UNIVERSIDAD NACIONAL DE CAJAMARCA

FACULTAD DE INGENIERIA

ESCUELA ACADÉMICO PROFESIONAL DE INGENIERIA DE SISTEMAS

PROYECTO PROFESIONAL

ANALISIS DE RIESGOS DE TI PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD DE LA INFORMACION EN EL GOBIERNO REGIONAL DE CAJAMARCA

PARA OPTAR EL TITULO PROFESIONAL DE

INGENIERO DE SISTEMAS

PRESENTADO POR EL BACHILLER:

REINALDO JAVIER ALIAGA INFANTE

CAJAMARCA - PERÚ

2014

DEDICATORIA

Dedico este trabajo a Dios por darme vida, a mis padres por darme su apoyo incondicional, contribuyendo a lograr las metas y objetivos que me propuse.

AGRADECIMIENTO

A mi familia, quienes me enseñaron a seguir adelante frente a las adversidades. Al Ing. Edwin Valencia Castillo, por su valiosa guía y asesoramiento en el desarrollo del presente proyecto. A todas las personas del Gobierno Regional de Cajamarca que ayudaron directa e indirectamente en la realización de este trabajo.

RESUMEN

En la actualidad toda organización está obligada a implementar procesos para proteger la información del negocio y todo aquello que tenga relación con la creación y procesamiento de información. Y cuando hablamos de todo aquello que tenga relación nos referimos a personas, equipamiento, infraestructura que permiten convertir los datos en información que hoy en día es el valor más preciado para cualquier empresa.

Para el desarrollo del presente proyecto profesional era imperativo utilizar una metodología de análisis de riesgos, como MAGERIT, OCTAVE, ISO 27005, entre otras más; pues por un tema normativo exigido por la Oficina Nacional de Gobierno Electrónico e Informática se ha utilizado la NTP-ISO/IEC 27005:2009 que más que una metodología es una guía que nos proporciona directrices para la gestión de riesgos en la seguridad de la información.

Dando inicio al proceso metodológico se ha identificado los macro procesos del Gobierno Regional de Cajamarca y posteriormente centrarse en el proceso core del negocio (Gestión de Proyectos de Inversión Pública). Partiendo de un sub proceso se ha identificado los activos de información como son documentos, sistemas, equipos y personas; para luego centrarnos únicamente en los activos de TI relevantes para el proceso core.

Se han definido los activos de TI más relevantes teniendo en cuenta los pilares de la seguridad de la información (Integridad/Confidencialidad/Disponibilidad), luego identificar y valorar amenazas y vulnerabilidades las cuales permitieron determinar los niveles de riesgos de los activos de información de TI.

Finalmente, con ayuda de la NTP-ISO/IEC 27001:2008 y NTP-ISO/IEC 17799:2007 se ha identificado los controles a implementar para cada riesgo identificado, ya es responsabilidad de la institución la implementación de cada uno de los controles.

ÍNDICE

INDICE DE FIGURAS

INDICE DE CUADROS

I. INTRODUCCIÓN

Actualmente la mayoría de las organizaciones indistintamente de su tamaño, privada o pública; ven la forma de apoyar sus procesos en el uso de TI[1], permitiendo monitorearlos, agilizarlos y principalmente para obtener datos, transformarlos en información y obtener beneficios tales como decisiones oportunas y ventaja competitiva.

Por tal, la información se ha convertido en un bien muy valioso para cualquier organización; se trate de información impresa, escrita en un papel, guardada electrónicamente o enviada por correo o medios electrónicos.

Pero preguntas como ¿Qué consecuencias tendría la pérdida o robo de información en la organización?, ¿Qué información depende de las tecnologías de información?, ¿Las TI están siendo utilizadas y protegidas adecuadamente?, ¿Qué pasaría si algún componente de TI no funciona?; son las que conllevan a reflexionar e intentar tomar acciones para proteger la información y los activos relacionados directamente con ésta.

En relación a Seguridad de la Información se utiliza el término activo de información no sólo para referirse a tecnología, sino también a documentación física y digital, espacios físicos como oficinas y edificios, personas; los cuales deben ser identificados en un proceso de análisis de riesgos e implementación del SGSI[2].

Para implementar un SGSI, en la fase de planear se debe realizar un análisis de riesgos que no es más que identificar activos de información, valorarlos y priorizarlos; identificar amenazas y vulnerabilidades; para luego determinar los niveles de riesgos a los cuales están expuestos los activos, identificar los controles especificados en la NTP-ISO/IEC 27001:2008 y luego implementarlos basándose en la NTP-ISO/IEC 17799:2007.

[1] TI: Tecnologías de Información
[2] SGSI: Sistema de Gestión de la Seguridad de la Información

II. PLANTEAMIENTO DEL PROBLEMA

2.1. DEFINICIÓN

El Gobierno Regional de Cajamarca tiene por finalidad esencial fomentar el desarrollo regional integral y sostenible, promoviendo la inversión pública, privada y el empleo, además de garantizar el ejercicio pleno de los derechos y la igualdad de oportunidades de sus habitantes, de acuerdo con los planes y programas nacionales, regionales y locales de desarrollo.

Desde el año 2009, la tecnología ha ido tomando relevancia en el desempeño de la institución. Implementaciones tecnológicas como "Gobierno Electrónico", Portales Institucionales para dar apoyo a la ley de transparencia, sistema SIGA[3] (complementario al sistema SIAF[4]) para dar soporte a las áreas administrativas son los antecedentes más notables de los logros alcanzados por el área de TI del Gobierno Regional de Cajamarca. Estos servicios se ven soportados por activos tecnológicos como son servidores, comunicaciones, bases de datos, personas, y otros más.

Al ofrecer servicios tecnológicos que apoyen a los procesos y obtener información, ha conllevado a adquirir equipamiento tecnológico que soporte a dichos servicios. El crecimiento rápido en tecnología y personal en el Gobierno Regional de Cajamarca trajo consecuencias negativas en relación a la seguridad de la información por no tener los controles adecuados para asegurar los activos de información.

Los cambios constantes de personal, transición de mandatos, averías en servidores, pérdida de comunicaciones a nivel de redes de datos, cortes de fluido eléctrico, ausencia de equipamiento y software adecuado han causado que la información o los servicios que la respalda no cumplan con los pilares en las que se basa la seguridad de la información que son disponibilidad, confidencialidad e integridad.

La falta de políticas e implementación de controles hace que la información de la institución sea muy vulnerable y sensible a pérdida.

[3] SIGA: Sistema Integral de Gestión Administrativa
[4] SIAF: Sistema Integral de Administración Financiera

2.2. OBJETIVOS

2.2.1. OBJETIVO GENERAL

Realizar un análisis de riesgos de TI que permita implementar un Sistema de Gestión de la Seguridad de la Información bajo la Norma Técnica Peruana NTP-ISO/IEC 27001:2008.

2.2.2. OBJETIVOS ESPECÍFICOS

- ✓ Identificar y priorizar el(los) proceso(s) crítico(s) de negocio del Gobierno Regional de Cajamarca.
- ✓ Evaluar y elegir metodologías de análisis de riesgos de TI
- ✓ Identificar Activos de Información basados en el(los) proceso(s) críticos.
- ✓ Identificar y valorar las amenazas de los activos de información
- ✓ Identificar y valorar las vulnerabilidades de los activos de información.
- ✓ Identificar los riesgos asociados a los activos de información.
- ✓ Identificar controles en función a la norma técnica peruana NTP-ISO/IEC 27001:2008 basándonos en los resultados del análisis de riesgos, que permitirá tomar como base para la implementación de un Sistema de Gestión de la seguridad de la información.

2.3. ALCANCE DEL PROYECTO

A nivel geográfico el proyecto ***"ANÁLISIS DE RIESGOS DE TI PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN EN EL GOBIERNO REGIONAL DE CAJAMARCA"*** tendrá como alcance sólo la sede central del Gobierno Regional de Cajamarca.

Además sólo el proyecto tomará atención en los activos de Tecnologías de Información que conforman el o los procesos a analizar.

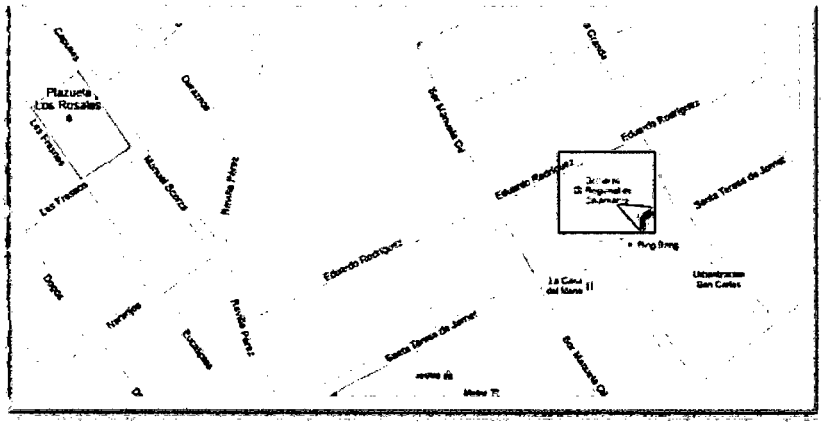


Figura 1: Ubicación Geográfica
Fuente: www.google.com

2.4. JUSTIFICACIÓN

En la actualidad la información es el activo más importante para cualquier empresa; es por ello que su aseguramiento conjuntamente con los distintos componentes que la soportan debe ser un objetivo primordial para una organización.

En el Gobierno Regional de Cajamarca no existe una cultura organizacional tanto de la alta gerencia como los niveles operativos que apoyen a la protección y aseguramiento de la información, pues aún no han tomado conciencia de la importancia de los activos de información para la continuidad del negocio.

Para cualquier implementación de un Sistema de Gestión de Seguridad de la Información, se debe realizar un análisis de riesgos (relacionados a la seguridad de la información) que permita identificar los activos de información más importantes, amenazas y vulnerabilidades; para determinar el nivel de impacto que causaría la ocurrencia de un incidente de seguridad de la información; y luego identificar los controles a implementar.

Por expuesto y además dar inicio al cumplimiento de la normativa dispuesta por la ONGEI[5] se da por justificado el desarrollo del presente proyecto.

[5] ONGEI: Oficina Nacional de Gobierno Electrónico e Informática

III. MARCO TEÓRICO

3.1. SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

El objeto de SGSI[6] es diseñar, implantar, mantener un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando los riesgos de seguridad de la información.

El propósito de un SGSI es garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

Un SGSI ayuda a establecer políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición menor al nivel de riesgo que la propia organización ha decidido asumir [9].

La adopción de un SGSI debe ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización está influenciado por las necesidades y objetivos del negocio, requisitos de seguridad, procesos, tamaño y estructura de la organización [7].

Todo proceso de gestión debe de ser eficiente durante el tiempo, y el SGSI no es la excepción; por tal se debe de seguir modelos que permitan la mejora continua, es por ello que un SGSI se basa en el modelo PDCA.

3.1.1. MODELO PDCA[7]

Un SGSI hace uso de un modelo de mejora continua y al igual que otros sistemas se basa en el modelo PDCA iniciales en inglés de Plan-Do-Check-Act, la figura 2 muestra un panorama general del modelo PDCA para un SGSI.

[6] SGSI: Sistema de Gestión de la Seguridad de la Información
[7] PDCA: Plan, Do, Check, Act (Planear, Hacer, Verificar, Actuar)

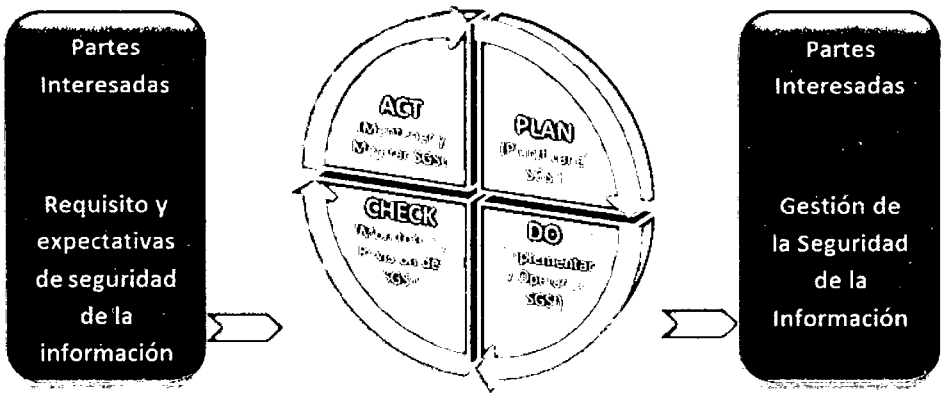


Figura 2: Modelo PDCA aplicado al proceso SGSI
Fuente: NTP-ISO/IEC 27001:2008

Planear (Establecer el SGSI)	Establecer las políticas, objetivos, procesos y procedimientos de seguridad relevantes para administrar el riesgo y mejorar la seguridad de la información para obtener resultados de acuerdo con las políticas y objetivos de la organización.
Hacer (Implementar y Operar el SGSI)	Implementar y operar las políticas, controles, procesos y procedimientos de seguridad.
Verificar (Monitorear y revisar el SGSI	Monitorear y evaluar el funcionamiento de los procesos con respecto a las políticas, objetivos y experiencia práctica de seguridad, informando sobre los resultados obtenidos a la gerencia para su revisión.
Actuar (Mantener y mejorar el SGSI)	Tomar acciones correctivas y preventivas basándose en los resultados de la revisión gerencial para alcanzar la mejora continua del ISMS.

Tabla 1: PDCA – Descripción
Fuente: NTP-ISO/IEC 27001-2008

3.1.2. BENEFICIOS DE LA IMPLEMENTACIÓN DE UN SGSI

En [9] se hace referencia a lo siguiente:

- Reducción del riesgo de pérdida, robo o corrupción de información.
- Los usuarios tienen acceso a la información a través medidas de seguridad.
- Los riesgos y sus controles son continuamente revisados.
- Posibilidad de integrarse con otros sistemas de gestión (ISO 9001, ISO 14001, OHSAS 18001...).
- Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.
- Imagen de empresa.
- Confianza y reglas claras para las personas de la organización.
- Reducción de costes y mejora de los procesos y servicio.
- Aumento de la motivación y satisfacción del personal.

