de Desarrollo, Pruebas, Capacitación y Producción

Controles contra código malicioso:

Objetivo: Garantizar que la información y los servicios de procesamiento de información estén protegida contra malware o código malicioso, mediante la implantación de controles de detección, prevención y recuperación, combinando con una conciencia apropiada de los usuarios. El detalle de los controles, procedimientos y actividades se muestran en la figura 16.

Situaciones de riesgos a mitigar: P1, C4, C6, A1, A7, A13, A21, A27, I1, I6.

Responsable: Infraestructura de TI y Redes, Comunicaciones y Seguridad.

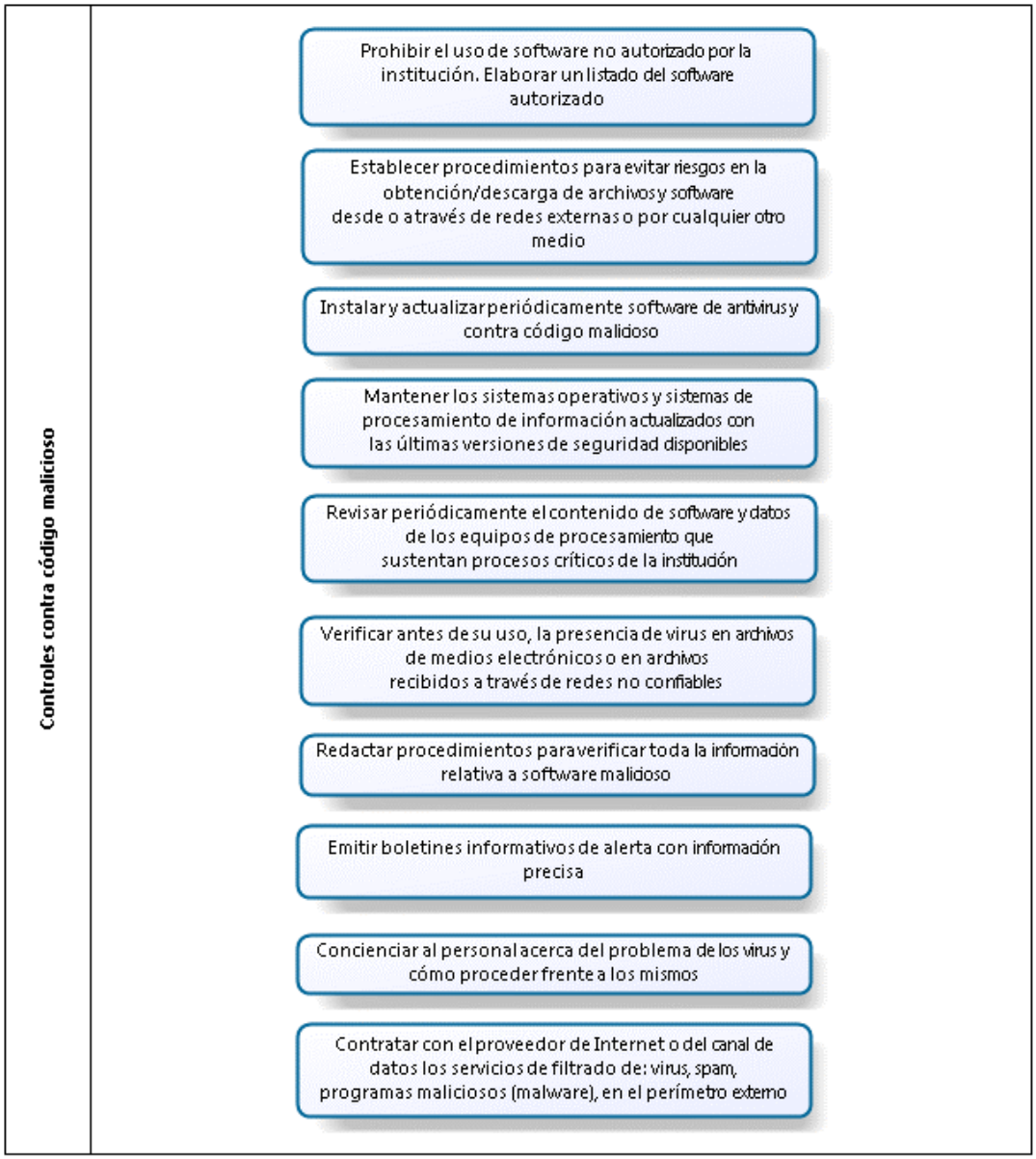

Figura 16. Controles contra código malicioso

Controles contra códigos móviles:

Objetivo: Controlar de forma lógica el acceso de dispositivos móviles a la red LAN institucional, mediante el uso de herramientas de bloqueo y criptografía. El detalle de los controles, procedimientos y actividades se muestran en la figura 17.

Situaciones de riesgos a mitigar: I1, I6.

Responsable: Área de Redes, Comunicaciones y Seguridades

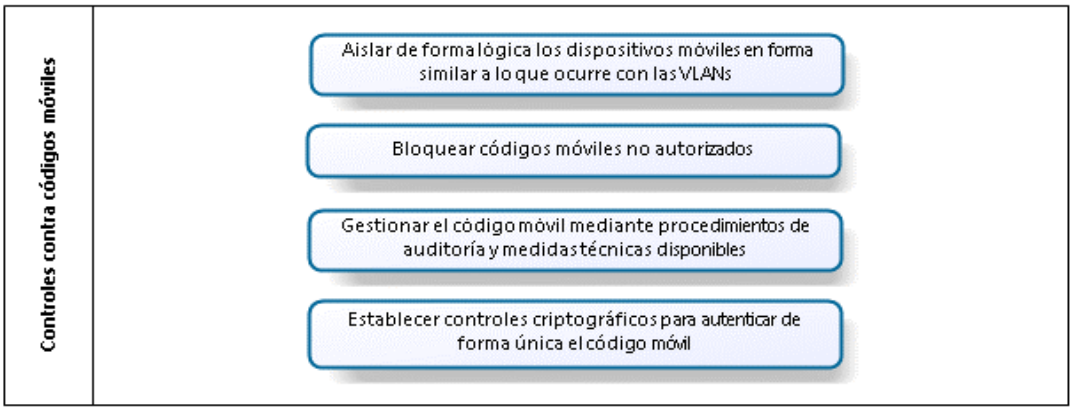

Figura 17. Controles contra códigos móviles

Controles de las redes:

Objetivo: Establecer controles para proteger la confidencialidad e integridad de los datos que viajan a través de las redes públicas, redes locales e inalámbricas a través del uso de VPNs, o esquemas de protección de datos para capas superiores, para todos los servicios. El detalle de los controles y actividades se muestran en la figura 18.

Situaciones de riesgos a mitigar: A18, A32, I6, I7, I8, I9.

Responsable: Área de Redes, Comunicaciones y Seguridad

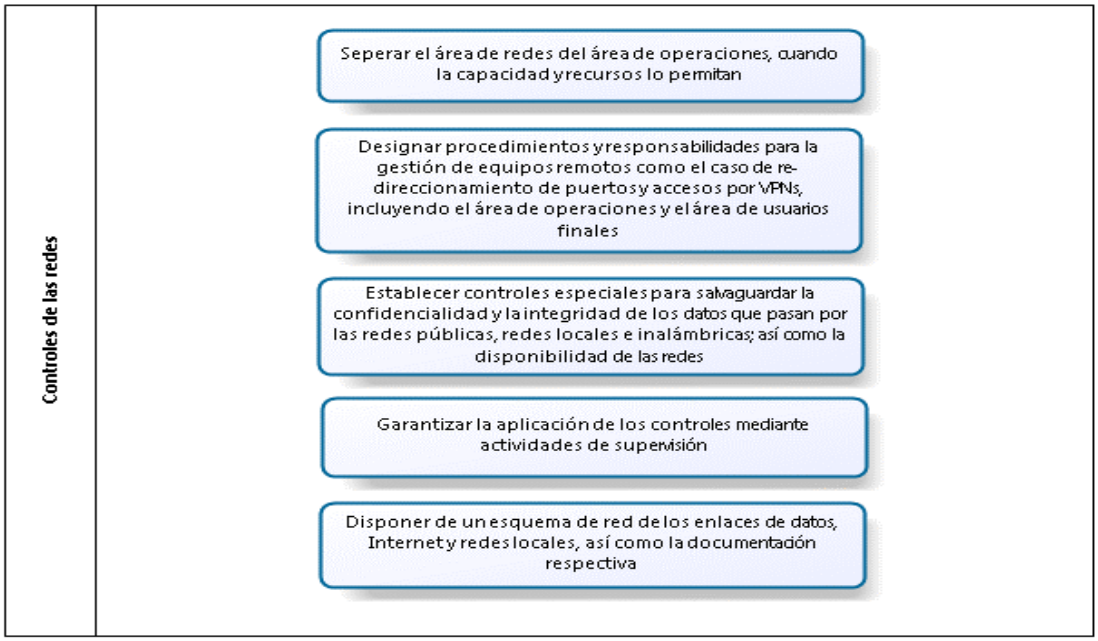

Figura 18. Controles de las redes

Seguridad de los servicios de la red:

Objetivo: Incorporar tecnologías de autenticación y cifrado en los diferentes servicios del SINFIP como son los servicios web ofrecidos a otras instituciones públicas. El detalle de los controles, procedimientos y actividades se muestran en la figura 19.

Situaciones de riesgos a mitigar: A18, A32, I6, I7, I8, I9.

Responsable: Área de Redes, Comunicaciones y Seguridades

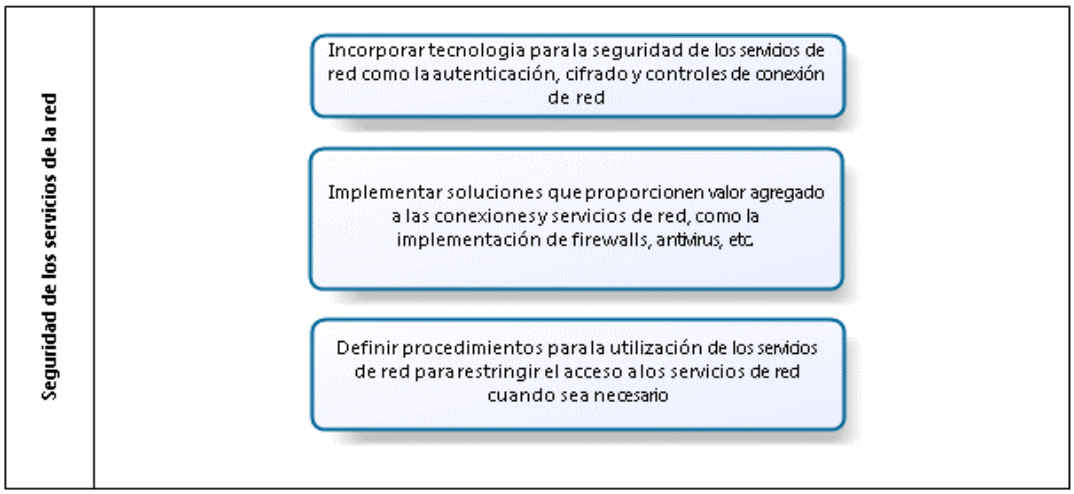

Figura 19. Seguridad de los servicios de la red

Mensajería electrónica:

Objetivo: Mantener la seguridad de la información transferida dentro de la organización y con una entidad externa. Proteger apropiadamente la información incluida en mensajería electrónica. Ver el detalle en la figura 20.

Situaciones de riesgos a mitigar: I6, I7.

Responsable: Área de Redes, Comunicaciones y Seguridades.

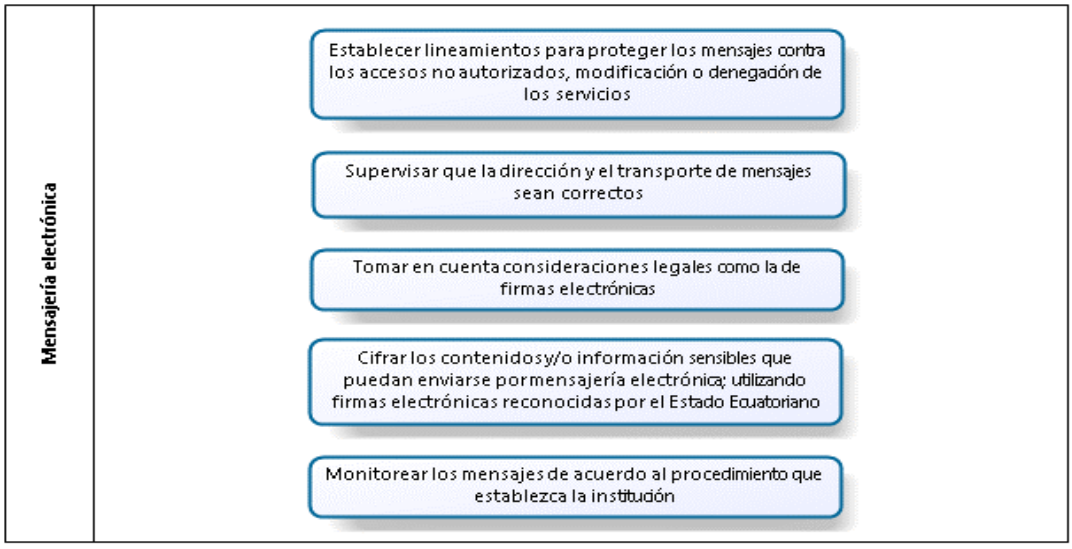

Figura 20. Mensajería Electrónica

Políticas y Procedimientos para el intercambio de información:

Objetivo: Implementar controles, procedimientos y políticas de transferencia formales para proteger la transferencia de información a través de las diferentes alternativas de comunicación. El detalle de los controles, procedimientos y actividades se muestran en la figura 21.

Situaciones de riesgos a mitigar: A3, A9, A15, A23, A29, I6, I7, I9.