3.2. ANÁLISIS Y GESTIÓN DE RIESGOS

3.2.1. ANÁLISIS DE RIESGOS

El primer paso en la gestión de riesgos es el análisis de riesgos. Los analistas de riesgos proceden a realizar entrevistas al personal de la organización para obtener de información. En esta fase se identifican los activos de la organización, identificando las relaciones que se establecen entre activos. De esta forma se obtiene el "árbol de activos" que representan las distintas dependencias y relaciones entre activos, es decir, todos aquellos elementos que están "encadenados entre sí" en términos de seguridad.

También se identifican el conjunto de amenazas, estableciendo para cada activo, cual es la vulnerabilidad que presenta frente a dicha amenaza. Además, se cuantifica el impacto, para el caso en el que la amenaza se materializase. Dado que los activos se encuentran jerarquizados y se encuentran establecidas las relaciones de dependencia entre los activos de las diferentes categorías, hemos conseguido de forma explícita documentar la "cadena de fallo" en caso de un incidente de seguridad.

La experiencia y la sucesiva revisión de la información generada en estudios de riesgos anteriores permitirán ajustar de forma más exacta las diferentes dependencias entre activos. Con toda esta información, tendremos una estimación del costo que podría producir la materialización de una amenaza sobre un activo. Teniendo en cuenta las relaciones funcionales y de dependencias entre activos, se hallan los valores de riesgo.

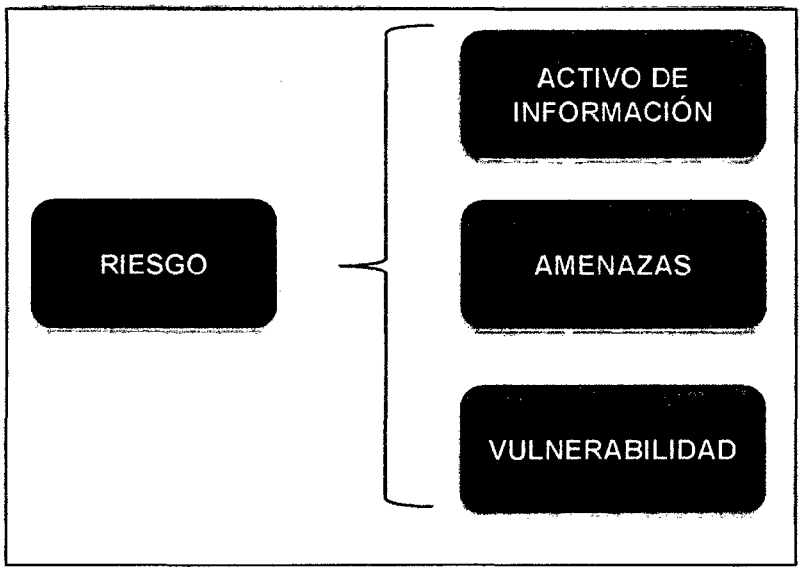


Figura 3: Identificación de Riesgos

3.2.2. GESTIÓN DE RIESGOS

En [10] se hace referencia a lo siguiente:

En esta fase, se procede a la interpretación del riesgo. Una vez identificado los puntos débiles, deben seleccionarse el conjunto de controles a implementar para disminuir los niveles de riesgo a los valores deseados. Para ello, deberán especificarse los mecanismos de control que se encuentran implantados hasta ese momento y cuál es su grado de cumplimiento.

Este proceso se ayuda de la simulación. Se van probando selecciones de diferentes mecanismos de control y se estudia en qué medida reducen los niveles de riesgo a los márgenes deseados. Es muy importante realizar las correctas estimaciones de la efectividad de los diferentes mecanismos de control para ajustar de forma precisa los valores de riesgo. Una vez obtenidos estos resultados, se establece de nuevo reuniones con el equipo responsable

del proyecto de la organización en estudio. De esta forma, se analizan los resultados obtenidos y se establece un plan de implantación de mecanismos.

Para garantizar que la empresa gestiona sus riesgos de forma coherente, se debe definir un proceso repetible para gestionar los riesgos de TI.

Existen múltiples metodologías de gestión de riesgos, entre las más importantes figuran Magerit[8], ISO 27005, Octave[9].

3.3. MARCO DE REFERENCIA

Para la implementación del presente proyecto profesional tomaremos como referencia las normas más importantes de la familia ISO 27000, Magerit, Cobit e ITIL las cuales se mencionan brevemente en los siguientes apartados.

3.3.1. FAMILIA DE NORMAS DE SEGURIDAD DE LA INFORMACIÓN 27000

En [9] se hace referencia a lo siguiente:

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

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

La familia de normas ISO 27000 es un conjunto de estándares desarrollados por la ISO[10] e IEC[11], que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

El conjunto de normas ISO/IEC 27000 tienen su origen en la norma BS 7799 de la BSI[12] que apareció por primera vez en 1995, con objeto de proporcionar a

[8] MAGERIT: Metodología de Análisis y Gestión de Riesgos de Tecnologías de Información
[9] OCTAVE: Operationally Critical Threat, Asset, and Vulnerability Evaluation
[10] ISO: International Organization for Standardization - Organización Interacional de Normalización
[11] IEC: International Electrotechnical Commission – Comisión Electrónica Internacional
[12] BSI: British Standards Institution

cualquier empresa un conjunto de buenas prácticas para la gestión de la seguridad de su información.

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

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

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

En 2005, con más de 1700 empresas certificadas en BS 7799-2, esta norma se publicó por ISO, con algunos cambios, como estándar ISO 27001. Al tiempo se revisó y actualizó la ISO 17799. Esta última norma se renombró como ISO 27002:2005 el 1 de Julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión.

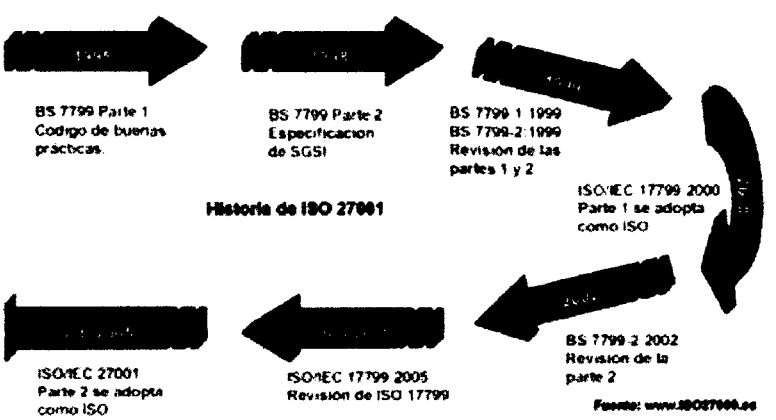


Figura 4: Evolución ISO/IEC 27000

Fuente: www.iso27000.es

La Familia ISO/IEC 27000 está conformada por una serie de normas que permiten ser una guía para mejorar la seguridad de la información en cualquier organización independientemente del rubro y tamaño. En el gráfico siguiente se

observa las principales normas de esta familia y que son de competencia para el desarrollo del presente proyecto serán descritas brevemente.

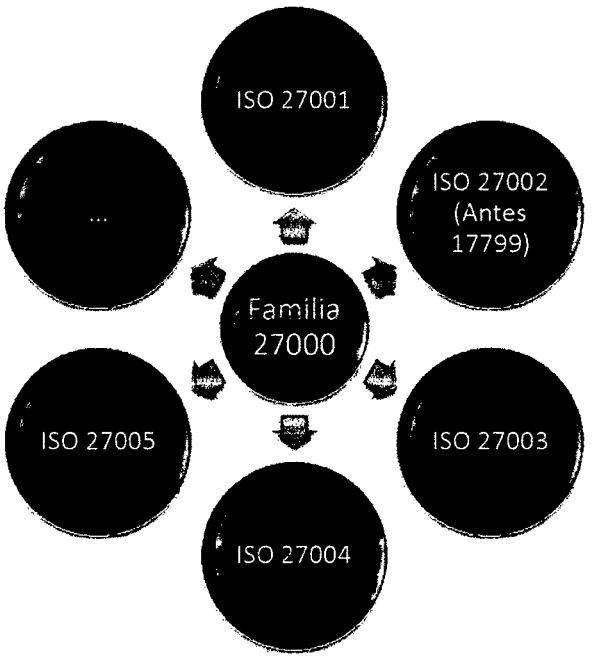


Figura 5: Familia ISO/IEC 27000

Varias de las normas de la familia ISO/IEC 27000 son aplicadas en el Perú bajo las iniciales NTP[13]. Las Normas técnicas peruanas publicadas por INDECOPI[14] son la NTP-ISO/IEC 27001:2008, NTP-ISO/IEC 17799:2007 (norma que en el Perú aún no ha sido renombrada), NTP-ISO/IEC 27003:2012 y NTP-ISO/IEC 27005:2009.

A. DESCRIPCIÓN GENERAL NTP-ISO/IEC 27001:2008

Norma técnica peruana elaborada por el Comité Técnico Permanente de Codificación e Intercambio Electrónico de Datos en el año 2008 donde se especifica los requerimientos obligatorios para establecer, implementar, operar, monitorear, mantener y mejorar un SGSI dentro de una organización. Cabe recalcar que esta norma es una transcripción de la norma internacional ISO/IEC 27001 del idioma inglés al español, al igual que

[13] NTP: Norma Técnica Peruana
[14] INDECOPI: Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual

sucede con las demás normas técnicas peruanas relacionadas a seguridad de la información [7]

Está norma tiene como fin asegurar una adecuada selección de controles de seguridad para proteger los activos de información.

El 23 de mayo del 2012 se publica la Resolución Ministerial N° 129-2012-PCM para aprobar el uso obligatorio de la "NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos" para entidades integrantes del Sistema Nacional de Información. Esta resolución también especifica que la certificación no es obligatoria y será decisión de cada entidad pública asumiendo los costos que implique dicha certificación.

La ISO 27001 es la única certificable de toda la familia; además existen certificaciones para profesionales en relación a su implementación y auditoría principalmente.

En apartados anteriores se menciona que un SGSI de basa en un modelo de mejora continua denominado PDCA (Plan-Do-Check-Act) y es en este modelo donde enfatiza la norma.

En la siguiente figura se muestra todos los puntos que detalla esta norma técnica peruana:

Figura 6: Estructura NTP-ISO/IEC 27001:2008
Fuente: NTP-ISO/IEC 27001:2008

En resumen, la implementación se debe iniciar definiendo el alcance del SGSI dentro de la organización, identificar activos de información que serán incluidos dentro del SGSI. Luego se debe definir una política del SGSI que será aprobada por la alta dirección y servirá como guía para la implementación del Sistema de Gestión. Finalmente se deberá de realizar un análisis de riesgos que permita identificar los activos de información que

tienen un alto grado de probabilidad de violar los pilares de un SGSI - confidencialidad, integridad y disponibilidad - El resultado del análisis de riesgos permitirá identificar los controles a implementar que son mencionados en forma residual en el "ANEXO 1" de esta NTP.

B. DESCRIPCIÓN GENERAL NTP-ISO/IEC 17799:2007

La ISO renombró esta norma como ISO/IEC 27002, en el Perú aún no ha sido renombrada, así que para el presente documento seguiremos mencionando a la norma como NTP-ISO/IEC 17799:2007.

Esta NTP fue elaborada por el Comité Técnico de Normalización de Codificación e Intercambio Electrónico de Datos, y el 22 de agosto del 2007 se aprueba el uso obligatorio de la NTP-ISO/IEC17799:2007 en las instituciones estatales mediante la Resolución Ministerial 246-2007-PCM.

Luego de aprobar el uso obligatorio de la NTP-ISO/IEC 27001, quedó sin efecto la Resolución Ministerial 197-2011-PCM que establecía la fecha límite de implementación de la NTP-ISO/IEC 17799:2007 en las entidades públicas.

La explicación se debe a lo siguiente: La ISO 27001 establece el marco de trabajo para definir un SGSI, centrándose en la visión de la gestión de la seguridad como un proceso continuo en el tiempo, y para certificar un proceso u organización es necesario analizar y gestionar los ***riesgos*** fundamentales a los que están expuestos. Mientras las ISO 17799 es una guía de buenas prácticas que ayuda a las organizaciones a mejorar la seguridad de la información, quien establece una serie de objetivos de control que deberían ser perseguidos por las organizaciones.

La norma contempla 11 dominios, 39 objetivos de control y 133 controles, sin embargo, la propia norma indica que no existe ningún tipo de priorización entre controles, y que las "sugerencias" que realiza no tienen por qué ser ni siquiera convenientes, en función del caso en cuestión [9]

En la figura 7 y en la tabla 2 se mencionan los dominios, objetivos de control y controles.

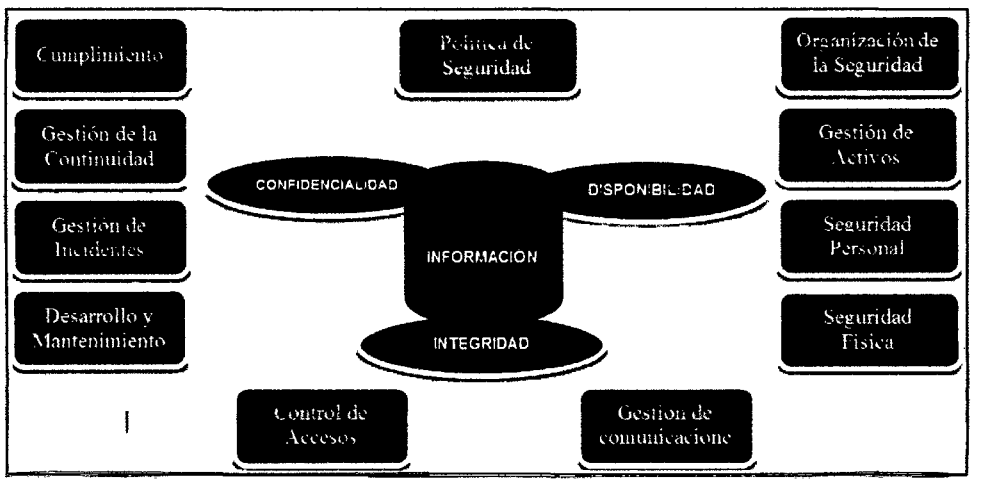


Figura 7: Dominios NTP-ISO/IEC 17799

A.5 Política de Seguridad		
	A.5.1 Política de Seguridad de la Información	
		A.5.1.1 Documentos de política de seguridad de la información
		A.5.1.2 Revisión de la política de seguridad de información
A.6 Seguridad Organizacional		
	A.6.1 Organización Interna	
		A.6.1.1 Comité de Gestión de seguridad de la información
		A.6.1.2 Coordinación de la seguridad de la información
		A.6.1.3 Asignación de responsabilidades sobre seguridad de la información
		A.6.1.4 Proceso de autorización para las nuevas instalaciones de procesamiento de información
		A.6.1.5 Acuerdos de Confidencialidad
		A.6.1.6 Contacto con autoridades
		A.6.1.7 Contacto con grupos de interés especial
		A.6.1.8 Revisión independiente de la seguridad de la información
	A.6.2 Seguridad del acceso a terceras partes	
		A.6.2.1 Identificación de riesgos por el acceso de terceros
		A.6.2.2 Requisitos de seguridad cuando se trata con clientes
		A.6.2.3 Requisitos de seguridad en contratos con terceros
A.7 Gestión de activos		
	A.7.1 Responsabilidad por los activos	

		A.7.1.1 Inventario de activos
		A.7.1.2 Propiedad de los activos
		A.7.1.3 Uso aceptable de los activos
	A.7.2 Clasificación de la información	
		A.7.2.1 Guías de clasificación
		A.7.2.2 Etiquetado y tratamiento de la información
A.8 Seguridad en recursos humanos		
	A.8.1 Previa al empleo	
		A.8.1.1 Roles y responsabilidades
		A.8.1.2 Investigación
		A.8.1.3Términos y condiciones de la relación laboral
	A.8.2 Durante el empleo	
		A.8.2.1 Gestión de responsabilidades
		A.8.2.2 Concientización, educación y entrenamiento en la seguridad de la Información
		A.8.2.3 Proceso disciplinario
	A.8.3 Finalización o cambio de empleo	
		A.8.3.1 Responsabilidades de finalización
		A.8.3.2 Devolución de activos
		A.8.3.3 Retiro de los derechos de acceso
A.9 Seguridad física y del entorno		
	A.9.1 Áreas seguras	
		A.9.1.1 Seguridad física perimetral
		A.9.1.2 Controles físicos de entradas
		A.9.1.3 Seguridad de oficinas, despachos y recursos
		A.9.1.4 Protección contra amenazas externas y ambientales
		A.9.1.5 El trabajo en las áreas seguras
		A.9.1.6 Áreas de carga, descarga y acceso público
	A.9.2 Seguridad de los equipos	
		A.9.2.1 Ubicación y protección de equipos
		A.9.2.2 Suministro eléctrico
		A.9.2.3 Seguridad de cableado
		A.9.2.4 Mantenimiento de equipos
		A.9.2.5 Seguridad de equipos fuera de los locales de la organización
		A.9.2.6 Seguridad en el re-uso o eliminación de equipos
		A.9.2.7 Retiro de propiedad
A.10 Gestión de comunicaciones y operaciones		
	A.10.1 Procedimientos y responsabilidades de operación	
		A.10.1.1 Documentación de procedimientos operativos

		A.10.1.2 Gestión de cambios
		A.10.1.3 Segregación de tareas
		A.10.1.4 Separación de las instalaciones de desarrollo, prueba y operación
	A.10.2 Gestión de entrega de servicios externos	
		A.10.2.1 Entrega de servicios
		A.10.2.2 Monitoreo y revisión de los servicios externos
		A.10.2.3 Gestión de cambios de los servicios externos
	A.10.3 Planificación y aceptación del sistema	
		A.10.3.1 Gestión de la capacidad
		A.10.3.2 Aceptación del sistema
	A.10.4 Protección contra software malicioso	
		A.10.4.1 Controles contra software malicioso
		A.10.4.2 Controles contra software móvil
	A.10.5 Gestión interna de respaldo y recuperación	
		A.10.5.1 Recuperación de la información
	A.10.6 Gestión de seguridad de redes	
		A.10.6.1 Controles de red
		A.10.6.2 Seguridad de los servicios de red
	A.10.7 Utilización y seguridad de los medios de información	
		A.10.7.1 Gestión de medios removibles
		A.10.7.2 Eliminación de medios
		A.10.7.3 Procedimientos de manipulación de la información
		A.10.7.4 Seguridad de la documentación de sistemas
	A.10.8 Intercambio de Información	
		A.10.8.1 Políticas y procedimientos para el intercambio de información
		A.10.8.2 Acuerdos de intercambio
		A.10.8.3 Seguridad de medios físicos en tránsito
		A.10.8.4 Seguridad del correo electrónico
		A.10.8.5 Seguridad en los sistemas de información de negocio
	A.10.9 Servicios de comercio electrónico	
		A.10.9.1 Seguridad en el comercio electrónico
		A.10.9.2 Seguridad en las transacciones en línea
		A.10.9.3 Información disponible públicamente
	A.10.10 Monitoreo	
		A.10.10.1 Registro de auditoría
		A.10.10.2 Uso del sistema de monitoreo
		A.10.10.3 Protección de la información de registro

		A.10.10.4 Registros de administrador y operador
		A.10.10.5 Registros con faltas
		A.10.10.6 Sincronización del reloj
A.11 Control de accesos		
	A.11.1 Requisitos de negocio para el control de accesos	
		A.11.1.1 Política de control de accesos
	A.11.2 Gestión de acceso de usuarios	
		A.11.2.1 Registro de usuarios
		A.11.2.2 Gestión de privilegios
		A.11.2.3 Gestión de contraseñas de usuario
		A.11.2.4 Revisión de los derechos de acceso de los usuarios
	A.11.3 Responsabilidades de los usuarios	
		A.11.3.1 Uso de contraseñas
		A.11.3.2 Equipo informático de usuario desatendido
		A.11.3.3 Política de pantalla y escritorio limpio
	A.11.4 Control de acceso a la red	
		A.11.4.1 Política de uso de los servicios de la red
		A.11.4.2 Autenticación de usuarios para conexiones externas
		A.11.4.3 Autenticación de equipos en la red
		A.11.4.4 Protección para la configuración de puertos y diagnóstico remoto
		A.11.4.5 Segregación de las redes
		A.11..4.6 Control de conexión a las redes
		A.11.4.7 Control de enrutamiento en la red
	A.11.5 Control de acceso al sistema operativo	
		A.11.5.1 Procedimientos seguros de conexión
		A.11.5.2 Identificación y autenticación del usuario
		A.11.5.3 Sistema de gestión de contraseñas
		A.11.5.4 Uso de programas utilitarios del sistema
		A.11.5.5 Desconexión automática de terminales
		A.11.5.6 Limitación del tiempo de conexión
	A.11.6 Control de acceso a las aplicaciones e información	
		A.11.6.1 Restricción de acceso a la información
		A.11.6.2 Aislamiento de sistemas sensibles
	A.11.7 Informática móvil y teletrabajo	
		A.11.7.1 Informática y comunicaciones móviles
		A.11.7.2 Teletrabajo
A.12 Adquisición de sistemas de información, desarrollo y mantenimiento		
	A.12.1 Requisitos de seguridad de los sistemas de información	

		A.12.1.1 Análisis y especificación de los requisitos de seguridad
	A.12.2 Proceso correcto en aplicaciones	
		A.12.2.1 Validación de los datos de entrada
		A.12.2.2 Control del proceso interno
		A.12.2.3 Integridad de mensajes
		A.12.2.4 Validación de los datos de salida
	A.12.3 Controles criptográficos	
		A.12.3.1 Política de uso de los controles criptográficos
		A.12.3.2 Gestión de claves
	A.12.4 Seguridad de los archivos del sistema	
		A.12.4.1 Control del software en producción
		A.12.4.2 Protección de los datos de prueba del sistema
		A.12.4.3 Control de acceso a la librería de programas fuente
	A.12.5 Seguridad en los procesos de desarrollo y soporte	
		A.12.5.1 Procedimientos de control de cambios
		A.12.5.2 Revisión técnica de los cambios en el sistema operativo
		A.12.5.3 Restricciones en los cambios a los paquetes de software
		A.12.5.4 Fuga de información
		A.12.5.5 Desarrollo externo de software
	A.12.6 Gestión de vulnerabilidades técnicas	
		A.12.6.1 Control de vulnerabilidades técnicas
A.13 Gestión de incidentes en la seguridad de la información		
	A.13.1 Reportando eventos y debilidades en la seguridad de la información	
		A.13.1.1 Reportando eventos de la seguridad de la información
		A.13.1.2 Reportando debilidades de la seguridad de la información
	A.13.2 Gestión de los incidentes y mejoras en la seguridad de la información	
		A.13.2.1 Responsabilidades y procedimientos
		A.13.2.2 Aprendiendo de los incidentes en la seguridad de la información
		A.13.2.3 Recolección de evidencia
A.14 Gestión de la continuidad del negocio		
	A.14.1 Aspectos de la gestión de continuidad del negocio en la seguridad de la información	
		A.14.1.1 Incluyendo la seguridad de la información en la gestión de la continuidad del negocio

		A.14.1.2 Continuidad del negocio y evaluación de riesgos
		A.14.1.3 Desarrollando e implementando planes de continuidad que incluyen la seguridad de la información
		A.14.1.4 Marco de planificación de la continuidad del negocio
		A.14.1.5 Probando, mantenimiento y reevaluando los planes de continuidad del negocio
A.15 Cumplimiento		
	A.15.1.1 Identificación de los requisitos legales	
		A.15.1.1 Identificación de la legislación aplicable
		A.15.1.2 Derechos de propiedad intelectual (DPI)
		A.15.1.3 Salvaguardas de los registros de la organización
		A.15.1.4 Protección de los datos y privacidad de la información personal
		A.15.1.5 Prevención en el mal uso de las instalaciones de procesamiento de la información
		A.15.1.6 Regulación de los controles criptográficos
	A.15.2 Cumplimiento con las políticas y estándares de seguridad y del cumplimiento técnico	
		A.15.2.1 Cumplimiento con los estándares y la política de seguridad
		A.15.2.2 Comprobación del cumplimiento técnico
	A.15.3 Consideraciones sobre la auditoría de sistemas	
		A.15.3.1 Controles de auditoría de sistemas
		A.15.3.2 Protección de las herramientas de auditoría de sistemas

Tabla 2: Objetivos de Control y Controles NTP-ISO/IEC 17799
Fuente: NTP-ISO/IEC 17799

C. DESCRIPCIÓN GENERAL NTP-ISO/IEC 27003:2012

Esta norma técnica peruana fue publicada el 12 de Octubre del 2012 bajo la denominación de "*Técnicas de Seguridad. Directrices para la Implementación de un Sistema de Gestión de la Seguridad de la Información*"

Esta NTP se centra en aspectos críticos necesarios para el exitoso diseño e implementación de un SGSI de acuerdo a la norma NTP-ISO/IEC 27001:2008. Describe el proceso de delimitación, diseño y puesta en marcha de diferentes planes de implementación de un SGSI. Igualmente incluye el proceso para obtener la aprobación de la Gerencia para

implementar un SGSI, define un alcance inicial del SGSI, y proporciona una guía de cómo hacer desde la planeación inicial hasta la implementación final de un proyecto de SGSI.

En [5] se hace referencia lo siguiente:

El contenido de esta nueva norma se detalla a continuación:

- (1) Alcance
- (2) Referencias Normativas
- (3) Términos y Definiciones
- (4) Estructura de esta Norma Internacional
- (5) Obteniendo la aprobación de la alta dirección para iniciar un SGSI
- (6) Definir el alcance del SGSI, límites y políticas
- (7) Evaluación de los requerimientos de seguridad de la información
- (8) Evaluación de Riesgos y Plan de tratamiento de riesgos
- (9) Diseño del SGSI
- Anexo A: lista de chequeo para la implementación de un SGSI.
- Anexo B: Roles y responsabilidades en seguridad de la información
- Anexo C: Información sobre auditorías internas.
- Anexo D: Estructura de las políticas de seguridad.
- Anexo E: Monitoreo y seguimiento del SGSI.

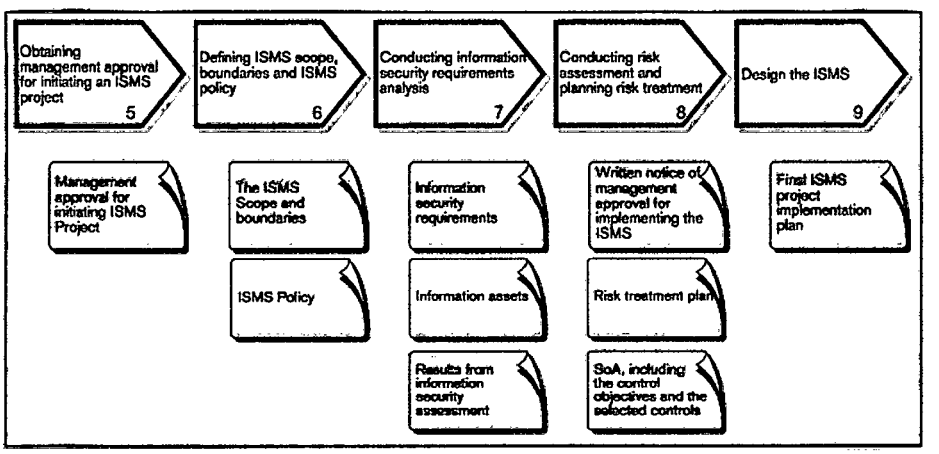


Figura 8: Etapas NTP-ISO/IEC 27003:2012
Fuente: ISO/IEC 27003

Parte de esta norma será utilizada para la implementación del presente proyecto.

D. DESCRIPCIÓN GENERAL NTP-ISO/IEC 27005:2009

En [4] se hace referencia a:

La norma NTP-ISO/IEC 27005:2009 proporciona directrices para la gestión de riesgos de seguridad de la información en una organización, dando particular soporte a los requisitos de un SGSI de acuerdo a la norma NTP-ISO/IEC 27001:2008.

La gestión del riesgo en la seguridad de la información debería ser una parte integral de todas las actividades de gestión de seguridad de la información y se deberían aplicar tanto a la implementación como al funcionamiento continuo de un SGSI.

La gestión del riesgo en la seguridad de la información debería ser un proceso continuo. Tal proceso debería establecer el contexto, evaluar los riesgos, tratar los riesgos utilizando un plan de tratamiento para implementar las recomendaciones y decisiones. La gestión del riesgo analiza lo que puede suceder y cuáles pueden ser las posibles consecuencias, antes de decidir lo que se debería hacer y cuando hacerlo, con el fin de reducir el riesgo hasta un nivel aceptable.