Responsable: Área de Redes, Comunicaciones y Seguridades

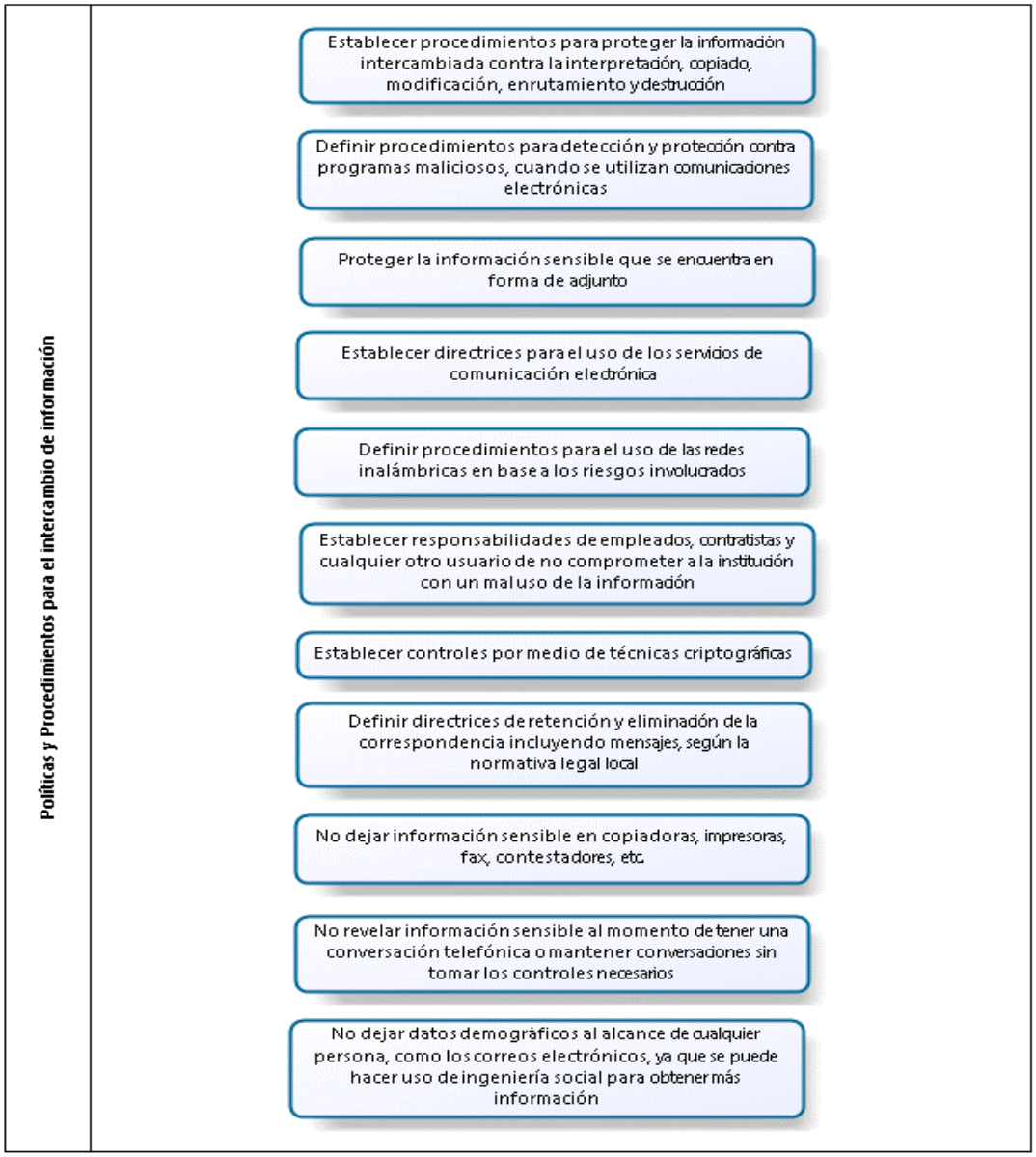

Figura 21. Políticas y Procedimientos para el intercambio de información

Acuerdos para el intercambio de información:

Objetivo: Definir acuerdos de cooperación para la transferencia segura de información de negocio entre la entidad y terceras partes. El detalle de los controles, procedimientos y actividades se muestran en la figura 22.

Situaciones de riesgos a mitigar: A3, A9, A15, A23, A29, I6, I7, I9, I10.

Responsable: Director de Operaciones, en coordinación con el área de Redes, Comunicaciones y Seguridades.

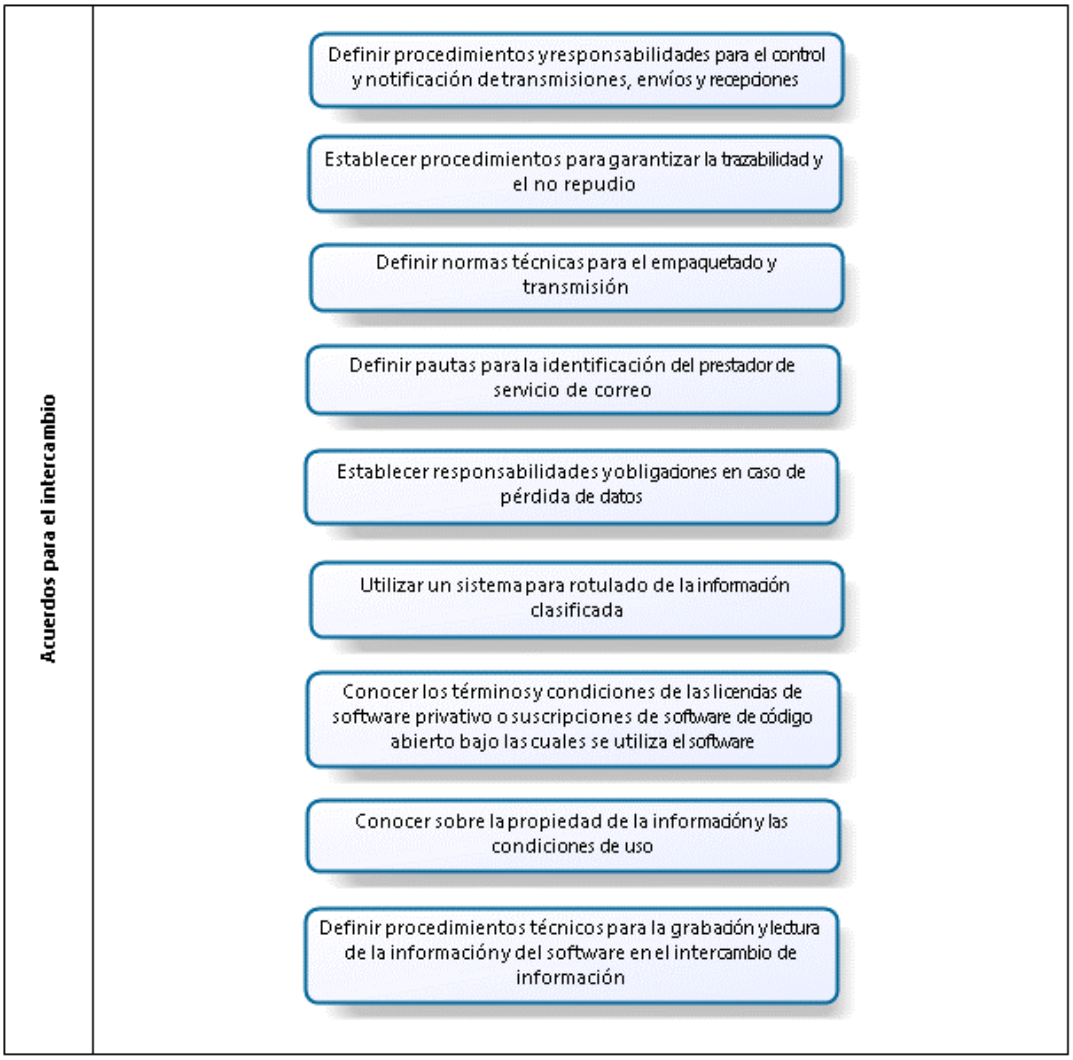

Figura 22. Acuerdos para el intercambio

Transacciones en línea:

Objetivo: Establecer procedimientos para garantizar la confidencialidad, integridad y autenticidad en transacciones realizadas sobre los diferentes servicios, como el uso de firma electrónica y cifrado de canales de comunicación. Involucrar la participación de una entidad certificadora calificada. El detalle de los controles, procedimientos y actividades se muestran en la figura 23.

Situaciones de riesgos a mitigar: A2, A8, A14, A22, A28, I6, I9, I10.

Responsable: Área de Redes, Comunicaciones y Seguridades

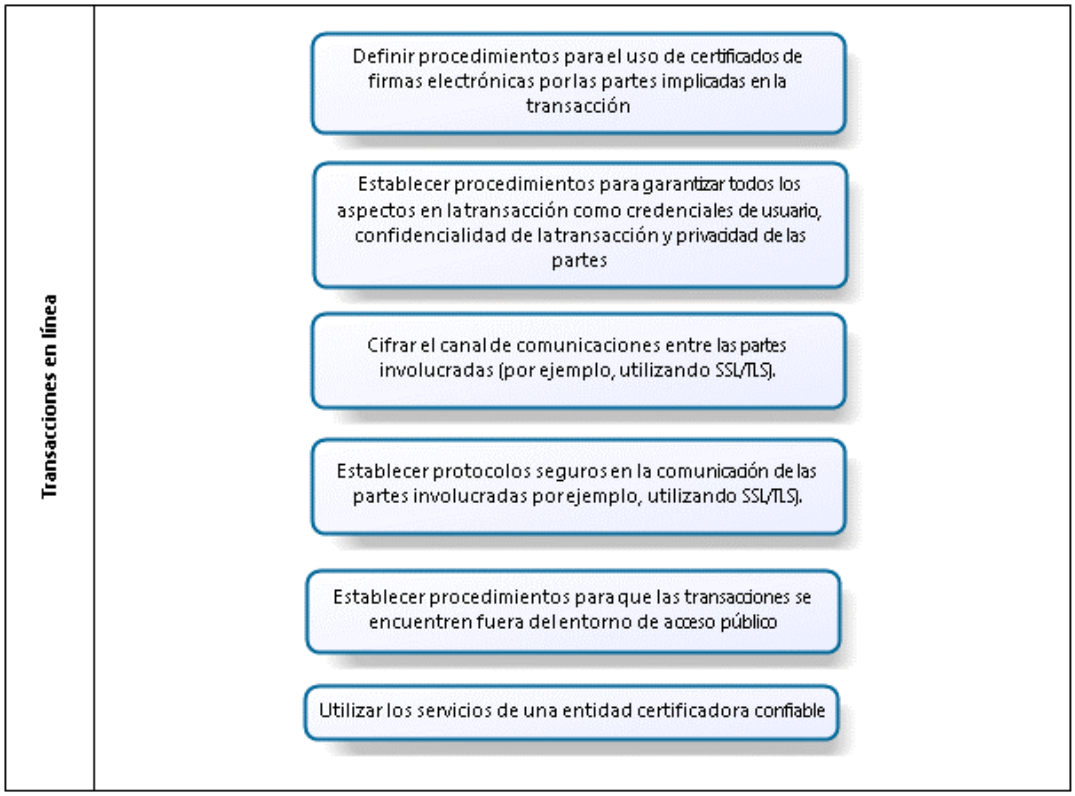

Figura 23. Transacciones en línea

Registro de auditorías:

Objetivo: Registrar toda la información posible relacionada con accesos a servicios y configuraciones, como por ejemplo fecha, hora, y detalle de eventos, para su futuro uso en actividades de auditorías. El detalle de los controles, procedimientos y actividades se muestran en la figura 24.

Situaciones de riesgos a mitigar: A4, A10, A17, A24, A31, I2, I4.

Responsable: Áreas de Infraestructura de TI, y Redes, Comunicaciones y Seguridades

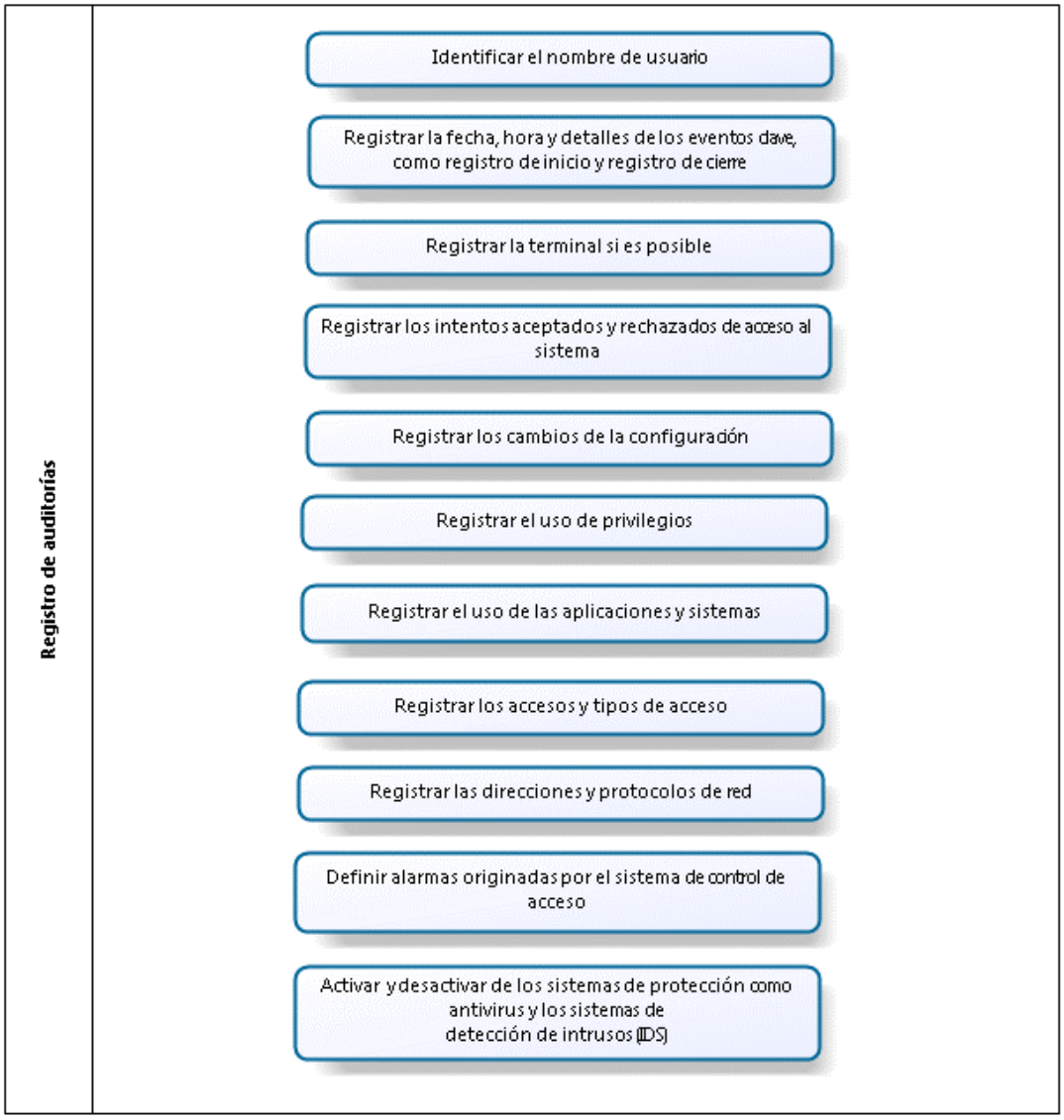

Figura 24. Registro de auditorías

Monitoreo de uso del sistema:

Objetivo: Monitorear accesos autorizados, operaciones privilegiadas, intentos de acceso no autorizados, alertas o fallos del sistema, cambios de configuración, sobre los diferentes sistemas y servicios. El monitoreo debe realizarse de forma continua. El detalle de los controles, procedimientos y actividades se muestran en la figura 25.