La gestión del riesgo en la seguridad de la información debería contribuir a:

- La identificación de los riesgos.
- La evaluación de los riesgos en términos de sus consecuencias para el negocio y la probabilidad de su ocurrencia.
- La comunicación y entendimiento de la probabilidad y las consecuencias de estos riesgos.
- El establecimiento del orden de prioridad para el tratamiento de los riesgos.
- La priorización de las acciones para reducir la ocurrencia de los riesgos.

- La participación de los interesados cuando se toman las decisiones sobre gestión del riesgo y mantenerlos informados sobre el estado de la gestión del riesgo
- La eficacia del monitoreo del tratamiento del riesgo
- El monitoreo y revisión con regularidad del riesgo y los procesos de gestión de riesgos
- La captura de información para mejorar el enfoque de la gestión de riesgos
- La educación de los directores y del personal acerca de los riesgos y las acciones que se toman para mitigarlos

El proceso de gestión del riesgo en la seguridad de la información se puede aplicar a la organización en su totalidad, a una parte separada de la organización (por ejemplo, un departamento, una ubicación física, un servicio), a cualquier sistema de información, existente o planificado, o a aspectos particulares del control (por ejemplo, la planificación de la continuidad del negocio).

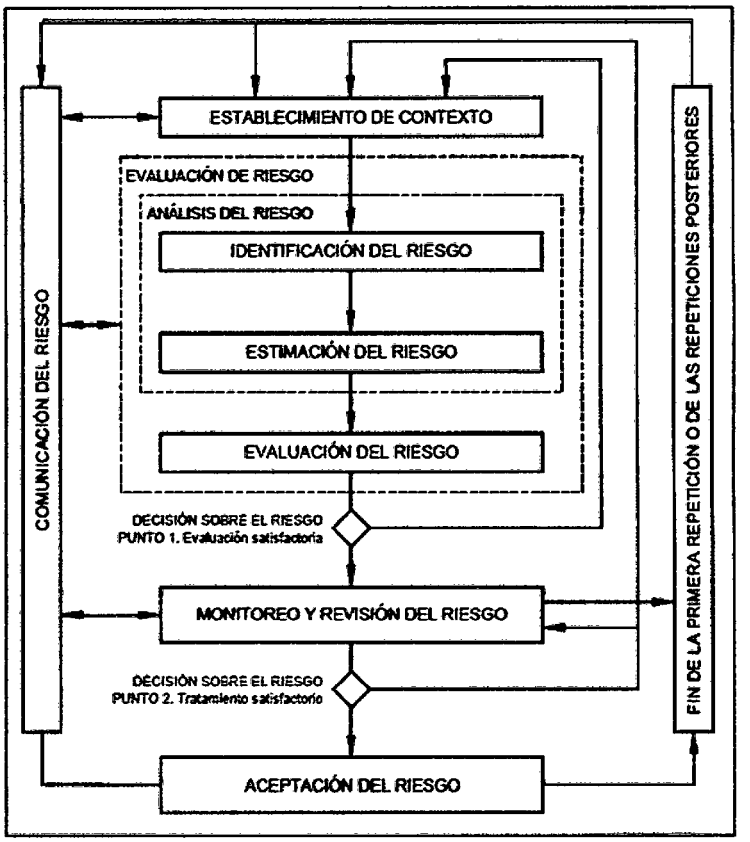


Figura 9: Proceso de Gestión de Riesgos
Fuente: NTP-ISO/IEC 27005:2009

PROCESO SGSI	PROCESO DE GESTIÓN DEL RIESGO EN SEGURIDAD DE LA INFORMACIÓN
Planificar (Plan)	Establecer el contexto Valoración del riesgo Planificación del tratamiento del riesgo Aceptación del riesgo
Hacer (Do)	Implementación del plan de tratamiento del riesgo
Verificar (Check)	Monitoreo y revisión continuos de los riesgos
Actuar (Act)	Mantener y mejorar el proceso de gestión del riesgo en la seguridad de la información

Tabla 3: Modelo PDCA
Fuente: NTP-ISO/IEC 27005:2009

3.3.2. COBIT

COBIT[15] 5 provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Dicho de una manera sencilla, ayuda a las empresas a crear el valor óptimo desde TI manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos. COBIT 5 permite a las TI ser gobernadas y gestionadas de un modo holístico para toda la empresa, abarcando al negocio completo de principio a fin y las áreas funcionales de responsabilidad de TI, considerando los intereses relacionados con TI de las partes interesadas internas y externas. COBIT 5 es genérico y útil para empresas de todos los tamaños, tanto comerciales, como sin ánimo de lucro o del sector público [8].

COBIT 5 se basa en cinco principios (figura 10) claves para el gobierno y la gestión de las TI empresariales.

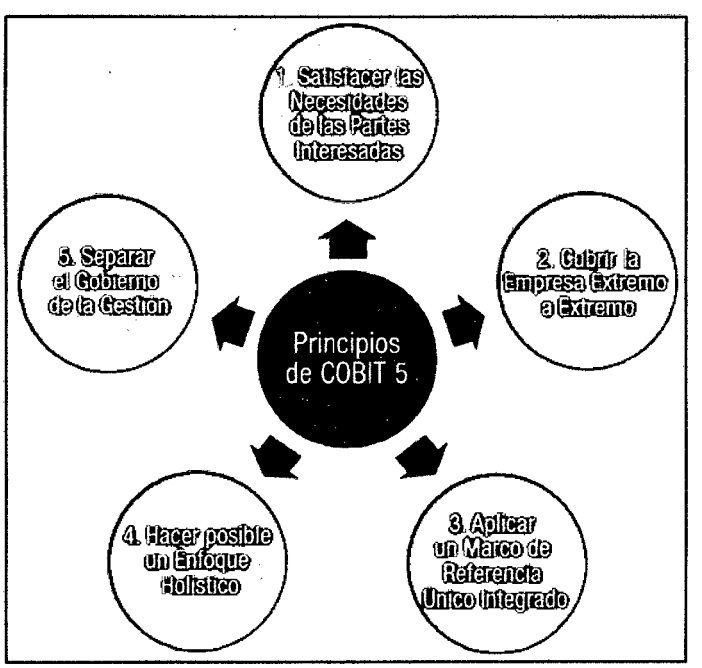


Figura 10: Principios de COBIT 5
Fuente: Cobit 5 Framework

[15] COBIT: Control Objectives for Information and related Technology

3.3.3. ITIL

En [11] se hace referencia de lo siguiente:

ITIL[16] es el estándar de facto del mercado para la Administración de Servicios de IT y desarrollado en el Reino Unido donde contribuyeron diversas organizaciones. ITIL se define como una biblioteca que documenta las Buenas Prácticas de la Gestión de Servicios de TI.

ITIL fue desarrollada al reconocer que las organizaciones dependen cada vez más de la Informática para alcanzar sus objetivos corporativos. Esta dependencia en aumento ha dado como resultado una necesidad creciente de servicios informáticos de calidad que se correspondan con los objetivos del negocio, y que satisfagan los requisitos y las expectativas del cliente. A través de los años, el énfasis pasó de estar sobre el desarrollo de las aplicaciones TI a la gestión de servicios TI. La aplicación TI (a veces nombrada como un sistema de información) sólo contribuye a realizar los objetivos corporativos si el sistema está a disposición de los usuarios y, en caso de fallos o modificaciones necesarias, es soportado por los procesos de mantenimiento y operaciones [11].

A lo largo de todo el ciclo de los productos TI, la fase de operaciones alcanza cerca del 70-80% del total del tiempo y del coste, y el resto se invierte en el desarrollo del producto. De esta manera, los procesos eficaces y eficientes de la Gestión de Servicios TI se convierten en esenciales para el éxito de los departamentos de TI. Esto se aplica a cualquier tipo de organización, grande o pequeña, pública o privada, con servicios TI centralizados o descentralizados, con servicios TI internos o suministrados por terceros. En todos los casos, el servicio debe ser fiable, consistente, de alta calidad, y de coste aceptable [11].

[16] ITIL: Biblioteca de Infraestructura de Tecnologías de la Información

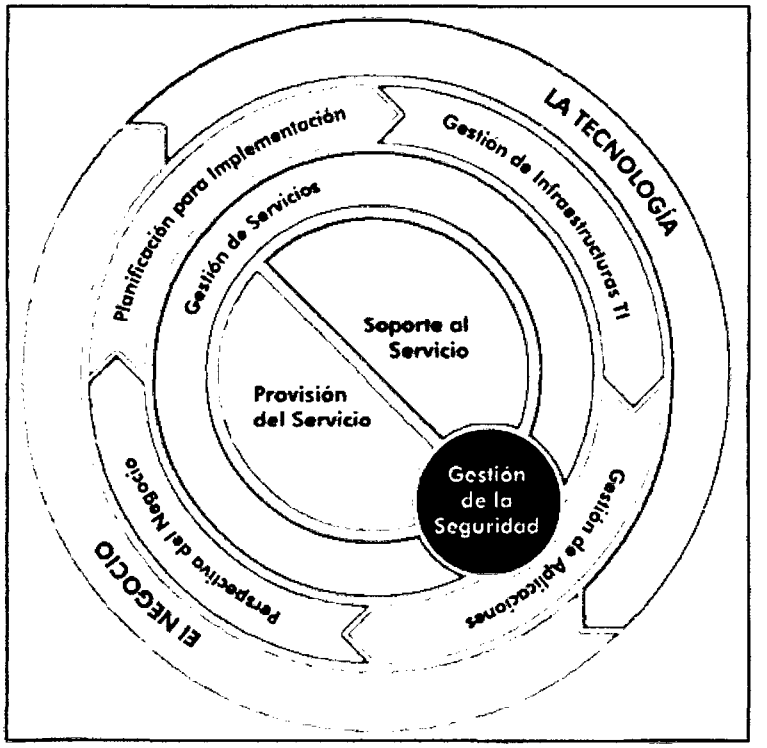


Figura 11: ITIL
Fuente: http://itil.osiatis.es

ITIL está basada en la administración de servicios desde el punto de vista del negocio, en un conjunto de 11 procesos divididos en dos secciones:

Service Support: Procesos de Soporte y Operación de los servicios y sistemas en el día a día

- *Gestión de Incidentes*: Minimizar el impacto en las operaciones del negocio, restaurando los niveles normales de servicio de acuerdo a los tiempos establecidos. Este proceso debe asegurar la mejor forma de lograr los niveles de servicio, calidad y disponibilidad establecidos.
- *Gestión de Problemas*: Minimizar la interrupción de los servicios de TI organizando los recursos de TI para resolver problemas de acuerdo a lo que el negocio requiere, previniendo la recurrencia de incidentes y problemas encontrando la causa raíz y actuando proactivamente para la prevención de incidentes problemas y errores.

- *Gestión de Service Desk*: Actuar como punto central de contacto entre el usuario y la administración de servicios. Manejar los incidentes y requerimientos, proveer una interface para otras actividades como Change, Problem, Configuration, Release, Service Level and IT Service Continuity Management.

- *Gestión de Configuración*: Proveer un modelo lógico de la infraestructura de TI para identificar, controlar, mantener y verificar las versiones de todos los elementos de configuración existentes, su estado, relaciones y ciclos de vida.

- *Gestión de Cambios*: Administrar todos los cambios que pueden impactar en la habilidad de TI en entregar servicios a través de un proceso formal, centralizado, programado y controlado para asegurar que la infraestructura de TI se encuentra alineada con los requerimientos del negocio con un mínimo riesgo.

- *Gestión de Versiones*: Manejar efectivamente el uso de servicios dentro de la organización de TI realizando el planeamiento, diseño, construcción, testing y distribución del software y hardware en un ambiente de producción asegurando que solo las versiones probadas y autorizadas estén en uso.

Service Delivery: Procesos de optimización del Servicio alineados con el Negocio

- *Gestión de Niveles de Servicio*: Mantener y graduar la mejora del servicio TI alineado con los requerimientos del negocio a través de un ciclo constante de acuerdos, monitoreo de acuerdos, reportes y revisión si los servicios de TI cubren con los requerimientos de usuarios especificados en los SLA, fomentando acciones para erradicar SLA no aceptables.

- *Gestión de Capacidad*: Entender los requerimientos futuros del negocio, la operación de la organización, la infraestructura de TI, asegurar que toda la actual y futura capacidad y aspectos de performance de los requerimientos del negocio son proveídos de una manera efectiva en el manejo de costo.

- *Gestión de Disponibilidad*: Asegurarse que en la entrega de servicios de TI los recursos estén disponibles en el lugar, cuándo y por quien sean

requeridos, realizando el planeamiento y construcción de una infraestructura confiable manteniendo soporte clave de acuerdo a los requerimientos de servicios.

- *Gestión de Continuidad*: Soportar el proceso de administración de la continuidad del negocio asegurando que los servicios de TI puedan ser recuperados de acuerdo a la escala de tiempo acordada con el negocio.
- *Gestión Financiera*: Proveer una administración efectiva de costos de los activos y los recursos financieros usados en la provisión de servicios de TI. Gestionar los costos de la infraestructura de TI y proveer una base financiera saludable para las decisiones de negocio relacionadas a TI identificando y contabilizando el costo de la entrega de los servicios, y donde sea posible recobrando costos en una manera equitativa.

IV. DESARROLLO DEL PROYECTO

4.1. IDENTIFICACIÓN DE PROCESOS CRÍTICOS

4.1.1. GENERALIDADES GOBIERNO REGIONAL DE CAJAMARCA

En [12] se hace referencia a lo siguiente:

Sector del Gobierno Regional de Cajamarca

Administrativas Públicas en General

Legitimidad y naturaleza jurídica

Los Gobiernos Regionales emanan de la voluntad popular. El Gobierno Regional de Cajamarca es una persona jurídica de derecho público, con autonomía política, económica y administrativa en asuntos de su competencia, constituyendo, para su administración económica y financiera, un Pliego Presupuestal.

Misión del Gobierno Regional de Cajamarca

El Gobierno Regional de Cajamarca, en cumplimiento de sus competencias exclusivas, compartidas y delegadas, contribuye al desarrollo integral y sostenible de la región, organizando y conduciendo democrática, descentralizada y desconcentradamente la gestión pública regional, en el marco de las políticas nacionales y sectoriales.

Visión del Gobierno Regional de Cajamarca

Institución pública regional con identidad propia, capital humano calificado y nivel tecnológico avanzado, capaz de administrar y brindar con calidad recursos y servicios públicos, propiciar condiciones favorables para el desarrollo de la inversión privada y liderar procesos de concertación con la sociedad civil, en el marco de una efectiva lucha contra la pobreza y la defensa del medio ambiente y sus recursos.

Estructura orgánica del Gobierno Regional de Cajamarca

La estructura orgánica del Gobierno Regional de Cajamarca se puede visualizar en la siguiente figura.

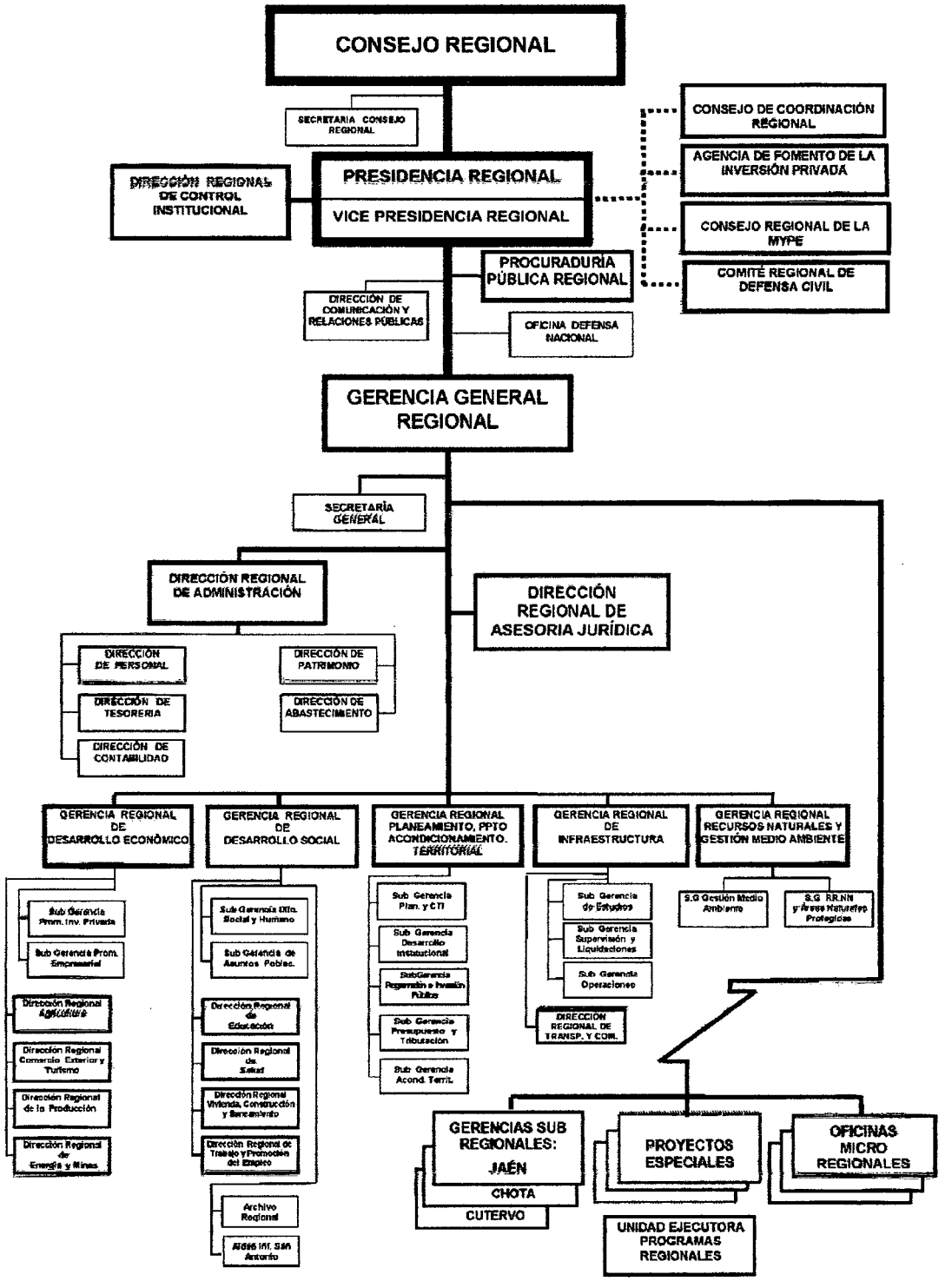


Figura 12: Organigrama Gobierno Regional de Cajamarca
Fuente: www.regioncajamarca.gob.pe

En el organigrama no figura el área de TI, esta área es denominada "Centro de Información y Sistemas" y pertenece a la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial. El Centro de Información y Sistemas brinda los servicios de TI en los cuales se apoyan varios de los procesos del GRC[17].

4.1.2. PROCESOS DEL GOBIERNO REGIONAL DE CAJAMARCA

A. MAPA DE PROCESOS

Para tener un panorama general interno del Gobierno Regional de Cajamarca, se ha graficado el mapa de procesos (*Figura 13*), donde se identifican los procesos estratégicos, operativos y de apoyo. En ellos también se tiene en cuenta a la sociedad y a los proveedores. La sociedad (ciudadanía) es a quienes va orientado los servicios y es a los que se tiene que satisfacer con proyectos de envergadura en educación, salud, comunicaciones, etc.

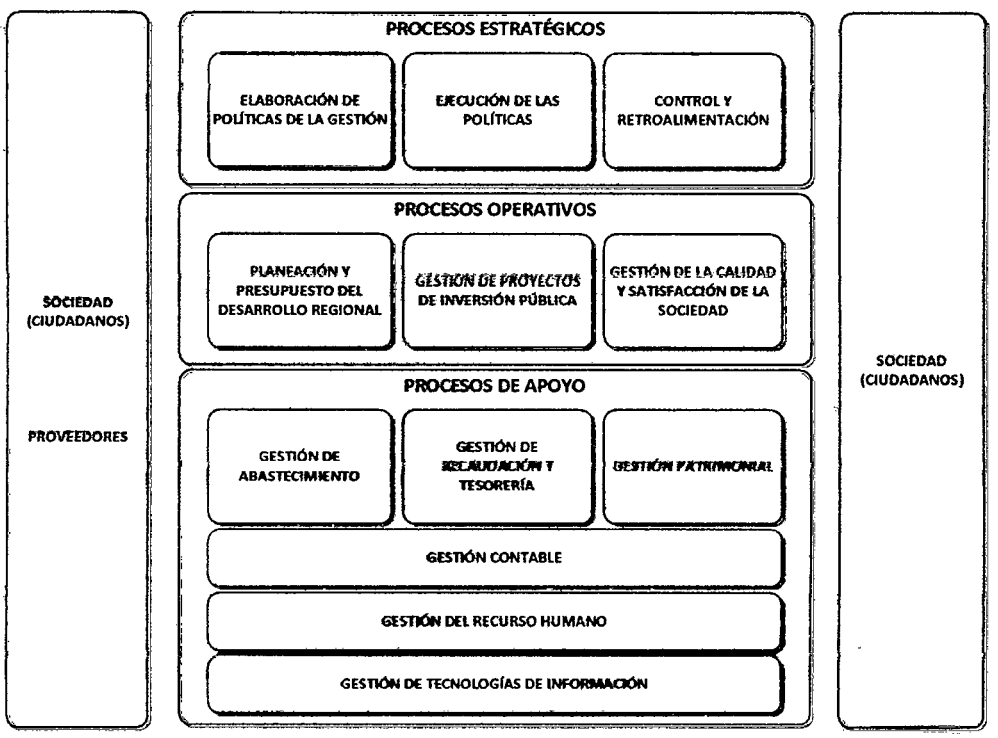


Figura 13: Mapa de Procesos Gobierno Regional

[17] GRC: Gobierno Regional de Cajamarca

En el mapa de procesos se ha identificado un proceso operativo que es el core del negocio "Gestión de Proyectos de Inversión Pública" y en el que nos centraremos.

B. PROCESO GESTIÓN DE PROYECTOS DE INVERSIÓN PÚBLICA

En [13] se hace referencia a lo siguiente:

Ciclo de un Proyecto de Inversión Pública

El ciclo de un proyecto de inversión pública contempla las fases de Pre Inversión, Inversión y Post Inversión.

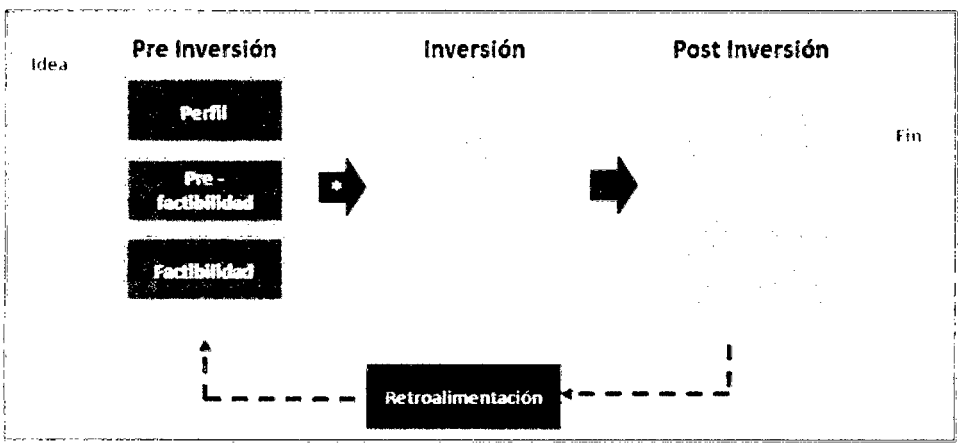


Figura 14: Fases de un PIP
Fuente: www.mef.gob.pe

Fase de Pre Inversión

La Pre Inversión tiene como objetivo evaluar la conveniencia de realizar un PIP, es decir, exige contar con los estudios que sustenten que es socialmente rentable, sostenible y concordante con los lineamientos de política establecida por las autoridades correspondientes. Estos criterios sustentan su declaración de viabilidad, requisito indispensable para iniciar su ejecución.

Los estudios de Pre Inversión se deben basar en un diagnóstico del área de influencia del PIP, del servicio sobre el cual se intervendría, así como de los grupos involucrados en todo el ciclo. Con sustento en el diagnóstico se definirá el problema a solucionar, sus causas y sus efectos; sobre esta base, se plantea el PIP y las alternativas de solución. Es necesario conocer la brecha de servicios que atenderá el PIP, que será el punto de referencia

para dimensionar los recursos y estimar los costos de inversión, operación y mantenimiento. Finalmente, se estimarán los flujos de beneficios y costos sociales para definir su rentabilidad social. Es importante, así mismo, demostrar la sostenibilidad en la provisión de los servicios objeto de intervención.

Es importante mencionar que no todos los proyectos requieren el mismo nivel de análisis técnico en la fase de pre inversión: a mayor magnitud de inversión, mayores serán los riesgos de pérdida de recursos y, consecuentemente, es mayor la necesidad de información y estudios técnicos que reduzcan la incertidumbre en la toma de decisiones.

Los niveles de estudios de pre inversión mínimos que deberá tener un proyecto para poder ser declarado viable son los siguientes:

MONTO DE UN PROYECTO	ESTUDIOS REQUERIDOS
Hasta S./ 1'200,000	Perfil simplificado
Mayor a S./ 1'200,000 Hasta S./ 10'000,000.00	Perfil
Mayor a S./ 10'000,000.00	Factibilidad

Tabla 4: Fases de Estudio de un PIP[18]
Fuente: www.mef.gob.pe

La UF[19] es la responsable de formular los estudios de pre inversión del proyecto y puede ser cualquier oficina o entidad del sector público (Ministerios, Gobiernos Nacionales, Gobiernos Regionales o Gobiernos Locales) que sea designada formalmente en la entidad y registrada por la Oficina de Programación de Inversiones correspondiente.

Los PIP son registrados por la UF en el Banco de Proyectos del SNIP[20], utilizando un formato estándar. De acuerdo con las competencias de las OPI[21], el Banco asignará automáticamente a la responsable de su evaluación; dicha OPI es la que declarará la viabilidad al PIP si cumple con

[18] PIP: Proyecto de Inversión Pública
[19] UF: Unidad Formuladora
[20] SNIP: Sistema Nacional de Inversión Pública
[21] OPI: Oficina de Programación e Inversiones

los criterios establecidos. La DGPM[22] declara la viabilidad de los PIP que son financiados con endeudamiento público.

El Banco de Proyectos es una herramienta informática que permite almacenar, actualizar, publicar y consultar información resumida, relevante y estandarizada de los proyectos en su fase de pre inversión.

Fase de Inversión

Una vez que un proyecto ha cumplido satisfactoriamente la fase de pre inversión, es decir, cuenta con los estudios de pre inversión (perfil, pre factibilidad y factibilidad) y ha sido declarado viable por la OPI correspondiente, se encuentra habilitado para ingresar a la Fase de Inversión.

En esta fase se puede distinguir las etapas de: Diseño (el desarrollo del estudio definitivo, expediente técnico u otro documento equivalente) y la ejecución misma del proyecto, que debe ceñirse a los parámetros técnicos, económicos y ambientales con los cuales fue declarado viable:

- Diseño: Se elabora el estudio de detalle (o equivalente) del proyecto, incluyendo la planificación de la ejecución, el presupuesto, las metas físicas proyectadas, las especificaciones técnicas, el programa de conservación y reposición de equipos y los requerimientos estimados de personal para la operación y mantenimiento.
- Ejecución: Se realiza la implementación de las actividades programas y, según caso, el desarrollo de la obra física. En esta etapa se realizan las acciones del proyecto, la licitación de los bienes, servicios u obras a adquirir e implementar, el seguimiento y control de los contratos así como la revisión periódica de los avances de la ejecución del proyecto. El cierre de la ejecución del proyecto marca el fin de la Fase de Inversión.

La UE[23] es responsable de la elaboración del estudio de detalle (o equivalente), de la ejecución, cierre y transferencia del proyecto a la Entidad responsable de la operación y mantenimiento, cuando corresponda.

[22] DGPM: Dirección General de Programación Multianual

Post Inversión

La post inversión comprende la operación y mantenimiento del proyecto así como la evaluación ex post. Esta última fase se inicia cuando se ha cerrado la ejecución del proyecto y éste ha sido transferido a la Entidad responsable de su operación y mantenimiento. En esta fase, y durante todo su periodo de vida útil, se concreta la generación de beneficios del proyecto.