Situaciones de riesgos a mitigar: A4, A10, A17, A24, A31, I2, I4.

Responsable: Áreas de Infraestructura de TI, y Redes, Comunicaciones y Seguridades

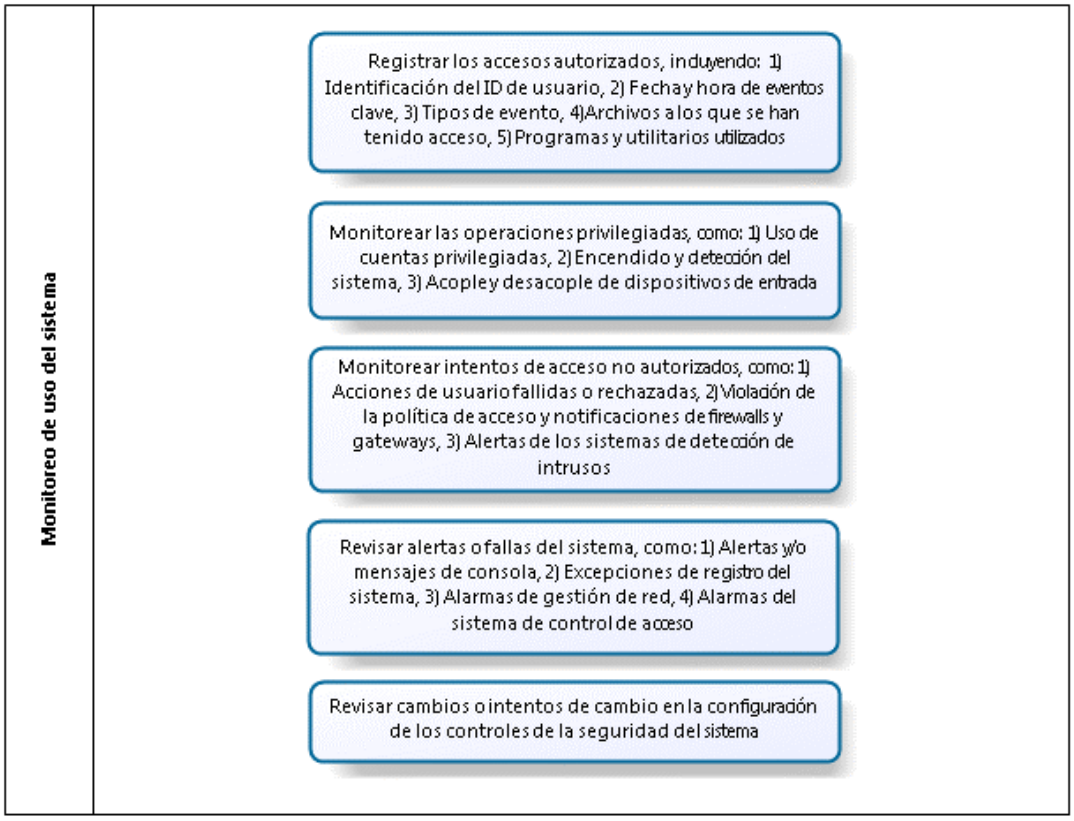

Figura 25. Monitoreo de uso del sistema

Protección del registro de la información:

Objetivo: Proteger la información de registro de todos los eventos generados sobre los diferentes servicios y sistemas, mediante mecanismos adecuados de respaldos. El detalle de los controles, procedimientos y actividades se muestran en la figura 26.

Situaciones de riesgos a mitigar: A4, A10, A17, A24, A31, I2, I4.

Responsable: Área de Infraestructura de TI

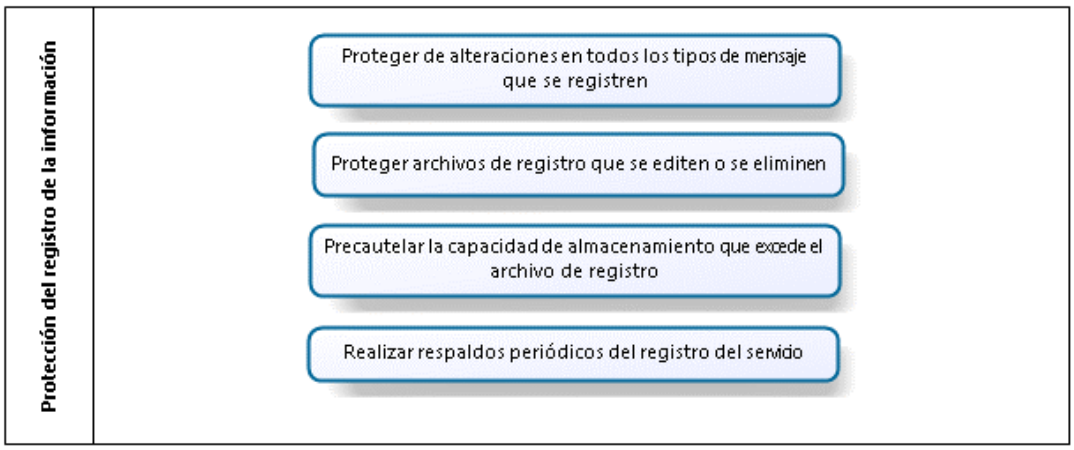

Figura 26. Protección del registro de la información

Registro del administrador y del operador:

Objetivo: Registrar toda la información posible de los eventos generados por el acceso de administradores y operadores a los diferentes sistemas y plataformas. Evitar el uso de nombres genéricos para las identificaciones de cuentas de usuarios. El detalle de los controles, procedimientos y actividades se muestran en la figura 27.

Situaciones de riesgos a mitigar: A4, A10, A17, A24, A31, I2, I4.

Responsable: Áreas de Infraestructura de TI, y Redes, Comunicaciones y Seguridades

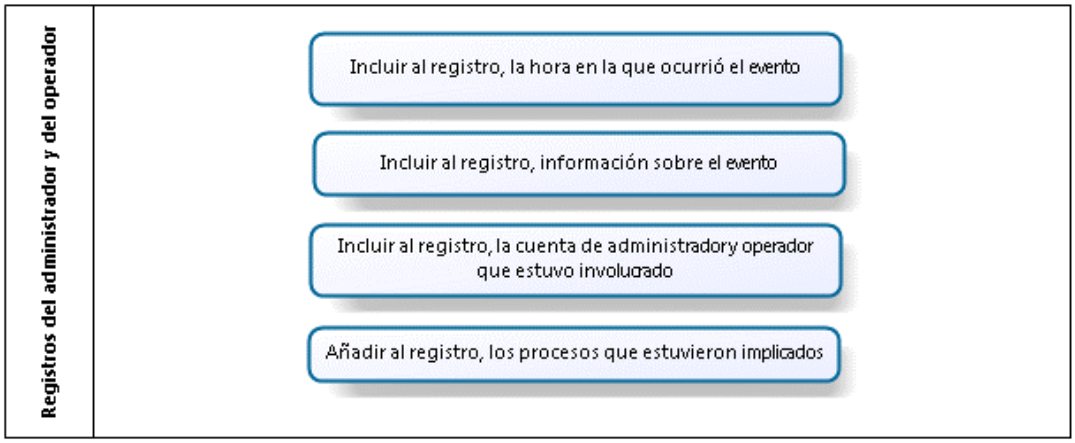

Figura 27. Registros del administrador y del operador

5.8.2 Control de Acceso

Los objetivos, procedimientos y actividades seleccionados, relacionados con la gestión de control de acceso son:

Gestión de privilegios:

Objetivo: Controlar la asignación de privilegios a usuarios de los diferentes servicios, sistemas y sobre todo bases de datos, mediante el establecimiento de un procedimiento formal que incluya la respectiva autorización. El detalle de los controles, procedimientos y actividades se muestran en la figura 28.

Situaciones de riesgos a mitigar: A2, A4, A8, A10, A14, A17, A22, A24, A28, A31, I2, I4.

Responsable: Área de Infraestructura de TI.

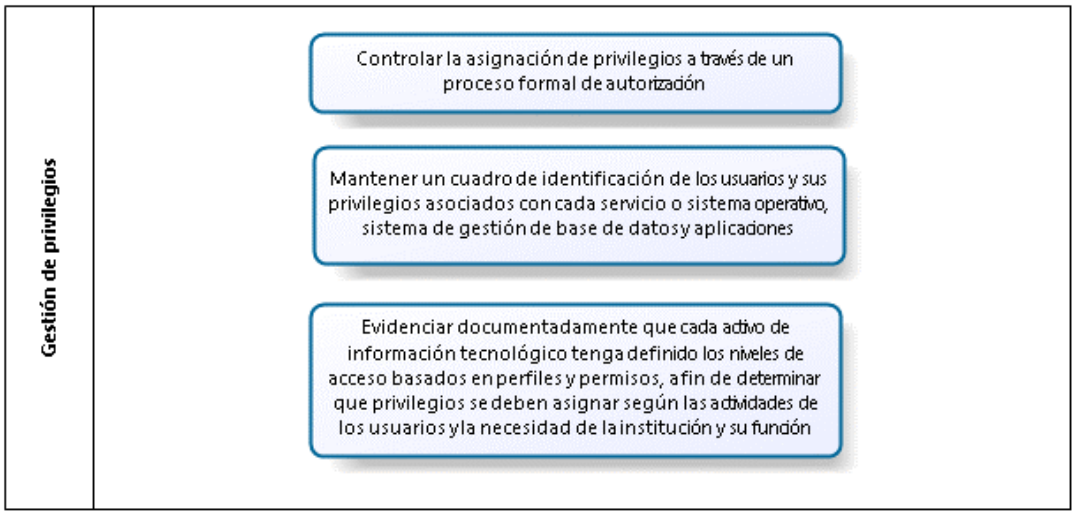

Figura 28. Gestión de privilegios

Gestión de contraseñas para usuarios:

Objetivo: Establecer procedimientos formales de asignación y reseteo de contraseñas, sobre todo para administradores y operadores de los sistemas y servicios. El detalle de los controles, procedimientos y actividades se muestran en la figura 29.

Situaciones de riesgos a mitigar: A2, A4, A8, A10, A14, A16, A17, A22, A24, A28, A30, A31, I2, I4.

Responsable: Área de Infraestructura de TI, y Redes, Comunicaciones y Seguridad

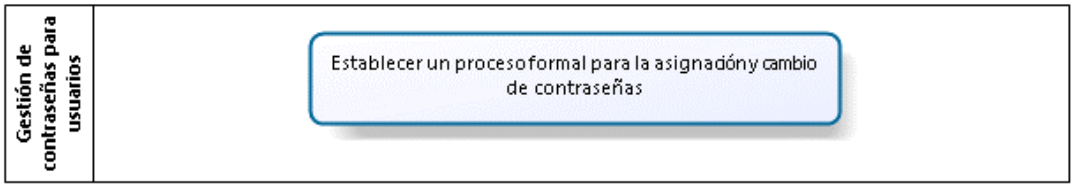

Figura 29. Gestión de contraseñas para usuarios

Revisión de los derechos de acceso de los usuarios:

Objetivo: Mantener un control sobre los derechos de acceso de los usuarios a los diferentes aplicativos y servicios, mediante depuraciones periódicas que se realicen en coordinación con áreas de gestión de talento humano. El detalle de los controles, procedimientos y actividades se muestran en la figura 30.

Situaciones de riesgos a mitigar: A2, A4, A8, A10, A14, A16, A17, A22, A24, A28, A30, A31, I2, I4.

Responsable: Área de Infraestructura de TI.