- Operación y mantenimiento: En esta etapa se debe asegurar que el proyecto ha producido una mejora en la capacidad prestadora de bienes o servicios públicos de una Entidad de acuerdo a las condiciones previstas en el estudio que sustentó su declaración de viabilidad. Para ello, la Entidad responsable de su operación y mantenimiento, deberá priorizar la asignación de los recursos necesarios para dichas acciones.
- Evaluación ex post: Es un proceso que permite investigar en qué medida las metas alcanzadas por el proyecto se han traducido en los resultados esperados en correlato con lo previsto durante la fase de pre inversión. Las UE, en coordinación con la OPI que evaluó el proyecto, son las responsables por las evaluaciones ex post de los PIP que ejecutan. En los PIP cuya viabilidad ha sido declarada sobre la base de un Perfil, la evaluación Ex post la puede realizar una agencia independiente o un órgano distinto de la UE que pertenezca al propio Sector, Gobierno Regional o Local, sobre una muestra representativa de los PIP cuya ejecución haya finalizado. Los estudios de evaluación Ex post se considerará terminados cuando cuenten con la conformidad por parte de la DGPI respecto de la evaluación efectuada.

En los PIP cuya viabilidad ha sido declarada sobre la base de un estudio de Pre factibilidad o Factibilidad, una agencia independiente realiza la evaluación Ex post sobre una muestra representativa del total de los PIP cuya ejecución haya finalizado.

El proceso core "Gestión de Proyectos de Inversión Pública" se grafica del siguiente modo:

[23] UE: Unidad Ejecutora.

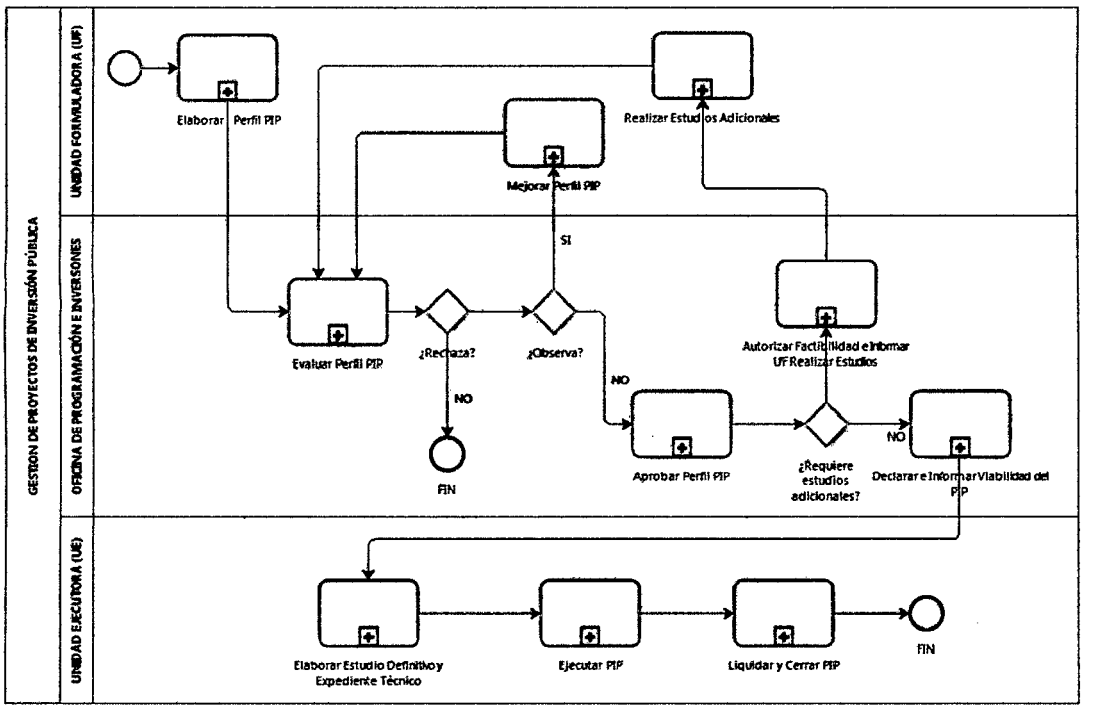


Figura 15: Proceso Gestión de Proyectos de Inversión Pública
Fuente: Elaborado por el autor

La figura 15 muestra todo el proceso de "Gestión de Proyectos de Inversión Pública", donde hemos identificado a los actores "Unidad Formuladora", "Oficina de Programación e Inversiones" y "Unidad Ejecutora". Para poder identificar ***los activos de información en general*** se debería desmenuzar cada uno de los subprocesos indicados.

Para efectos del presente proyecto se explotará el sub proceso "Elaborar Perfil PIP" permitiendo identificar los activos de información, y posteriormente sólo centramos en los activos de Tecnologías de Información.

C. SUB PROCESO ELABORAR PERFIL PIP

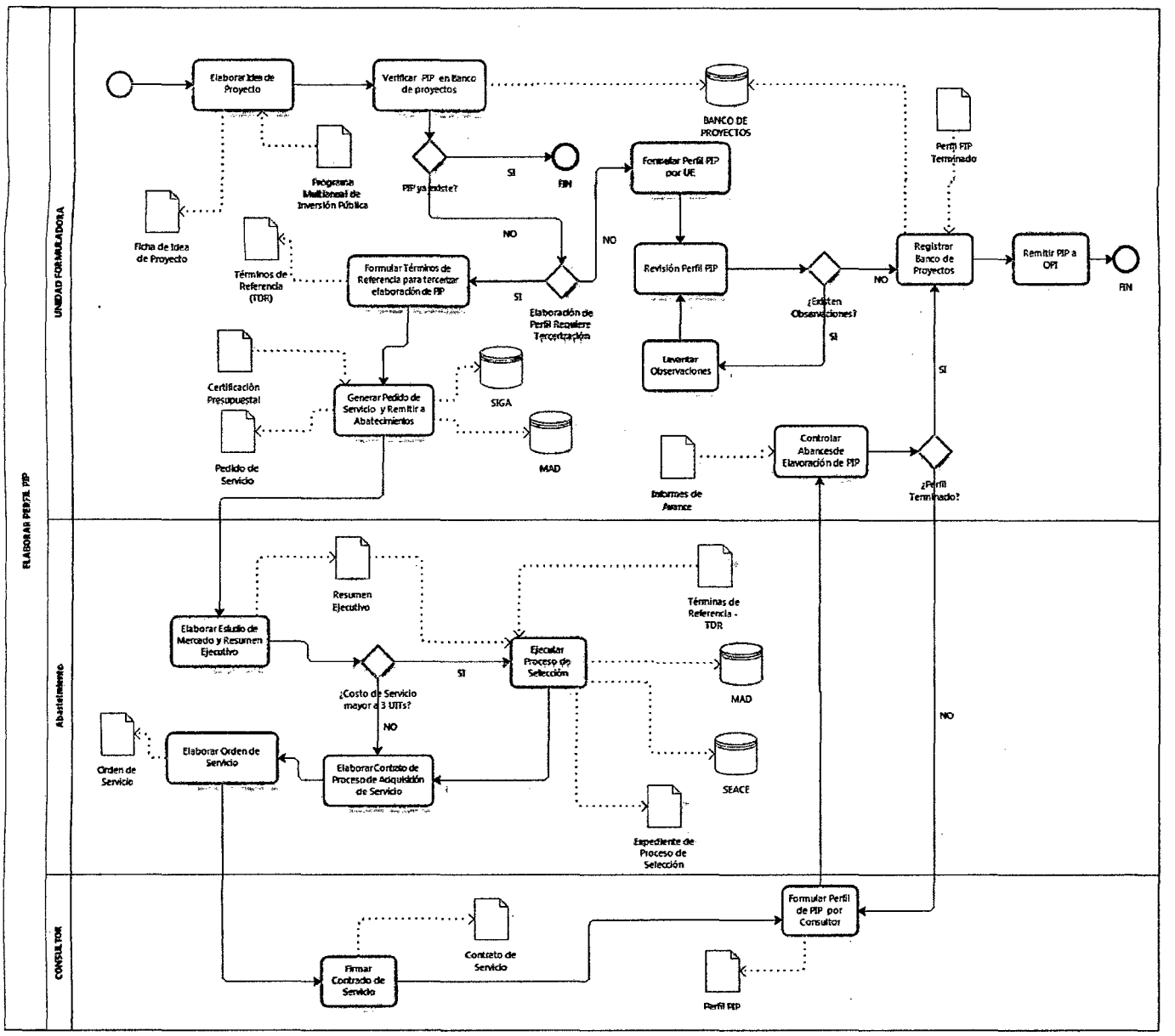


Figura 16: Sub Proceso Elaborar Perfil PIP
Fuente: Elaborado por el Autor

4.2. ANÁLISIS DE RIESGOS DE TI

El análisis de riesgos de tecnologías de información tiene sustento en la norma NTP-ISO/IEC 27005:2009.

La gestión de riesgos es un aspecto muy importante para dar soporte a un Sistema de Gestión de la Seguridad de la Información. Uno de los puntos importantes que

especifica la norma NTP-ISO/IEC 27005:2009 es tener en cuenta los objetivos estratégicos, políticas y estrategias de la organización, los procesos del negocio, entre otras más [4].

Para este proyecto tendremos muy en cuenta el Proceso Core del Gobierno Regional de Cajamarca, el cual ya fue detallado en apartados anteriores.

Las normas NTP-ISO/IEC 27001:2008 y NTP-ISO/IEC 27005:2009 nos sugieren definir los siguientes puntos:

- Alcance y límites del análisis de riesgos (NTP-ISO/IEC 27005:2009)
- Identificación de los activos de Información (NTP-ISO/IEC 27005:2009)
- Identificación de las amenazas (NTP-ISO/IEC 27005:2009)
- Identificación de controles existentes (NTP-ISO/IEC 27005:2009)
- Identificación de vulnerabilidades (NTP-ISO/IEC 27005:2009)
- Estimación del riesgo (NTP-ISO/IEC 27005:2009)
- Declaración de aplicabilidad (NTP-ISO/IEC 27001:2008)

4.2.1. ALCANCE Y LÍMITES

En todo Sistema de Gestión de Seguridad de la Información se debe de establecer su alcance y sus límites. El presente proyecto únicamente se concentrará en los activos de TI, excluyendo cualquier activo que no sea tecnología. Este alcance es obligatorio tenerlo en cuenta, a partir de este la gestión de riesgos (que incluye el análisis de riesgos) debe estar alineada al SGSI.

Declaración del Alcance:

El Análisis de Riesgos de TI en el Gobierno Regional de Cajamarca - Sede abarcará los principales activos de tecnologías de información vinculados al Proceso Core "Gestión de Proyectos de Inversión", permitiendo a futuro ejecutar acciones preventivas y correctivas para garantizar la Disponibilidad, Integridad y Confidencialidad los mismos.

La definición del alcance es muy importante para el desarrollo del proyecto, abarcar mucho implicaría posiblemente costos muy elevados que ocasionaría desechar las propuestas de mejora, y abarcar poco podría afectar a la continuidad del negocio.

En esta definición del alcance también se está centrando en el proceso core del Gobierno Regional de Cajamarca, que es "***Gestión de proyectos de Inversión Pública***", y lo definimos como el proceso más importante en base a la razón de ser de esta institución que es "contribuir con el desarrollo integral y sostenible de la región", y el desarrollo se da mediante la gestión de proyectos de inversión pública. También la norma NTP-ISO/IEC 27001:2008 especifica: "el diseño e implementación de un SGSI de una organización está influenciado por las necesidades y objetivos del negocio" [7].

4.2.2. REQUISITOS NORMATIVOS Y REGULATORIOS

Es importante menciona y tener en cuenta los requisitos normativos relacionados con la Seguridad de la Información, los cuales se detallan a continuación:

- ✓ ***Resolución Ministerial N° 129-2012-PCM:*** Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de Seguridad. Sistemas de gestión de seguridad de la Información. Requisitos" en todas las entidades integrantes del Sistema Nacional de Informática"
- ✓ ***Ley Nº 27291:*** Ley que permite el uso de medios electrónicos para la manifestación de voluntad y la utilización de la firma electrónica.
- ✓ ***Ley Nº 27269:*** Ley de Firmas y Certificados Digitales
- ✓ ***Ley Nº 27309:*** Ley que incorpora los delitos informáticos al Código Penal

- ✓ ***Código Penal, Artículo 154:*** Delito de Violación a la Intimidad
- ✓ ***Ley N° 28493:*** Ley que regula el uso del Correo Electrónico Comercial No Solicitado (SPAM)
- ✓ ***Decreto Supremo N° 043-2003-PCM:*** Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública
- ✓ ***Resolución Jefatural N° 088-2003-INEI:*** Directiva sobre "Normas para el uso del servicio de correo electrónico en las entidades de la Administración Pública"
- ✓ ***Ley N° 28612:*** Ley que norma el uso, adquisición y adecuación del software en la administración pública.
- ✓ ***Decreto Supremo N° 013-2003-PCM y sus modificatorias:*** Medidas para garantizar la legalidad de la adquisición de software en entidades y dependencias del sector público
- ✓ ***Ley N° 29733:*** Ley de Protección de los datos (LOPD) y privacidad de la información personal (artículo 2 numeral 6 de la Constitución Política del Perú).

4.2.3. EVALUACIÓN DEL ESTADO ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN

La Resolución Ministerial N° 129-2012-PCM indica el uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 27001:2008, por lo cual todas las instituciones están en la obligación de implementar un Sistema de Gestión de Seguridad de la Información.

Actualmente el Gobierno Regional de Cajamarca no cuenta con un Sistema de Gestión de Seguridad de la Información.