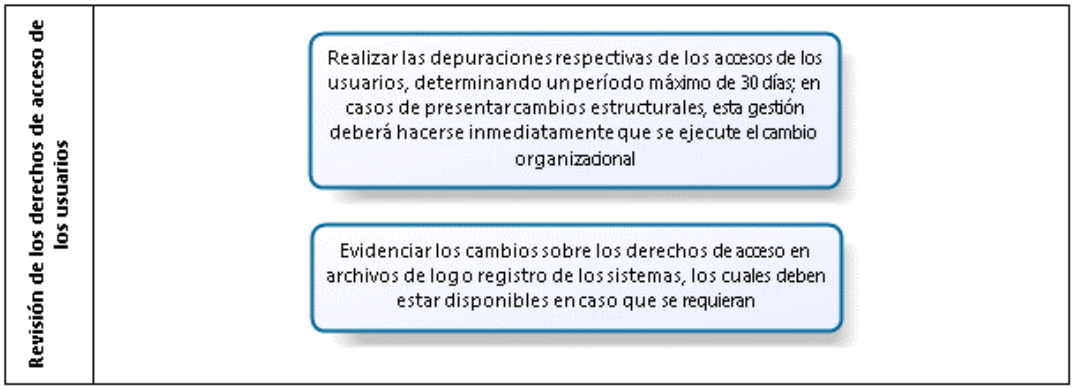

Figura 30. Revisión de los derechos de acceso de los usuarios

Uso de contraseñas:

Objetivo: Disponer de un procedimiento de uso de contraseñas de usuarios, que incluya mecanismos de generación y cambio de contraseñas con altos niveles de seguridad, sobre todo para administradores y operadores de los diferentes servicios y sistemas. El detalle de los controles, procedimientos y actividades se muestran en la figura 31.

Situaciones de riesgos a mitigar: A2, A4, A8, A10, A14, A16, A17, A22, A24, A28, A30, A31, I2, I4.

Responsable: Área de Infraestructura de TI en coordinación con el Oficial de Seguridad de la Información.

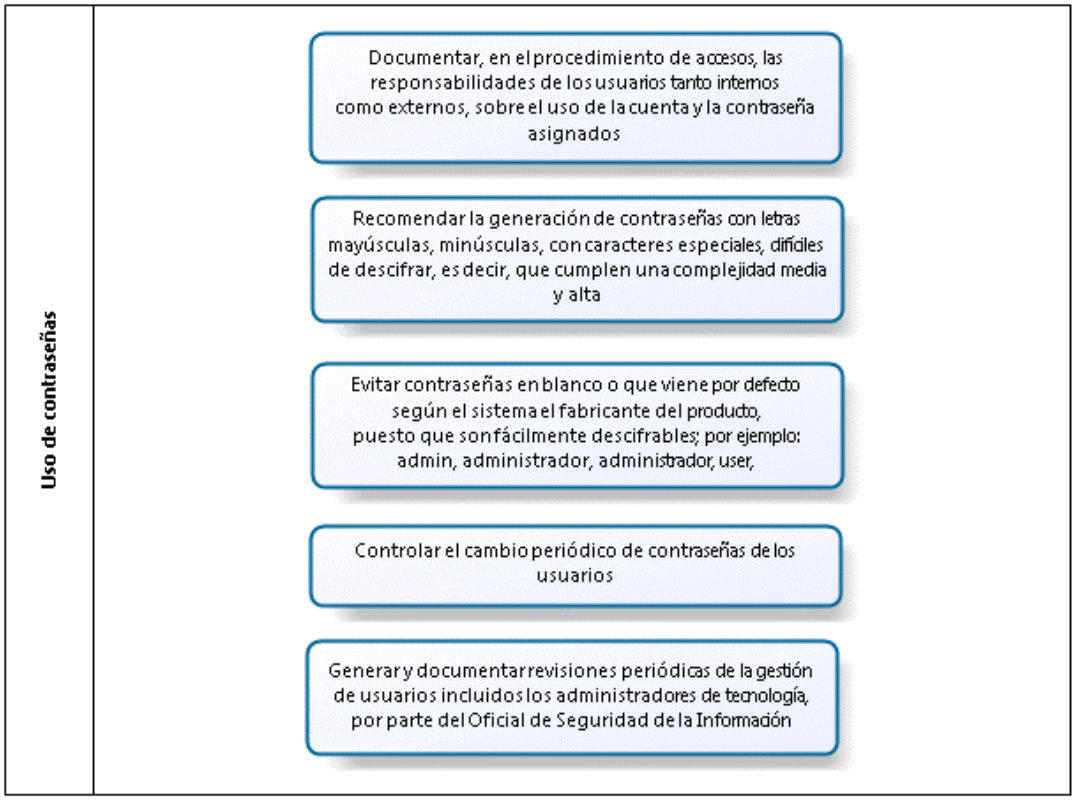

Figura 31. Uso de contraseñas

Equipo de usuario desatendido:

Objetivo: Implementar medidas y mecanismos para evitar que el terminal de los usuarios con privilegios de acceso a servicios de red críticos quede desprotegido ante ausencia del usuario y con sesiones activas. EL detalle del control se muestra en la figura 32.

Situaciones de riesgos a mitigar: A2, A4, A8, A10, A14, A16, A17, A22, A24, A28, A30, A31, I2, I3.

Responsable: Infraestructura de TI.

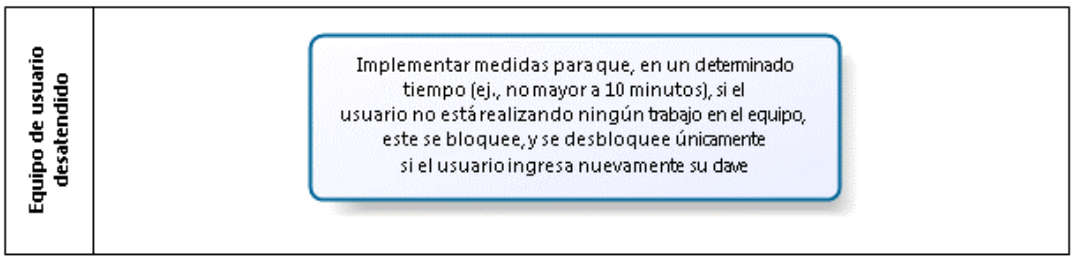

Figura 32. Equipo de usuario desatendido

Políticas de puesto de trabajo despejado y pantalla limpia:

Objetivo: Establecer políticas a ser cumplidas por los usuarios, incluidos administradores y operadores, de los diferentes sistemas, aplicativos y servicios, respecto al manejo de información sensible en formato digital o físico. El control se apoyará en implantación de mecanismos de desconexión automática de terminales desatendidas. El detalle de los controles, procedimientos y actividades se muestran en la figura 33.

Situaciones de riesgos a mitigar: A2, A3, A4, A8, A9, A10, A14, A15, A16, A17, A22, A23, A24, A28, A29, A30, A31, I2, I4.

Responsable: Oficial de Seguridad de la Información en coordinación con el área de Infraestructura de TI.

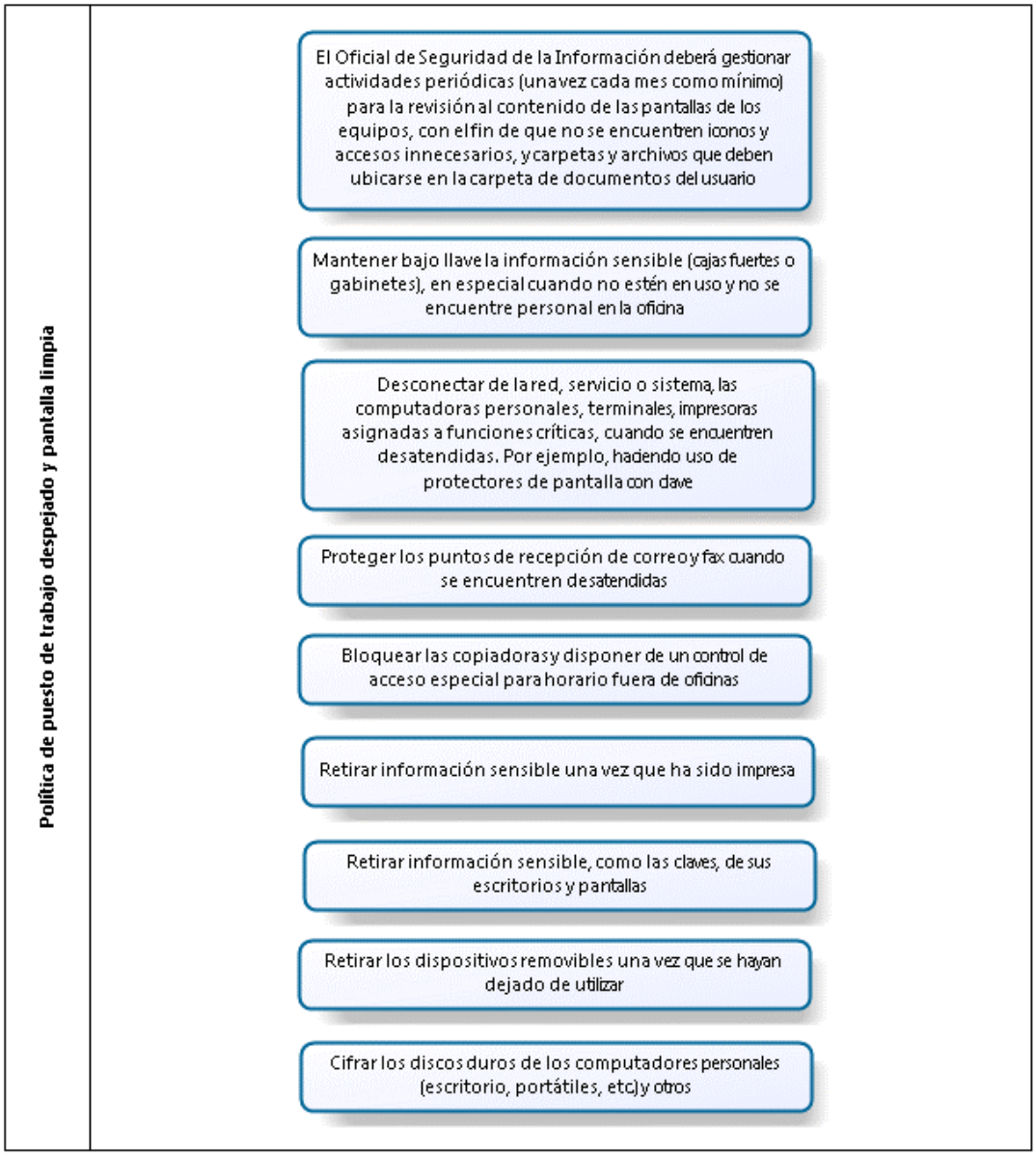

Figura 33. Política de puesto de trabajo despejado y pantalla limpia

Autenticación de usuarios para conexiones externas:

Objetivo: Generar mecanismos para garantizar la seguridad de la información transmitida por los canales de conexión remota, de usuarios administradores que de forma remota necesiten acceder a las configuraciones de sistemas, aplicaciones y servicios. El detalle de los controles, procedimientos y actividades se muestran en la figura 34.

Situaciones de riesgos a mitigar: I6, I7, I8, I9, I10.

Responsable: Área de Redes, Comunicaciones y Seguridades.

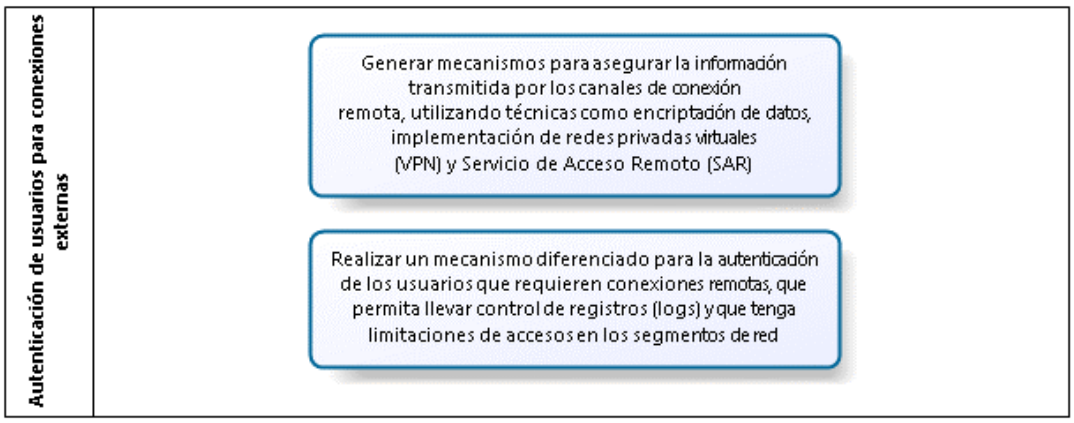

Figura 34. Autenticación de usuarios para conexiones externas

Protección de los puertos de configuración y diagnóstico remoto:

Objetivo: Establecer procedimientos de soporte especializado con el proveedor de este tipo de servicios, que incluya la definición de puertos específicos de comunicación a ser usados El detalle de los controles y actividades se muestran en la figura 35.

Situaciones de riesgos a mitigar: I6, I7, I8, I9, I10.

Responsable: Área de Infraestructura de TI, y, Redes, Comunicaciones y Seguridades.

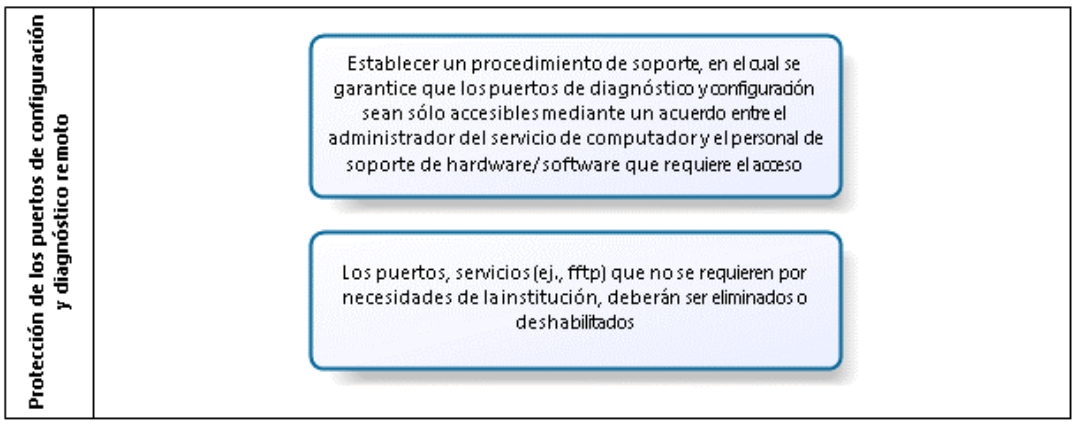

Figura 35. Protección de los puertos de configuración y diagnóstico remoto

Procedimiento de registro de inicio seguro:

Objetivo: Establecer procedimientos para el registro de inicio seguro de usuarios, incluyendo administradores y operadores, que esté acorde a la política de control de acceso de la entidad. Este procedimiento debe apalancarse de mecanismos de monitoreo

y registro de intentos exitosos y fallidos de autenticación en los diferentes sistemas, servicios y aplicativos. El detalle de los controles, procedimientos y actividades se muestran en la figura 36.