La única evidencia encontrada en relación al tema es la de implementar algunos controles de la ISO 17799 es mediante el Oficio N° 1512-2011-CG/ORCA, documento que fue emitido por la Contraloría General de la República luego de una Veeduría realizada en Noviembre del 2011 en donde se sugiere implementar los siguientes controles basados en la NTP-ISO/IEC 17799:

- 10.5.1 Recuperación de la Información
- 9.1.1 Perímetro de Seguridad Física
- 9.1.2 Controles físicos de entrada
- 9.2.1 Instalación y protección de equipos
- 9.4.1 Protección contra amenazas externas y ambientales
- 9.2.2 Suministro Eléctrico
- 11.2.2 Gestión de Privilegios
- 11.3.3 Política de pantalla y escritorio limpio
- 12.4.2 Protección de los datos de prueba del sistema
- 10.4.1 Medidas y controles contra software malicioso
- 11.2.4 Revisión de los derechos de acceso del usuario
- 10.1.1 Documentación de procedimientos operativos
- 10.1.2 Gestión de Cambios
- 12.5.1 Procedimientos de control de cambios
- 10.1.3 Segregación de tares
- 10.1.4 Separación de los recursos para desarrollo y para producción
- 9.2.3 Seguridad del Cableado

Recopilando información, haciendo inspecciones y entrevistas los controles mencionados no han sido implementados y no se cumplen.

También se ha identificado el uso de un aplicativo de mesa de ayuda mediante el cual se canaliza las incidencias, requerimientos y problemas de TI, es de importancia para llevar los controles de futuras incidencias en relación a la seguridad de la información. Pues la norma NTP-ISO/IEC 27001:2008 también sugiere llevar un inventario de incidencias relacionadas con seguridad de la información. Teniendo implementado un SGSI, se puede realizar un mapeo con marcos de trabajo como COBIT o ITIL (ver anexo 1.2), que se relación con diverso objetivos de control de la ISO 27002.

Concluimos que en el Gobierno Regional de Cajamarca no se ha implementado ningún control de la ISO 17799 (ahora ISO 27002), es por ello que se debería considerar todos los controles resultantes del análisis de riesgos.

4.2.4. IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN

4.2.4.1. IDENTIFICACIÓN

Para entrar ya de lleno al Análisis de Riesgos, la NTP-ISO/IEC 27005:2009 recomienda iniciar identificando los activos de información, luego valorarlos y priorizarlos; esto para evitar incluir activos de poca relevancia para el SGSI.

La identificación de activos en el presente proyecto vamos a partir del sub proceso ***"Elaborar Perfil PIP"***.

Una organización que tiene mapeados y debidamente documentados sus procesos, la implementación de un SGSI sería más sencilla, pues en base a ellos se podría identificar los activos de información iniciales, y a partir de ellos identificar activos de información de los cuales depende.

Explotar el sub proceso ***"Elaborar Perfil PIP"*** permitirá identificar los activos de TI más importantes de la sede del Gobierno Regional de Cajamarca, y es más que suficiente para identificar los activos de TI más relevantes del GRC; de acuerdo a la magnitud de la empresa y al alcance será obligatorio en otras situaciones explotar los procesos o sub procesos que sean necesarios para identificar activos no sólo de TI, sino activos de información en general.

Debemos tener en cuenta que el presente proyecto sólo se centrará en activos de TI; de no ser así se tendría que explotar y analizar todos los sub procesos inmersos en "Gestión de Proyectos de Inversión Pública", ya que es muy probable que se identifique información (documentación), personas, ambientes físicos, etc; que deberán ser protegidos.

En la siguiente tabla de detallan los activos identificados en el mapeo del sub proceso de la figura 16, los cuales los clasificamos como información y software:

TIPO	NOMBRE DE ACTIVO	DESCRIPCIÓN DEL ACTIVO DE INFORMACIÓN
INFORMACIÓN	**Programa Multianual de Inversión Pública – PMIP**	Conjunto de PIP a ser ejecutados en un período no menor de tres años y ordenados de acuerdo a las políticas y prioridades del sector.

Ficha de Idea de Proyecto	Consiste en la presentación de la información más relevante y directamente relacionada con el proyecto (Nombre, objetivos, nº beneficiarios, costo, tiempo de ejecución, responsable o responsables de la ejecución), es decir, se elabora un diagnóstico del estado en el que se encuentra el conocimiento acerca del tema del proyecto y un enfoque en particular describiendo si hubo con anterioridad proyectos relacionados con el propuesto, con la solución o con las alternativas de solución planteadas.
Términos de Referencia - TDR	Documento que contienen las especificaciones técnicas, objetivos y estructura de cómo ejecutar un determinado estudio, trabajo, proyecto, comité, conferencia, negociación, etc.
Certificación Presupuestal	Acto de administración, cuya finalidad es garantizar que se cuenta con el crédito presupuestario disponible y libre de afectación, para comprometer el gasto del proyecto con cargo al presupuesto institucional autorizado para el año fiscal respectivo, previo cumplimiento de las disposiciones legales vigentes que regulen el compromiso del proyecto a ejecutar . Dicha certificación implica la reserva del presupuesto, hasta el perfeccionamiento del compromiso y la realización del correspondiente registro presupuestario del Proyecto.
Pedido de Servicio	Documento creado por un centro de costo (cualquier área del GRC que cuente con presupuesto) mediante el cual se solicita al área de Abastecimientos la adquisición de un bien o servicio.
Informes de Avance	Documento que contiene la información parcial o totalizada de un Perfil.
Resumen Ejecutivo	Documento en el que se detalla los resultados de las cotizaciones determinando un valor referencial final para el bien o servicio que solicita el centro de costos (área usuaria)
Perfil de Proyecto de Inversión Pública	Documento que contiene una descripción simplificada de un proyecto. Además de definir el propósito y la pertenencia del proyecto, presenta un

		primer estimado de las actividades requeridas y de la inversión total que se necesitará, así como de los costos operativos anuales, y, en el caso de proyectos destinados a la generación de ingresos, del ingreso anual.
	Orden de Servicio	Luego de finalizada la etapa de cotización y de proceso de selección (si es el caso), se genera la orden de servicio mediante el sistema SIGA.
	Expediente Proceso de Selección	Documento que se actualiza de forma constante desde el inicio hasta el final del proceso de selección del servicio a adquirir (bases del proceso, propuestas técnicas y económicas de los postores, etc)
	Contrato de Servicio	Finalizado el proceso de cotización y proceso de selección (si es el caso), el área de abastecimientos genera el contrato mediante el cual se vincula al proveedor con cierto servicio solicitado por el área usuaria.
SOFTWARE	**Sistema MAD**	Aplicativo de gestión documentaria denominado Módulo de Administración Documentaria, empleado para el procesamiento y seguimiento de documentos del Gobierno Regional de Cajamarca.
	SEACE	El Sistema Electrónico de Contrataciones del Estado – SEACE, es un sistema integral, compuesto por políticas, procedimientos, normas y **software basado en el uso del internet,** con el fin de dar transparencia, optimizar, modernizar y generar ahorros en las contrataciones públicas del Perú.
	Sistema SIGA	Sistema Integrado de Gestión Administrativa, que es empleado para la administración logística del Gobierno Regional de Cajamarca.
	Banco de Proyectos	Es un aplicativo informático que sirve para almacenar, actualizar, publicar y consultar información resumida, relevante y estandarizada de los proyectos de inversión pública en su fase de pre inversión.

Tabla 5: Fase preliminar de identificación de activos de información

Ya identificados los principales activos de información, procedemos a identificar activos de información de los que depende cada activo de información detallados en la tabla 5. Para que un documento, un servicio un software exista es muy probable que dependa de otros activos y es esto lo que nos detalla la tabla 6.

CLASE DE ACTIVO	NOMBRE	ACTIVO DE INFORMACIÓN DEL QUE DEPENDE
ACTIVOS PRIMARIOS	**Programa Multianual de Inversión Pública - PMIP**	Impresora Microsoft Word Sistema Operativo Windows 7 Antivirus PC Escritorio Servicio de Directorio Activo
	Ficha de Idea de Proyecto	Impresora Microsoft Word Sistema Operativo Windows 7 Antivirus PC Escritorio Servicio de Directorio Activo
	Términos de Referencia - TDR	Impresora Microsoft Word Sistema Operativo Windows 7 Antivirus PC Escritorio Servicio de Directorio Activo
	Certificación Presupuestal	Impresora SIAF Sistema Operativo Windows 7 PC Escritorio Servicio de Directorio Activo
	Pedido de Servicio	Impresora Sistema SIGA Base de datos SIGA Sistema Operativo Windows 7 PC Escritorio Servicio de Directorio Activo
	Informes de Avance	Microsoft Word Sistema Operativo Windows 7 PC Escritorio Servicio de Directorio Activo
	Resumen Ejecutivo	Microsoft Word Sistema Operativo Windows 7 PC Escritorio Servicio de Directorio Activo

	Perfil de Proyecto de Inversión Pública	Microsoft Word Sistema Operativo Windows 7 PC Escritorio Servicio de Directorio Activo Banco de Proyectos
	Orden de Servicio	Impresora Sistema SIGA Base de datos SIGA Sistema Operativo Windows 7 PC Escritorio Servicio de Directorio Activo
	Expediente Proceso de Selección	Microsoft Word Sistema Operativo Windows 7 PC Escritorio Servicio de Directorio Activo
	Contrato de Servicio	Microsoft Word Sistema Operativo Windows 7 PC Escritorio Servicio de Directorio Activo
ACTIVOS DE SOPORTE	**Sistema MAD**	Base de datos MAD Gestor de Base de Datos Servidor Base de Datos/MAD/SIGA Sistema Operativo Windows Server 2008 R2 Datacenter Aire Acondicionado Sistema Contra incendios UPS para Datacenter Switch Core Swicth Acceso Firewall Cableado estructurado Administrador de Base de Datos Administrador de Redes y Servidores
	Fi	Servicio de Internet Sistema Operativo Windows 7 Pc de Escritorio Cableado Estructurado Switch Acceso Swicth Core Firewall Router ISP Datacenter Aire Acondicionado Sistema Contra incendios UPS para Datacenter Administrador de Redes y Servidores

	SISTEMA SIGA	Base de Datos SIGA Gestor de Base de Datos Servidor Base de Datos/MAD/SIGA Sistema Operativo Windows Server 2008 R2 Antivirus Datacenter Aire Acondicionado Sistema Contra incendios UPS para Datacenter Switch Core Swicth Acceso Firewall Cableado estructurado Administrador de Base de Datos Administrador de Redes y Servidores
	Banco de Proyectos	Servicio de Internet Sistema Operativo Windows 7 Antivirus Pc de Escritorio Cableado Estructurado Switch Acceso Swicth Core Firewall Router ISP Datacenter Aire Acondicionado Sistema Contra incendios UPS para Datacenter

Tabla 6: Dependencia de Activos de Información

Adicionalmente, de los activos identificados en la Tabla 6, se aprecian dos activos de información que son de vital importancia que deben de ser analizados.

CLASE DE ACTIVO	NOMBRE	ACTIVO DE INFORMACIÓN DEL QUE DEPENDE
ACTIVOS DE SOPORTE ADICIONALES	**Sistema SIAF**	DBFs de SIAF Servidor SIAF Sistema Operativo Windows Server 2008 Antivirus Datacenter Aire Acondicionado Sistema Contra incendios UPS para Datacenter Switch Core Swicth Acceso Firewall Cableado estructurado Administrador de Redes y Servidores
	Servicio de Directorio Activo	Servicio de DNS Sistema Operativo Windows Server 2008 R2 Antivirus Servidor de Directorio Activo y DNS Switch Core Switch Acceso Firewall Cableado Estructurado Datacenter Aire Acondicionado Sistema Contra incendios UPS para Datacenter Administrador de Redes y Servidores

Tabla 7: Dependencia de Activos de Información Adicionales

Finalmente consolidamos los activos de información, estos son mostrados en la tabla N° 8.

Es obligatorio identificar al dueño de cada activo de información, para que posteriormente se le asigne la responsabilidad de velar por la integridad, disponibilidad y confidencialidad de sus activos de información. La categorización de activos (clase de activo) se basa también en lo que nos especifica la norma NTP-ISO/IEC 27005:2009; activos primarios y activos de soporte. Luego de detallar cada uno de estos activos, sólo nos concentraremos en los activos de soporte relacionados a Tecnologías de Información específicamente.

CLASE DE ACTIVO	TIPO	NOMBRE DE ACTIVO	DUEÑO
ACTIVOS PRIMARIOS	INFORMACIÓN	Programa Multianual de Inversión Pública – PMIP	Gobierno Regional Cajamarca
		Ficha de Idea de Proyecto	Unidad Formuladora
		Términos de Referencia - TDR	Unidad Formuladora
		Certificación Presupuestal	Centro de Costo
		Pedido de Servicio	Dirección Regional de Administración
		Informes de Avance	Unidad Formuladora
		Resumen Ejecutivo	Dirección Regional de Administración
		Perfil de Proyecto de Inversión Pública	Unidad Formuladora
		Orden de Servicio	Dirección Regional de Administración
		Expediente Proceso de Selección	Dirección Regional de Administración
		Contrato de Servicio	Dirección Regional de Administración
		Base de Datos MAD	Centro de Información y Sistemas
		DBFs SIAF	Dirección Regional de Administración
		Base de datos SIGA	Dirección Regional de Administración
ACTIVOS DE SOPORTE	SOFTWARE	Antivirus	Centro de Información y Sistemas
		Banco de Proyectos	Ministerio de Economía y Finanzas
		Gestor de Base de Datos	Centro de Información y Sistemas
		Sistema MAD	Centro de Información y Sistemas
		Microsoft Word	Centro de Información y Sistemas

		SEACE	Organismo Supervisor de Contrataciones del estado
		Servicio de Directorio Activo	Centro de Información y Sistemas
		Servicio de DNS	Centro de Información y Sistemas
		Sistema SIAF	Ministerio de Economía y Finanzas
		Sistema SIGA	Ministerio de Economía y Finanzas
		Sistema Operativo Windows 7	Centro de Información y Sistemas
		Sistema Operativo Windows Server 2008 R2	Centro de Información y Sistemas
	HARDWARE	Impresora	Centro de Costo
		PC Escritorio	Centro de Información y Sistemas
		Servidor Base de Datos/MAD/SIGA	Centro de Información y Sistemas
		Servidor de Directorio Activo y DNS	Centro de Información y Sistemas
		UPS para Datacenter	Centro de Información y Sistemas
	REDES	Cableado estructurado	Centro de Información y Sistemas
		Firewall	Centro de Información y Sistemas
		Router ISP	Centro de Información y Sistemas
		Servicio de Internet	Centro de Información y Sistemas
		Swicth Acceso	Centro de Información y Sistemas
		Swicth Core	Centro de Información y Sistemas
	PERSONAL	Administrador de Base de Datos	Centro de Información y Sistemas
		Administrador de Redes y Servidores	Centro de Información y Sistemas

[redacted]	SHIO	Aire Acondicionado	Centro de Información y Sistemas
		Datacenter	Centro de Información y Sistemas
		Sistema Contra incendios del Datacenter	Centro de Información y Sistemas

Tabla 8: Consolidado de Activos de Información de TI

4.2.4.2. VALORACIÓN DE ACTIVOS

Teniendo en cuenta la norma NTP-ISO/IEC 27005-2009, la valoración de los activos puede ser mediante una estimación cualitativa o cuantitativa [4]. Optaremos por tener la estimación cualitativa, basándonos en los tres pilares de un SGSI que son confidencialidad, integridad y disponibilidad; también se podría realizar la combinación de ambas, la norma no la restringe; es decisión de cada organización. Para iniciar la valoración vamos a definir los siguientes parámetros que permitirán determinar si un activo es crítico o no.