Situaciones de riesgos a mitigar: A4, A10, A17, A24, A31, I2.

Responsable: Infraestructura de TI.

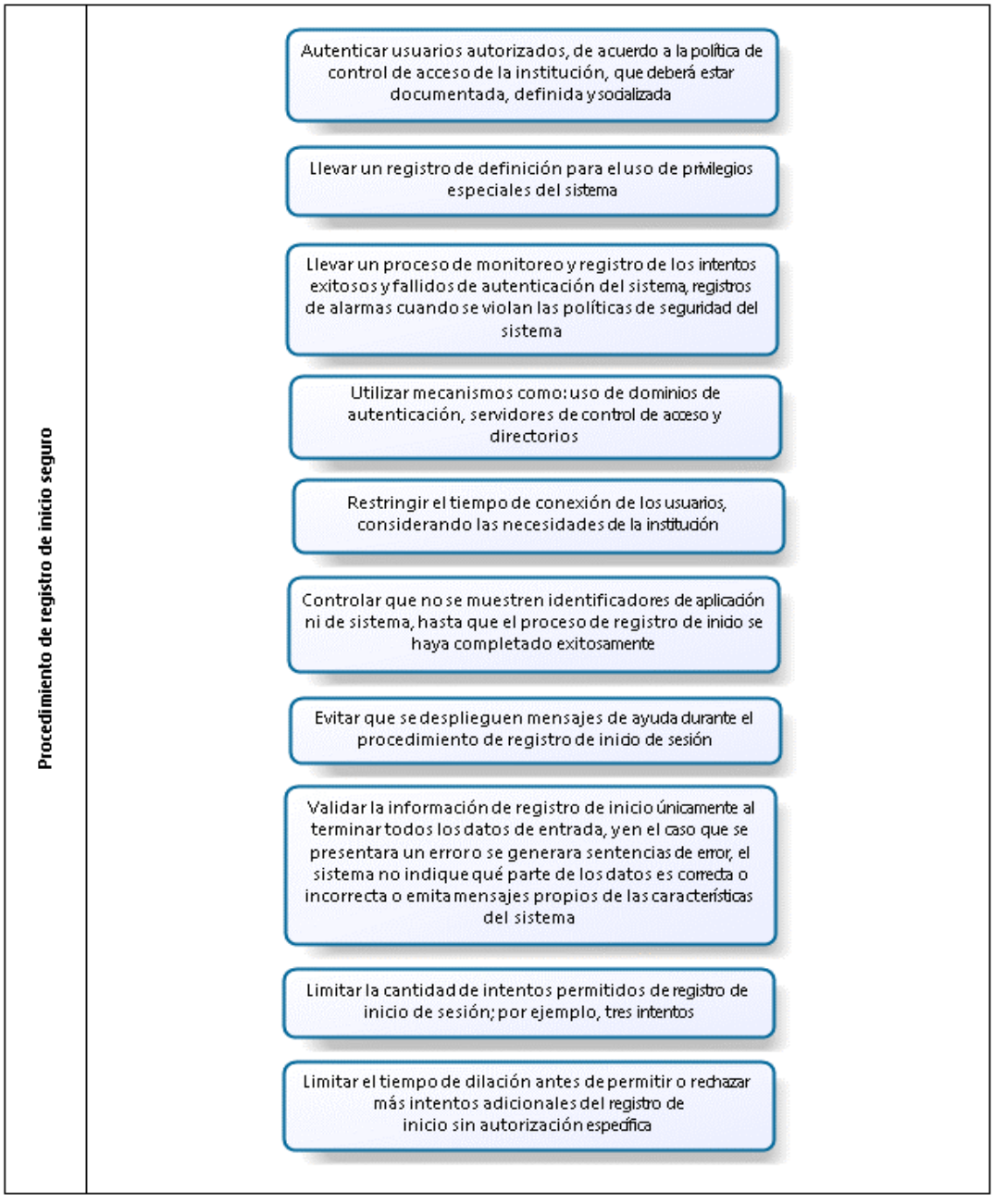

Figura 36. Procedimientos de registro de inicio seguro

Identificación y autenticación de usuarios:

Objetivo: Establecer procedimientos y mecanismos para garantizar que los usuarios, incluidos administradores y operadores de sistemas, aplicaciones y servicios, utilicen identificadores propios y evitar el uso de identificadores de terceras personas, y evitar el uso de identificadores genéricos. Adicionalmente se pretende disponer de toda la información necesaria para el rastreo de actividades de los usuarios. El detalle de los controles, procedimientos y actividades se muestran en la figura 37.

Situaciones de riesgos a mitigar: A4, A10, A17, A24, A31, I2.

Responsable: Área de Infraestructura de TI.

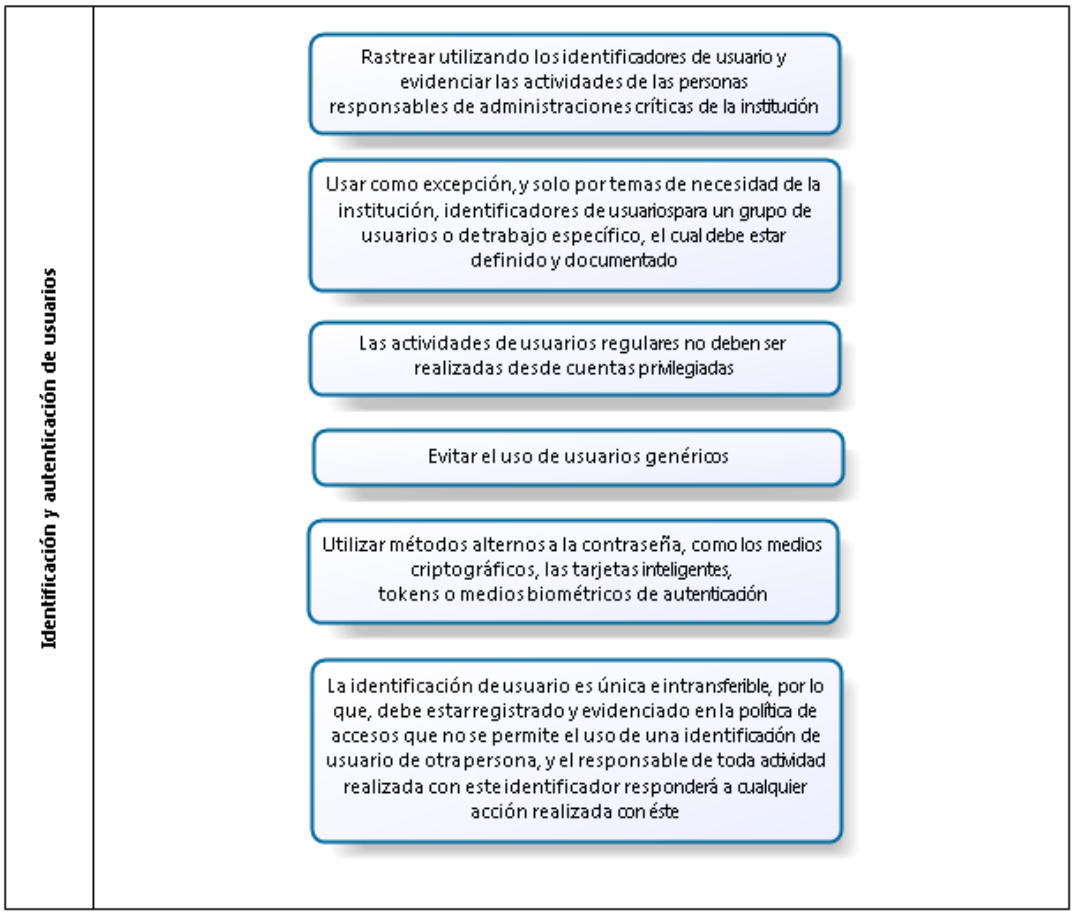

Figura 37. Identificación y autenticación de usuarios

Sistema de gestión de contraseñas:

Objetivo: Generar un procedimiento formal para la gestión y custodia de las contraseñas de usuarios con privilegios de acceso a información sensible, además de administradores de sistemas, servicios y aplicativos. Utilizar mecanismos de apoyo como el cifrado para el almacenaje y distribución de contraseñas. El detalle de los controles, procedimientos y actividades se muestran en la figura 38.

Situaciones de riesgos a mitigar: A4, A10, A17, A24, A31, I2.

Responsable: Área de Infraestructura de TI.

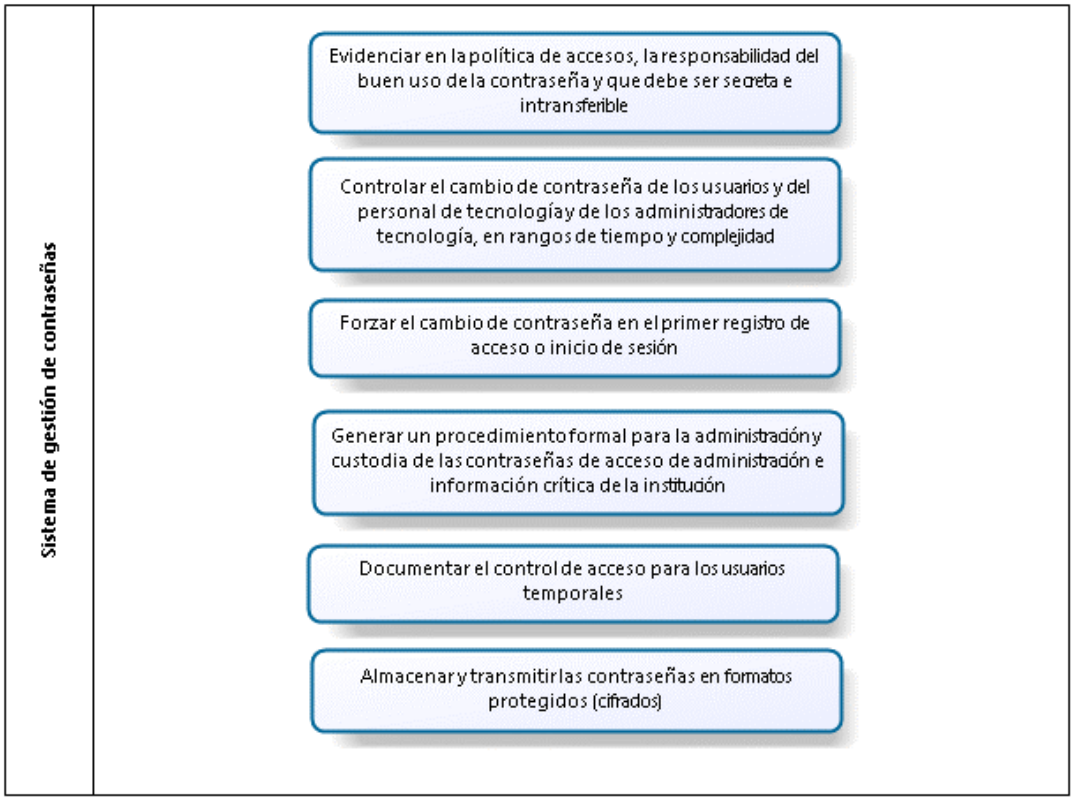

Figura 38. Sistema de gestión de contraseñas

Computación y comunicaciones móviles:

Objetivo: Implementar mecanismos para proteger la información almacenada en computadores y equipos portátiles, como aplicación de cifrado sobre particiones de discos duros. Adicionalmente concientizar a los usuarios de este tipo de equipos sobre los riesgos inherentes y las medidas a tomar. El detalle de los controles, procedimientos y actividades se muestran en la figura 39.

Situaciones de riesgos a mitigar: I7.

Responsable: Área de Infraestructura de TI.

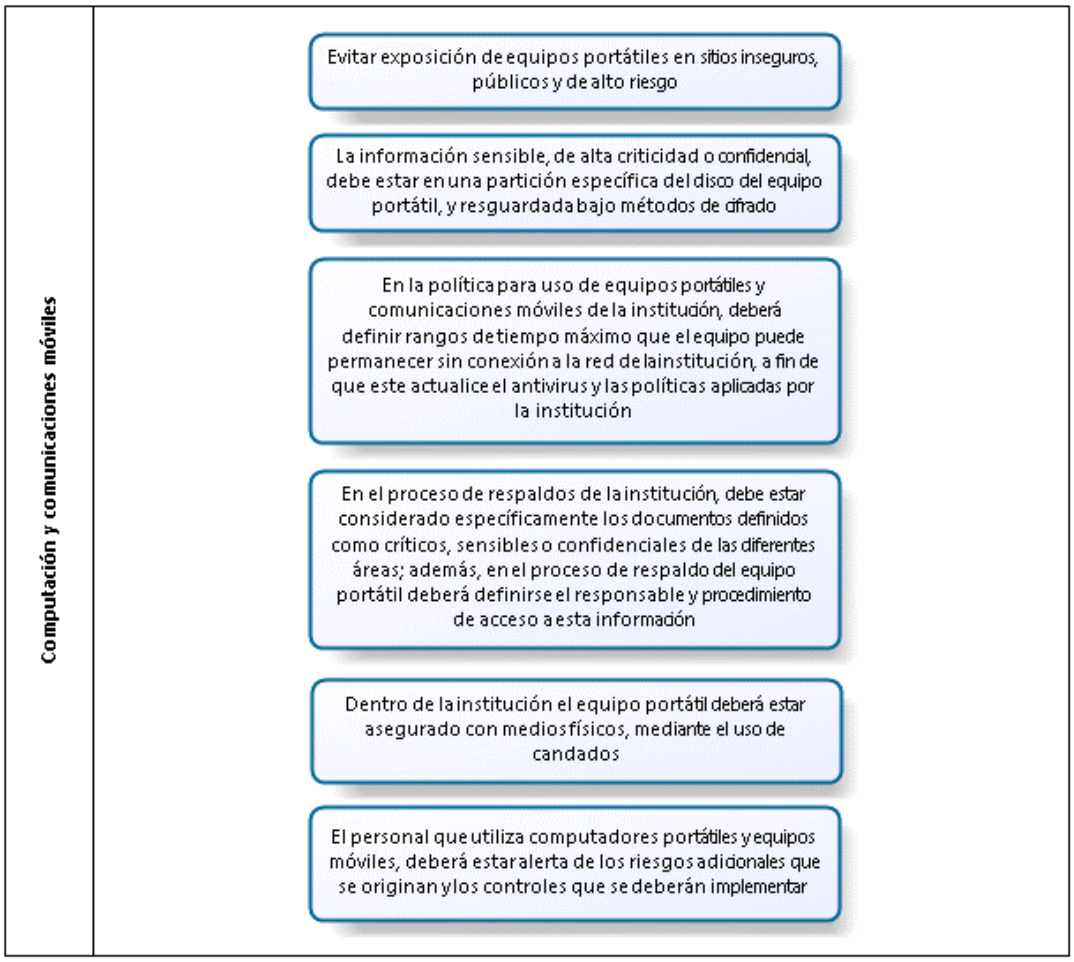

Figura 39. Computación y comunicaciones móviles

Trabajo remoto:

Objetivo: Establecer procedimientos y mecanismos que permitan a usuarios el poder realizar trabajo remoto debido a razones de fuerza mayor. Se debe tener especial cuidado sobre computadores que no son de propiedad de la institución y que serán usados en el trabajo remoto, para que incluyan políticas de seguridad como protección antivirus. El detalle de los controles, procedimientos y actividades se muestran en la figura 40.

Situaciones de riesgos a mitigar: A2, A8, A14, A22, A28, I4, I6, I7, I9.

Responsable: Área de Infraestructura de TI.

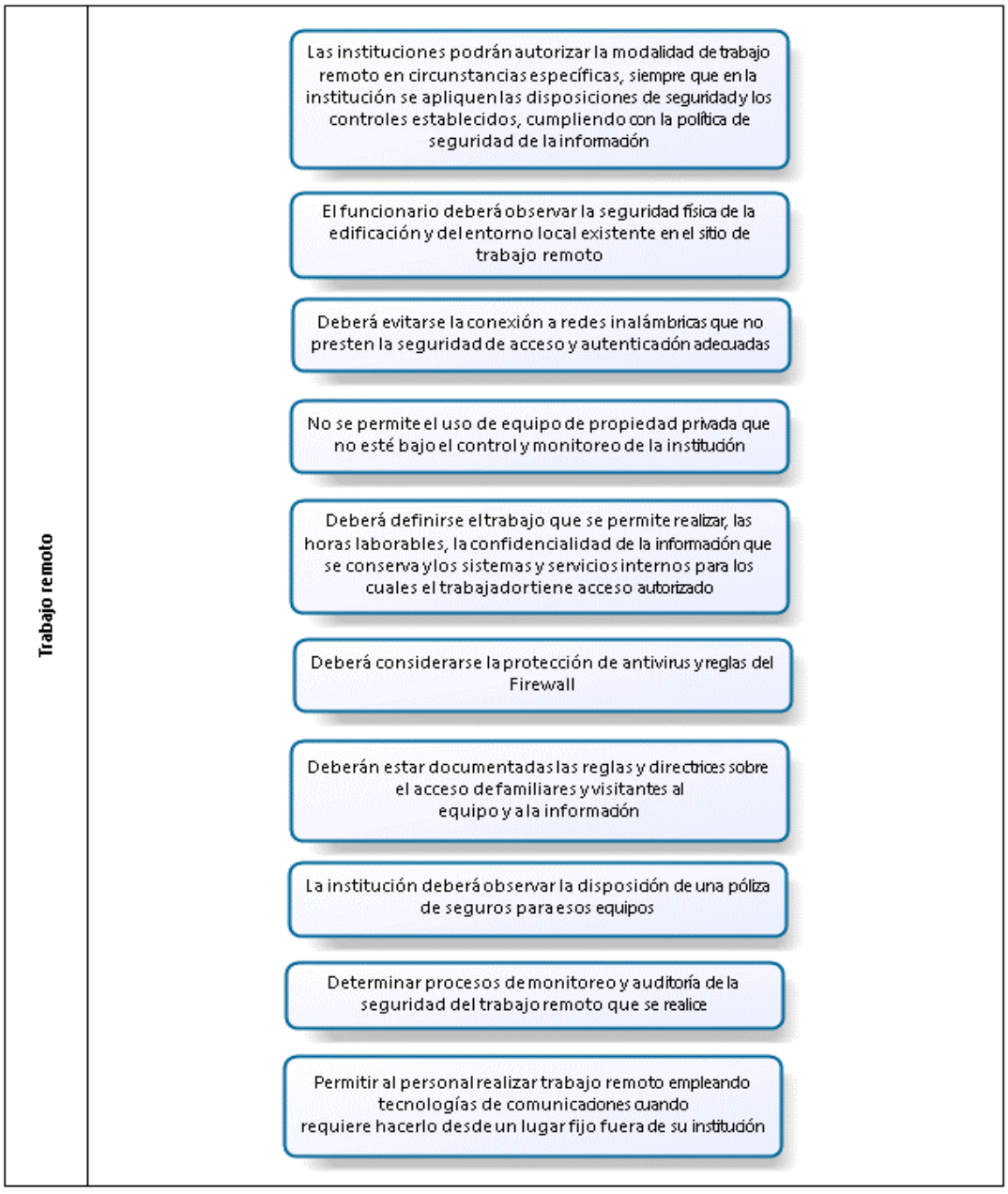

Figura 40. Trabajo remoto

5.8.3 Gestión de la Continuidad del Negocio

Los objetivos, procedimiento y actividades seleccionados, relacionados con la gestión de la continuidad del negocio son:

Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio:

Objetivo: Designar el responsable de coordinar actividades relacionadas con la continuidad de los diferentes servicios de TI. Definir una política de continuidad de los servicios de TI que incluya objetivos, alcance, funciones y responsabilidades. Identificar activos involucrados en los procesos críticos. El detalle de los controles, procedimientos y actividades se muestran en la figura 41.

Situaciones de riesgos a mitigar: A1, A2, A3, P2, P3, C1, C2, C3, C5, C7, S1, S2, S3, R1, R2, B1, SO1, SO2, A5, A6, A11, A12, A19, A20, A25, A26, A33, A34, I5.

Responsable: Director de Operaciones en coordinación con el oficial de seguridad del oficial de seguridad de la información y las diferentes áreas de TI.

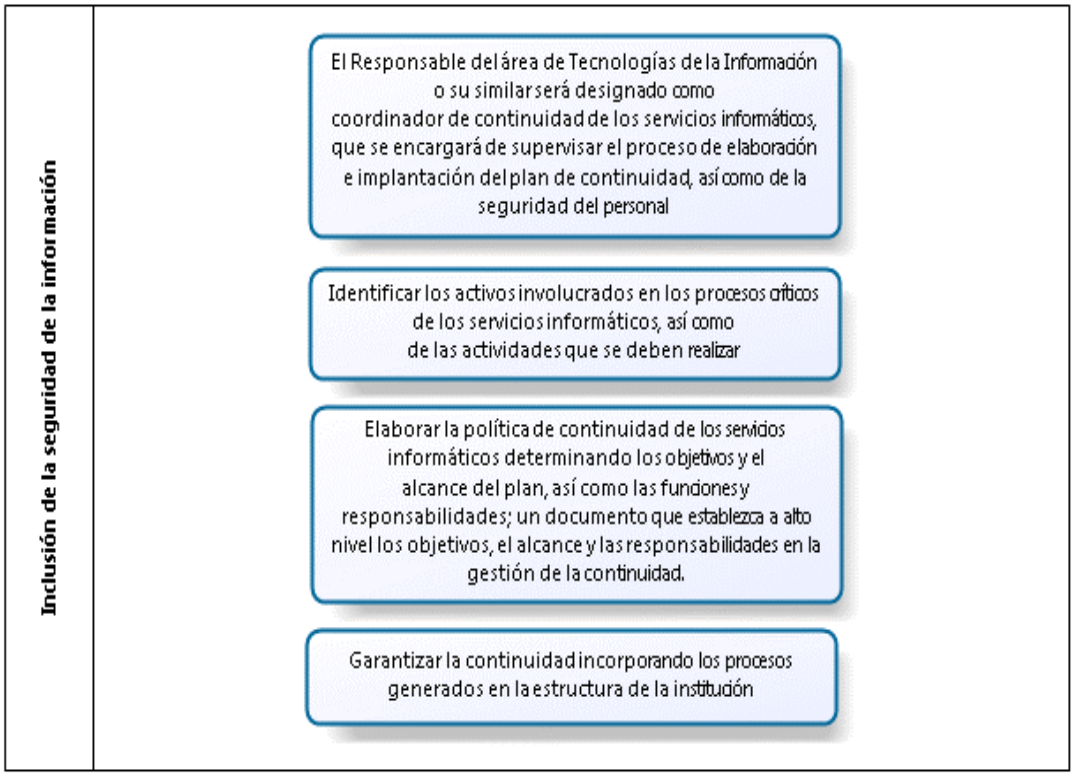

Figura 41. Inclusión de seguridad de la información en el proceso de gestión de continuidad del negocio

Continuidad del negocio y evaluación de riesgos:

Objetivo: Determinar los requerimientos de seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas. El detalle de los controles, procedimientos y actividades se muestran en la figura 42.

Situaciones de riesgos a mitigar: A1, A2, A3, P2, P3, C1, C2, C3, C5, C7, S1, S2, S3, R1, R2, B1, SO1, SO2, A5, A6, A11, A12, A19, A20, A25, A26, A33, A34, I5.

Responsable: Director de Operaciones en coordinación con todas las áreas de TI.

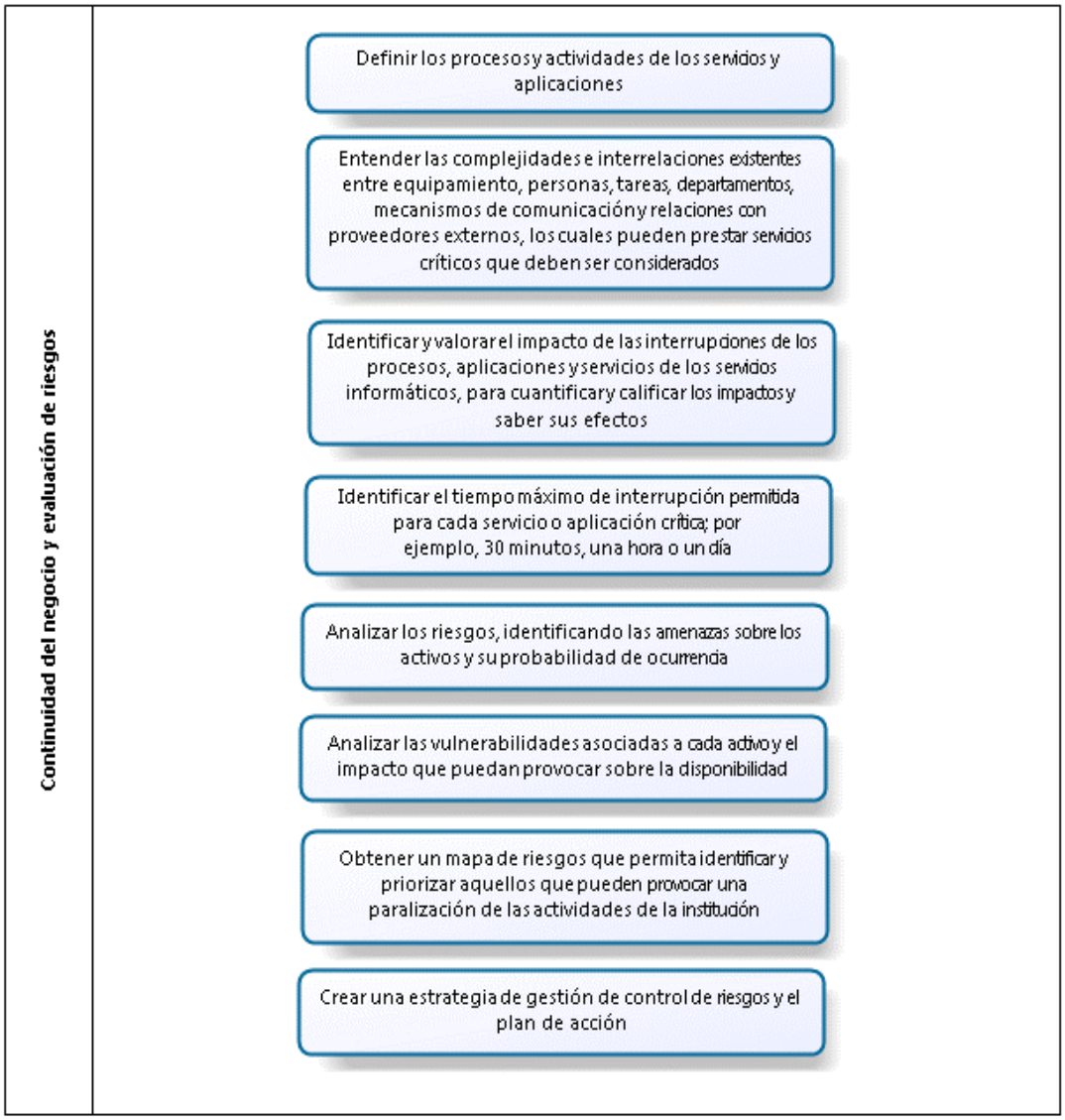

Figura 42. Continuidad del negocio y evaluación de riesgos

Desarrollo e implantación de planes de continuidad que incluya la seguridad de la información:

Objetivo: Establecer, documentar, implementar y mantener procesos, procedimientos y controles para garantizar los niveles requeridos de continuidad para la seguridad de la información durante situaciones adversas. El detalle de los controles, procedimientos y actividades se muestran en la figura 43.

Situaciones de riesgos a mitigar: A1, A2, A3, P2, P3, C1, C2, C3, C5, C7, S1, S2, S3, R1, R2, B1, SO1, SO2, A5, A6, A11, A12, A19, A20, A25, A26, A33, A34, I5.

Responsable: Director de Operaciones en coordinación con el oficial de seguridad de la información y las Áreas de TI.

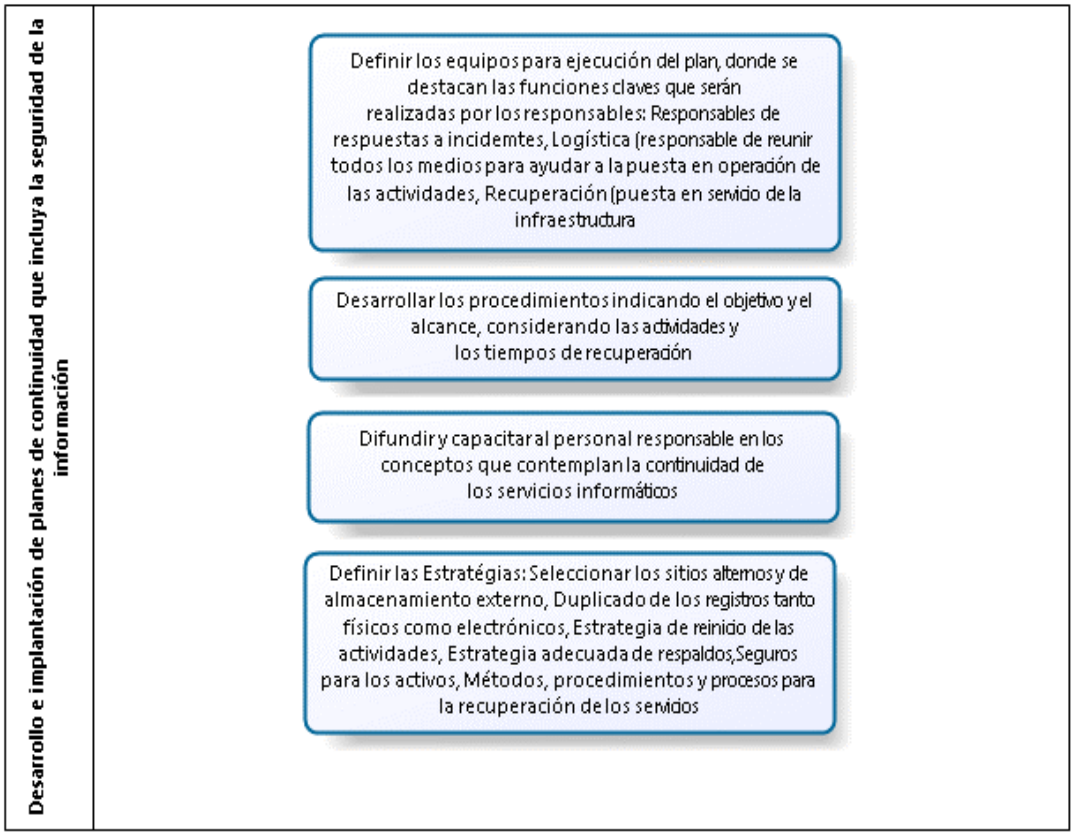

Figura 43. Desarrollo e implementación de planes de continuidad que incluya la seguridad de la información

Estructura para la planificación de la continuidad del negocio:

Objetivo: Definir procedimientos y actividades necesarios para la activación de los planes de continuidad del negocio, como son la definición de acuerdos de nivel de servicio internos y con proveedores externos de servicios, procedimientos de respaldos. El detalle de los controles, procedimientos y actividades se muestran en la figura 44.

Situaciones de riesgos a mitigar: A1, A2, A3, P2, P3, C1, C2, C3, C5, C7, S1, S2, S3, R1, R2, B1, SO1, SO2, A5, A6, A11, A12, A19, A20, A25, A26, A33, A34, I5.

Responsable: Director de Operaciones en coordinación con las Áreas de TI.

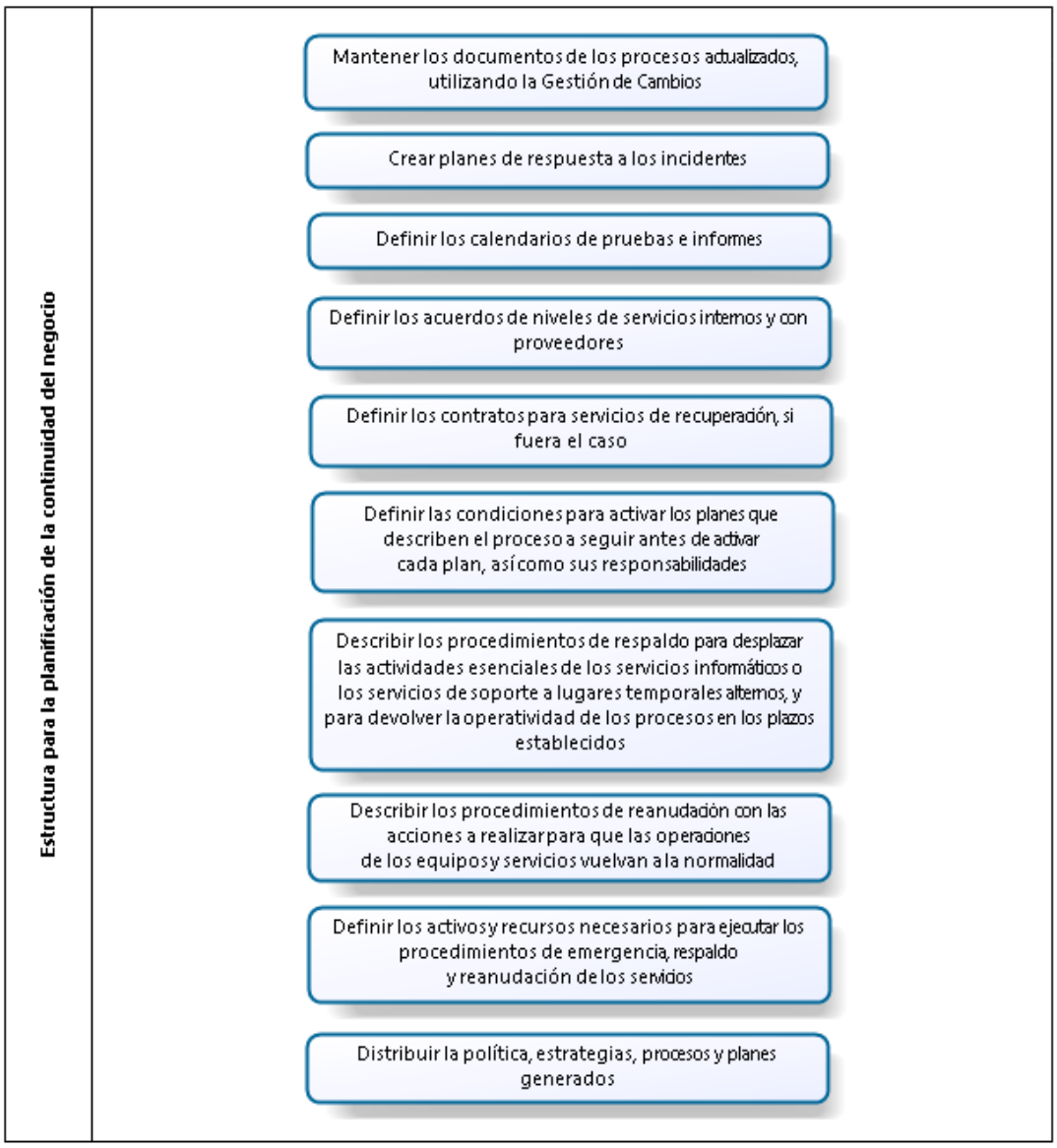

Figura 44. Estructura para la planificación de la continuidad del negocio

Pruebas, mantenimiento y revisión de los planes de continuidad del negocio:

Objetivo: Verificar los controles de continuidad de seguridad de la información establecidos e implementados, en intervalos regulares de tiempo, para garantizar que estos sean válidos y efectivos durante situaciones adversas. El detalle de los controles, procedimientos y actividades se muestran en la figura 45.

Situaciones de riesgos a mitigar: A1, A2, A3, P2, P3, C1, C2, C3, C5, C7, S1, S2, S3, R1, R2, B1, SO1, SO2, A5, A6, A11, A12, A19, A20, A25, A26, A33, A34, I5.

Responsable: Director de Operaciones en coordinación con las Áreas de TI.

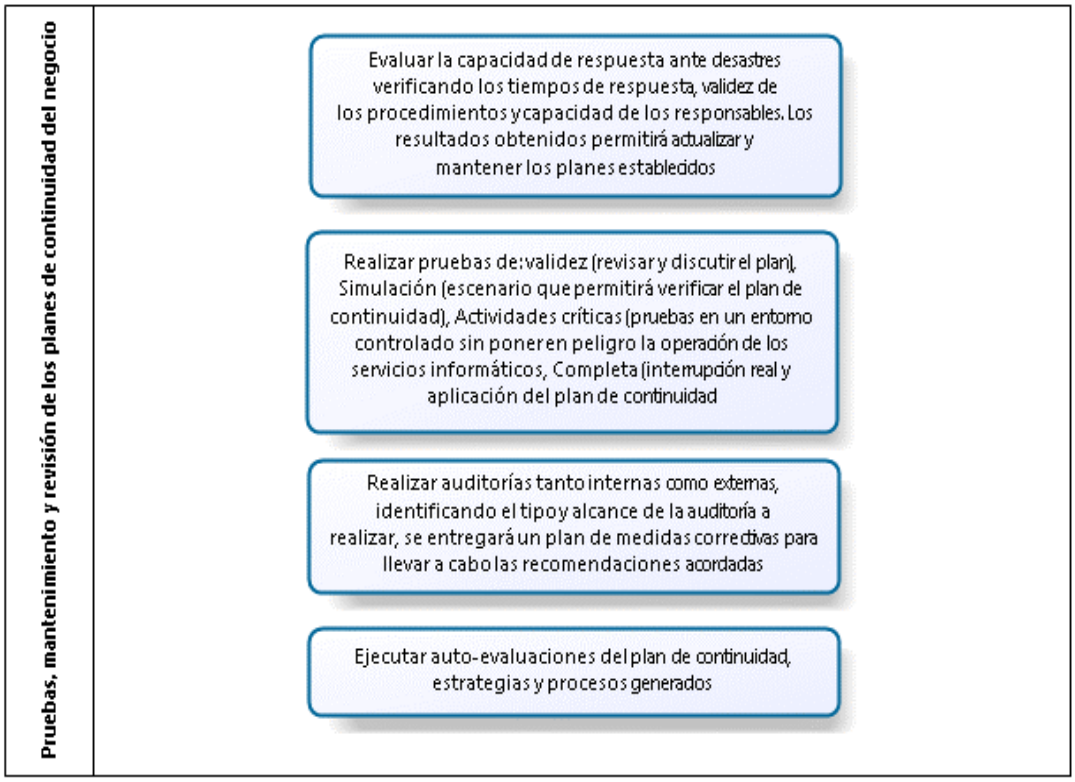

Figura 45. Pruebas, mantenimiento y revisión de los planes de continuidad del negocio

5.9 Declaración de Aplicabilidad

La selección de los objetivos de control y controles, mostrados en las figuras de la sección anterior, guarda relación con el análisis y evaluación de riegos realizado. Muchos de estos objetivos de control y controles se traducen en el desarrollo e implantación de procesos y procedimientos, por lo que el proyecto de implementación del EGSI y su respectivo SGSI es completamente viable, cumpliendo de esta forma lo establecido en la normativa vigente expuesta en el presente estudio.

6 Proceso para implementación de un objetivo de control

Como puede observarse en el detalle de los objetivos de control propuestos en el capítulo anterior, su implementación implica el levantamiento y puesta en operación de procesos específicos. La definición de procesos entre otros detalles proporciona información acerca de los recursos tecnológicos y humanos necesarios para su ejecución.

Algunos de los objetivos de control propuestos, en su detalle de controles y actividades, evidencia la necesidad de contar con una herramienta o solución tecnológica específica, además de talento humano calificado, tal es el caso por ejemplo de los objetivos de control relacionados con gestión de continuidad del negocio. Para implementar estos objetivos de control, que incluye procesos específicos, se debe contar con la participación de áreas especiales de asesoramiento y apoyo administrativo, definidas en el estatuto orgánico funcional del Ministerio de Finanzas del Ecuador [10].

El proceso planteado para la implementación de objetivos de control involucra la participación de las siguientes Direcciones, adicionales a la Dirección que sirve de escenario para la planificación del SGSI:

- Dirección de Administración de Talento Humano, que tiene como atribuciones y responsabilidades el gestionar los procesos de movimientos de personal.
- Dirección de Logística Institucional, que tiene como atribuciones y responsabilidades el dirigir la elaboración y la ejecución del sistema de adquisiciones.
- Dirección de Procesos y Mejora Continua, que tiene como atribuciones y responsabilidades el gestionar los procesos institucionales mediante la normativa y guías metodológicas, asesorar a la institución en temas relacionados a la gestión de procesos y la gestión de calidad, y promover e implementar proyectos de corrección, preventivas y de mejora de procesos.

La figura 46 muestra el proceso propuesto de implementación de objetivos de control:

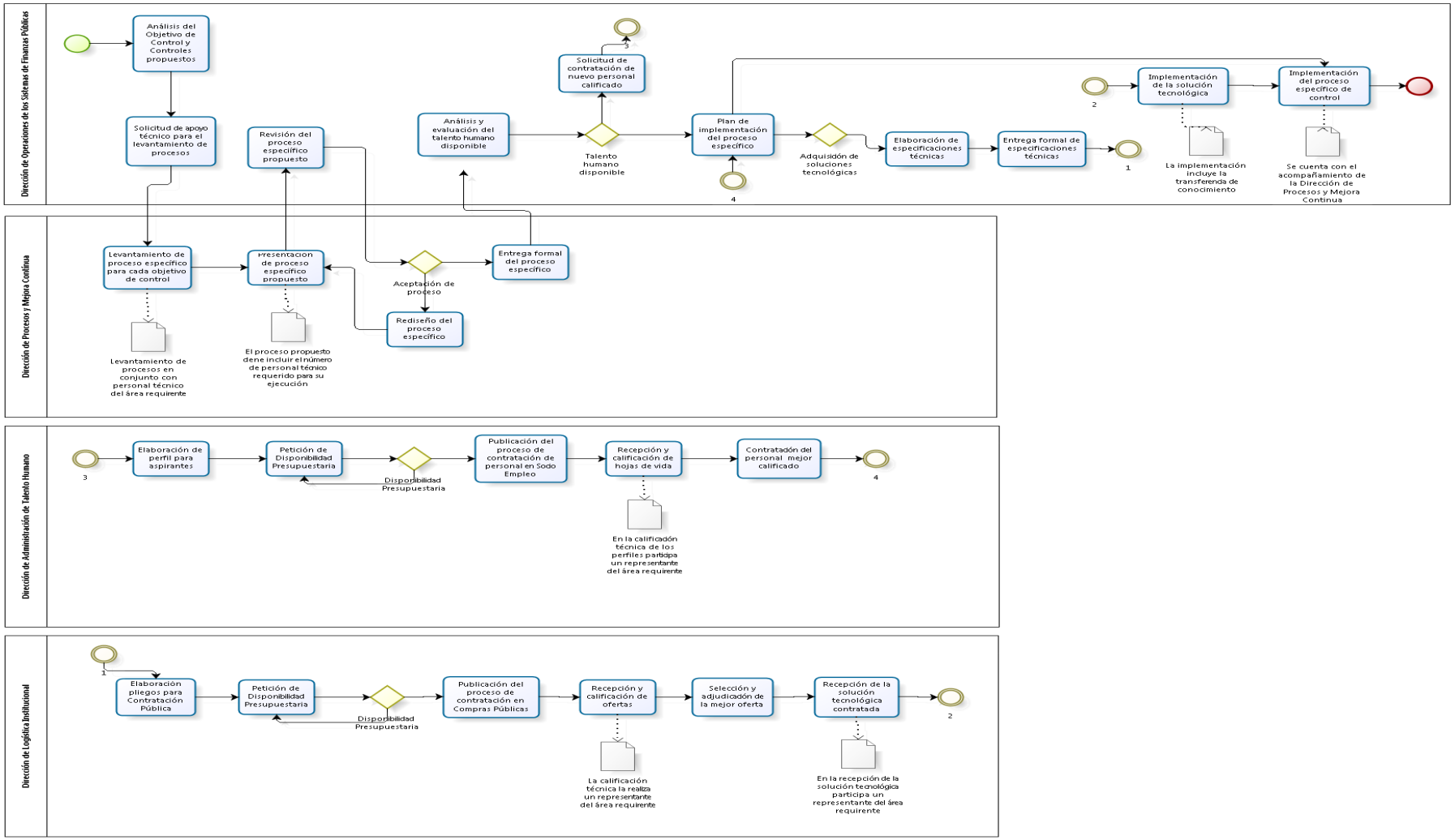

Figura 46. Proceso propuesto para implementación de objetivos de control

La descripción del proceso, mostrado en la figura 46, es la siguiente:

- El proceso inicia con el análisis del objetivo de control propuesto, por parte de la Dirección Nacional de Operaciones de los Sistemas de Finanzas Públicas, y se solicita formalmente a la Dirección de Procesos y Mejora Continua el asesoramiento para el levantamiento de procesos específicos, que incluya las actividades y controles detallados en el objetivo de control analizado.
- La Dirección de Procesos y Mejora Continua realiza el levantamiento de los procesos específicos, contando con el apoyo del personal técnico del área requirente, este caso la Dirección de Operaciones. Una vez levantada la información, se elabora una propuesta de proceso y se la somete a revisión por parte del área requirente.
- Si el proceso no es aceptado por parte del área requirente, la Dirección de Procesos y Mejora Continua realiza un rediseño, y lo vuelve a presentar hasta obtener la aceptación. Una vez aceptado el proceso, se procede a su entrega formal.
- La Dirección de Operaciones, tomando como referencia la información del proceso recibido, realiza una evaluación del número y capacidad de su personal técnico para implementar y operar el proceso. Si dispone del talento humano requerido, procede con la elaboración del plan de implementación del proceso.
- Si no se cuenta con el talento humano requerido, la Dirección de Operaciones realizará una solicitud de contratación de personal técnico calificado a la Dirección de Administración de Talento Humano.
- La Dirección de Administración de Talento Humano, una vez recibida la solicitud, procede a la elaboración de los perfiles de candidatos requeridos. Posteriormente se procede a la petición de disponibilidad presupuestaria. En este punto, el proceso no avanza hasta que se disponga de recursos financieros.
- Con la certificación de disponibilidad presupuestaria, la Dirección de Administración de Talento Humano procede a la publicación de los perfiles de candidatos requeridos a través del portal web de socio empleo, que es un servicio usado por las instituciones públicas para contratación de personal.
- Se procede a la recepción y calificación de hojas de vida de aspirantes. En la calificación participa un representante del área requirente, en este caso la Dirección de Operaciones. Los aspirantes cuyas hojas de vida hayan obtenido las mejores calificaciones serán contratados y vinculados a la institución.

- La Dirección de Operaciones, contando con el talento humano necesario, procede a elaborar el plan de implementación del proceso. En este punto, se verifica si para la implementación del proceso específico es necesario contar con alguna herramienta, servicio o solución tecnológica nueva. Si este es el caso entonces se procede a la elaboración de especificaciones técnicas de la solución o servicio tecnológico.
- Las especificaciones técnicas del servicio o solución tecnológica requerida es entregado formalmente a la Dirección de Logística Institucional para que inicie el proceso de adquisición.
- La Dirección de Logística Institucional, con las especificaciones recibidas, procede a la elaboración de los pliegos para contratación pública. Estos pliegos son básicamente formatos que deben ser llenados para su posterior publicación.
- Se solicita la respectiva disponibilidad presupuestaria para la adquisición. La Dirección de Logística Institucional, contando con la certificación de disponibilidad presupuestaria, procede a la publicación de los pliegos de adquisición en el portal web de Compras Públicas, que es un servicio por el cual las instituciones públicas publican sus procesos de adquisiciones para que sean atendidos por proveedores.
- Una vez publicado los pliegos de adquisición, después de un tiempo definido, se reciben y califican las ofertas realizadas por proveedores. De las ofertas calificadas, luego de un proceso de selección (ejemplo subasta inversa electrónica) se selecciona a la mejor oferta y se procede con la adjudicación al proveedor ganador.
- Cumplido el plazo de entrega establecido, se recibe la solución o servicio tecnológico. En la recepción participa un representante del área requirente.
- La Dirección de Operaciones procede con la implementación del servicio o solución tecnológica. Esta implementación involucra la transferencia de conocimiento al personal técnico de la Dirección, quienes se encargarán de su operación.
- Contando con las soluciones o servicios tecnológicos, la Dirección de Operaciones contando con el asesoramiento de la Dirección de Procesos y Mejora Continua, finalmente procede con la implementación de los procesos específicos de control.

7 Conclusiones

En resumen, la planificación del Sistema de Gestión de Seguridad de la Información realizada en el presente trabajo, incluyó los requisitos principales detallados en el estándar internacional ISO/IEC 27001:2013 y siguió los pasos de la guía de implementación propuesta en el estándar internacional ISO/IEC 27003:2010. Como conclusiones a esto se puede citar que:

- La definición del alcance del SGSI es muy importante para conocer sus límites de acción y de esta forma garantizar la consecución de los resultados esperados.
- La definición de políticas de seguridad es un requisito importante dado que expone los requerimientos generales de toda la institución respecto a seguridad de la información y constituye la base legal para la planificación de un SGSI.
- Un requisito fundamental para la planificación de un SGSI es sin duda la realización de un análisis y evaluación de riesgos, que se apoya en una metodología definida para su realización.
- Del análisis y evaluación de riesgos, se obtienen las situaciones de riesgos con mayor impacto, probabilidad de ocurrencia y necesidad de salvaguardas, que son la referencia para la selección de los objetivos de control y controles que el SGSI debe implementar.
- Para implementar un SGSI, es decir, para implementar los objetivos de control y controles seleccionados, dentro de una institución pública como es el Ministerio de Finanzas del Ecuador, se realizó una propuesta de proceso de implementación que incluye la participación de áreas en encargadas de gestionar la provisión de recursos tecnológicos y humanos, así como la asesoría en metodologías de gestión por procesos.

El aporte o valor que proporciona este trabajo final de máster se describen en las siguientes conclusiones:

- Para llevar a cabo la planificación de un sistema de gestión de seguridad de la información, es indispensable contar con el apoyo de las autoridades de la institución pública, como es el caso de este presente estudio. El inicio de la planificación de un SGSI debe contar con la autorización formal de las autoridades.
- Previo a iniciar la planificación de un SGSI, al interno de la entidad u organización pública, debe designarse al colaborador o funcionario que cumplirá el rol de oficial de seguridad de la información, para que cumpla tareas de elaboración y difusión de políticas de seguridad de la información.

Como observación al caso de estudio, dentro del Ministerio de Finanzas del Ecuador, el rol de oficial de seguridad de la información recae sobre el Viceministro de Finanzas; sin embargo, se recomienda que este rol, dentro de una institución pública, lo cumpla un colaborador que nivel jerárquico medio que no esté sujeto a inestabilidades políticas que generen cambios de autoridades.

- Des estudio realizado, y siguiendo lo establecido en los estándares internacionales ISO/IEC 27000, se concluye que la determinación de activos críticos y el análisis y evaluación de riesgos son pasos fundamentales para definir el enfoque del SGSI, es decir, los objetivos de control y controles a ser aplicados.
- Para que un SGSI genere los resultados esperados, es importante que los usuarios conozcan los aspectos fundamentales de seguridad de la información y lo traduzcan en buenas prácticas en el momento de realizar sus actividades de trabajo. La gestión de seguridad de la información se basa en el grado de conciencia que se pueda obtener de los usuarios sobre seguridad de la información.
- De acuerdo al estudio realizado y en base a información obtenida de fuentes bibliográficas, se puede establecer que el basar la gestión de seguridad de la información solamente en la aplicación de herramientas tecnológicas es un error. Una correcta gestión se realiza estableciendo procesos y procedimientos que sean claros y que ordenen los esfuerzos de trabajo. Muchos de los controles de seguridad propuestos en este estudio involucran el levantamiento de procesos y hacer el mejor uso de las herramientas tecnológicas ya existentes.

Como trabajos futuros que pueden realizarse a partir del presentado son:

- Levantamiento e implementación de procesos específicos de control de seguridad de la información relacionados con gestión de comunicaciones y operaciones.
- Levantamiento e implementación de procesos específicos de control de seguridad de la información relacionados con gestión de control de accesos
- Levantamiento e implementación de procesos específicos de control de seguridad de la información relacionados con gestión de continuidad del negocio.
- Diseño de un plan integral de continuidad del negocio, relacionado a provisión de servicios de TI, que incluya controles de seguridad de la información.

- Diseño de indicadores de gestión para medir la efectividad de la operación de un sistema de gestión de seguridad de la información, basado en el estándar internacional ISO/IEC 27004.

8 Bibliografía

[1] A. Calder, ISO27001 / ISO27002: A Pocket Guide. Ely, Cambridgeshire, United Kingdom: IT Governance Publishing, 2013.

[2] J. Guerrón, "Elaboración de un plan para la implementación del sistema de gestión de seguridad de la información," pp. 29, 2013.

[3] Instituto Ecuatoriano de Normalización, "NORMA TÉCNICA ECUATORIANA NTE INEN-ISO/IEC 27003:2012,".

[4] Instituto Nacional de Tecnologías de la Comunicación, "Modelo Unificado de Análisis de Riesgos de Seguridad Física y Lógica,".

[5] (). Sistema de Gestión de la Seguridad de la Información. Available: www.iso27000.es.

[6] A. Larrahondo, "Plan Director de Seguridad de la Información," 2013.

[7] J. Lillo, "Elaboración de un Plan de Implementación y Desarrollo de un Sistema de Gestión de la Seguridad de la Información basado en la norma ISO/IEC 27001:2005," 2014.

[8] Ministerio de Finanzas del Ecuador, "Acuerdo Ministerial No. 209, Implementación del Esquema Gubernamental de la Seguridad de la Información." 2014.

[9] Ministerio de Finanzas del Ecuador, "Política General de Seguridad de la Información (PGSI)," vol. 2.0, 2014.

[10] Ministerio de Finanzas del Ecuador, "Acuerdo Ministerial No. 254, Estatuto Orgánico Funcional del Ministerio de Finanzas," 2011.

[11] Ministerio de Finanzas del Ecuador, "Código Orgánico de Planificación y Finanzas Públicas," 2010.

[12] Organización Internacional de Estandarización, ISO, "Information technology - Security techniques - Information security management systems - Requirements," Iso/iec 27001, 2013.

[13] Organización Internacional de Estandarización, ISO, "Information techonoly - Security techniques - Information security management system implementation guidance," Iso/iec 27003, 2010.

[14] Secretaría Nacional de la Administración Pública del Ecuador, "Esquema Gubernamental de Seguridad de la Información EGSI," 2013.