CONFIDENCIALIDAD		
C	Confidencial	Activo restringido para un grupo del GRC
I	Uso Interno	Activo dispuesto sólo personal del GRC
P	Uso Pública	Activo dispuesto para el público en General

Tabla 9: Leyenda Valoración de Activos desde el punto de vista de Confidencialidad

INTEGRIDAD		
S	Sensible	Activo que requiere controles estrictos para su protección
I	Normal	Activo que requiere controles habituales para su protección
P	Baja	Activo que requiere controles mínimos para su protección

Tabla 10: Leyenda Valoración de Activos desde el punto de vista de Integridad

DISPONIBILIDAD		
MA	Muy Alta	Tiempo tolerable de interrupción menor a 2 horas
A	Alta	Tiempo tolerable mayor a 2 horas y menor a 4 horas
M	Media	Tiempo tolerable mayor a 4 horas y menor a 1 día
B	Baja	Tiempo tolerable mayor a 1 día y menor a 2

		días
MB	Muy Baja	Tiempo tolerable mayor a 2 días y menor a 7 días

Tabla 11: Leyenda Valoración de Activos desde el punto de vista de Disponibilidad

VALORACIÓN DEL ACTIVO		
CODIGO	VALOR	DESCRIPCION
A	Alto	Nivel Confidencialidad: Confidencial Nivel Integridad: Sensible Nivel Disponibilidad: Muy Alta, Alta
M	Medio	Nivel Confidencialidad: Uso Interno Nivel Integridad: Normal Nivel Disponibilidad: Media
B	Bajo	Nivel Confidencialidad: Uso Público Nivel Integridad: Baja Nivel Disponibilidad: Baja, Muy Baja

Tabla 12: Posibles Valores de un Activo de TI

Teniendo en cuenta los valores de las tablas 9, 10, 11 y 12; se ha elaborado un Excel que permita determinar los valores de los activos de TI identificados que son mostrados en el siguiente cuadro:

ID	ACTIVO	TIPO DE ACTIVO	CLASIFICACION INFORMACION			VALORACION DEL ACTIVO		
			CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	NIVEL	VALOR	
INF01	Base de Datos MAD	INF	Confidencial	Sensible	Alta	Alto	3	●
INF02	DBFs SIAF	INF	Confidencial	Sensible	Muy Alta	Alto	3	●
INF03	Base de datos SIGA	INF	Confidencial	Sensible	Muy Alta	Alto	3	●
SW01	Banco de Proyectos	SW	Uso Pública	Normal	Baja	Medio	2	○
SW02	Gestor de Base de Datos	SW	Confidencial	Normal	Muy Alta	Alto	3	●
SW03	Sistema MAD	SW	Confidencial	Normal	Muy Alta	Alto	3	●
SW04	Microsoft Word	SW	Uso Interno	Baja	Muy Baja	Medio	2	
SW05	SEACE	SW	Uso Pública	Normal	Media	Medio	2	○

SW06	Servicio de Directorio Activo	SW	Uso Interno	Normal	Muy Alta	Alto	3	●
SW07	Servicio de DNS	SW	Uso Interno	Normal	Muy Alta	Alto	3	●
SW08	Sistema SIAF	SW	Confidencial	Sensible	Muy Alta	Alto	3	●
SW09	Sistema SIGA	SW	Confidencial	Sensible	Muy Alta	Alto	3	●
SW10	Sistema Operativo Windows 7	SW	Uso Interno	Baja	Baja	Medio	2	
SW11	Sistema Operativo Windows Server 2008 R2	SW	Uso Interno	Normal	Muy Alta	Alto	3	●
SW12	Antivirus	SW	Uso Interno	Sensible	Muy Alta	Alto	3	●
HW01	Impresora	HW	Uso Interno	Baja	Muy Baja	Medio	2	○
HW02	PC Escritorio	HW	Uso Interno	Normal	Baja	Medio	2	
HW03	Servidor Base de Datos/MAD/SIGA	HW	Confidencial	Sensible	Muy Alta	Alto	3	●
HW04	Servidor de Directorio Activo y DNS	HW	Confidencial	Sensible	Muy Alta	Alto	3	●
HW05	Servidor SIAF	HW	Confidencial	Sensible	Muy Alta	Alto	3	●
HW06	UPS para Datacenter	HW	Uso Interno	Normal	Muy Alta	Alto	3	●
RED01	Cableado estructurado	REDES	Uso Interno	Normal	Muy Alta	Alto	3	●
RED02	Firewall	REDES	Uso Interno	Sensible	Muy Alta	Alto	3	●
RED03	Router ISP	REDES	Uso Interno	Baja	Muy Alta	Alto	3	●
RED04	Servicio de Internet	REDES	Uso Interno	Normal	Muy Alta	Alto	3	●
RED05	Swicth Acceso	REDES	Uso Interno	Normal	Alta	Alto	3	●
RED05	Swicth Core	REDES	Uso Interno	Sensible	Muy Alta	Alto	3	●
PER01	Administrador de Base de Datos	PERSONAL	Confidencial	Sensible	Muy Alta	Alto	3	●
PER02	Administrador de Redes y Servidores	PERSONAL	Confidencial	Sensible	Muy Alta	Alto	3	●

SIT01	Aire Acondicionado	SITIO	Uso Interno	Normal	Muy Alta	Alto	3
SIT03	Datacenter	SITIO	Confidencial	Normal	Muy Alta	Alto	3
SIT03	Sistema Contra incendios del Datacenter	SITIO	Uso Interno	Normal	Muy Alta	Alto	3

Tabla 13: Fase preliminar Valoración de Activos de Información

Luego de haber determinado la valoración de activos, sólo se quedarán los activos más críticos (Valor Alto - 3), y con ellos continuaremos el análisis de riesgos. No tendría sentido incluir todos los activos de información identificados, debido a que el análisis se volvería muy complejo, y la implementación de controles a todos los activos probablemente sería innecesaria, costosa y el Gobierno Regional de Cajamarca es muy posible que opte por no implementarlos.

Teniendo en cuenta las consideraciones del párrafo anterior, de los 32 activos de información de TI identificados; sólo 26 pasarán por el análisis de riesgos.

Como se puede observar en la siguiente tabla, cada activo está debidamente codificado, clasificado por tipo (como puede ser información, software, hardware, etc), clasificación basada en los pilares de la seguridad de la información y la valoración de activos. Esto permite tener el inventario de los activos de información que serán actualizados periódicamente, algunos de ellos ya no figurarán, otros continuarán y nuevos surgirán.

ID	ACTIVO	TIPO DE ACTIVO	CLASIFICACION INFORMACION			VALORACION DEL ACTIVO	
			CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	NIVEL	VALOR
INF01	Base de Datos MAD	INF	Confidencial	Sensible	Alta	Alto	3
INF02	DBFs SIAF	INF	Confidencial	Sensible	Muy Alta	Alto	3
INF03	Base de datos SIGA	INF	Confidencial	Sensible	Muy Alta	Alto	3
SW02	Gestor de Base de Datos	SW	Confidencial	Normal	Muy Alta	Alto	3

SW03	Sistema MAD	SW	Confidencial	Normal	Muy Alta	Alto	3	●
SW06	Servicio de Directorio Activo	SW	Uso Interno	Normal	Muy Alta	Alto	3	●
SW07	Servicio de DNS	SW	Uso Interno	Normal	Muy Alta	Alto	3	●
SW08	Sistema SIAF	SW	Confidencial	Sensible	Muy Alta	Alto	3	●
SW09	Sistema SIGA	SW	Confidencial	Sensible	Muy Alta	Alto	3	●
SW11	Sistema Operativo Windows Server 2008 R2	SW	Uso Interno	Normal	Muy Alta	Alto	3	●
SW12	Antivirus	SW	Uso Interno	Sensible	Muy Alta	Alto	3	●
HW03	Servidor Base de Datos/MAD/SIGA	HW	Confidencial	Sensible	Muy Alta	Alto	3	●
HW04	Servidor de Directorio Activo y DNS	HW	Confidencial	Sensible	Muy Alta	Alto	3	●
HW05	Servidor SIAF	HW	Confidencial	Sensible	Muy Alta	Alto	3	●
HW06	UPS para Datacenter	HW	Uso Interno	Normal	Muy Alta	Alto	3	●
RED01	Cableado estructurado	REDES	Uso Interno	Normal	Muy Alta	Alto	3	●
RED02	Firewall	REDES	Uso Interno	Sensible	Muy Alta	Alto	3	●
RED03	Router ISP	REDES	Uso Interno	Baja	Muy Alta	Alto	3	●
RED04	Servicio de Internet	REDES	Uso Interno	Normal	Muy Alta	Alto	3	●
RED05	Swicth Acceso	REDES	Uso Interno	Normal	Alta	Alto	3	●
RED05	Swicth Core	REDES	Uso Interno	Sensible	Muy Alta	Alto	3	●
PER01	Administrador de Base de Datos	PERSONAL	Confidencial	Sensible	Muy Alta	Alto	3	●
PER02	Administrador de Redes y Servidores	PERSONAL	Confidencial	Sensible	Muy Alta	Alto	3	●
SIT01	Aire Acondicionado	SITIO	Uso Interno	Normal	Muy Alta	Alto	3	●
SIT03	Datacenter	SITIO	Confidencial	Normal	Muy Alta	Alto	3	●

SIT03	Sistema Contra Incendios del Datacenter	SITIO	Uso Interno	Normal	Muy Alta	Alto	3

Tabla 14: Activos de Información de TI para análisis de riesgos

4.2.4.3. IDENTIFICACIÓN Y VALORACIÓN DE AMENAZAS

En [4] NTP-ISO/IEC 27005:2009 se hace referencia los dos siguientes párrafos:

Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas y, por lo tanto, a las organizaciones. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas. Es recomendable identificar tanto los orígenes de las amenazas accidentales como de las deliberadas. Una amenaza puede tener su origen dentro o fuera de la organización. Las amenazas se deberían identificar genéricamente y por tipo (por ejemplo, acciones no autorizadas, daño físico, fallas técnicas) y, cuando sea adecuado, las amenazas individuales dentro de la clase genérica identificada. Esto significa que ninguna amenaza se pasa por alto, incluidas las inesperadas, pero teniendo en cuenta que el volumen de trabajo requerido es limitado.

La identificación de las amenazas y la estimación de la probabilidad de ocurrencia puede ser obtenida de los propietarios o de los usuarios del activo, del personal de recursos humanos, del administrador de las instalaciones y de especialistas en seguridad de la información, expertos en seguridad física, área jurídica y otras organizaciones que incluyen organismos legales, bien sea autoridades, compañías de seguros y autoridades del gobierno nacional.

Teniendo en cuenta las indicaciones obtenidas de la norma NTP-ISO/IEC 27005:2009 y que han sido mencionados en el párrafo anterior, se han identificado las amenazas como se muestran en las siguientes tablas:

ORIGEN DE LAS AMENAZAS	
A	Accidentales
D	Deliberadas
E	Ambientales

Tabla 15: Origen de amenazas

ID	AMENAZA	ORIGEN
A01	Abuso de privilegios	A, D
A02	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	A, D
A03	Acceso de personas ajenas a la institución quienes podrían robar información	A, D
A04	Acceso no autorizado a la red	D
A05	Acceso no autorizado al Datacenter	A, D
A06	Accidentes del personal	A, D
A07	Ataque de hackers a las vulnerabilidades de las aplicaciones	D
A08	Caída del servicio	A,D, E
A09	Cambio de configuraciones no autorizadas en las aplicaciones o servicios	A, D
A10	Corrupción de Datos	A,D, E
A11	Deterioro / Obsolescencia de equipamiento	A,D, E
A12	Deterioro de la infraestructura física	A,D, E
A13	Deterioro del cableado de red	A,D, E
A14	Errores de operación de los usuarios	A, D
A15	Fácil descifrado de las contraseñas de los usuarios por parte de personas inescrupulosas	D
A16	Falla / Corte de suministro eléctrico	A,D, E
A17	Falla / Corte del servicio de Internet	A,D, E
A18	Falla de Equipo	A, D, E
A19	Falla equipo de aire acondicionado	A,D, E
A20	Fallo del Sistema Contra Incendios	A,D, E

A21	Fallo UPS principal del Datacenter	A,D, E
A22	Filtraciones de información y accesos no autorizados al sistema	
A23	Incendios	A, D
A24	Infección de software malicioso	A
A25	Interferencia Electromagnética	A, D, E
A26	Inundaciones	A,D, E
A27	Mal Funcionamiento del Sistema	
A28	Manipulación de hardware	A, D
A29	Penetración y propagación de virus en la intranet por mal uso de internet / o memorias extraíbles	A, D
A30	Renuncia/Ausentismo del personal al centro de labores	A, D
A31	Robo de Equipamiento	D
A32	Robo de Información	D
A33	Saturación del Servicio	A, D

Tabla 16: Lista de amenazas identificadas

Luego de haber identificado las amenazas, las relacionaremos con los activos de información de TI vinculados al análisis de riesgos; procedemos a valorar cada una de las amenazas teniendo en cuenta la probabilidad de ocurrencias y que es descrita en la siguiente leyenda:

PROB. DE OCURRENCIA	DEFINICIÓN
Muy Alta = 4	Una vez al mes
Alta = 3	Trimestral
Media =2	Semestral
Baja = 1	Una vez cada 1 año o más

Tabla 17: Leyenda valoración de amenazas

ID	ACTIVO	AMENAZAS	VALORACIÓN
INF01	BASE DE DATOS MAD	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	1
		Filtraciones de información y accesos no autorizados al sistema	1
		Corrupción de Datos	1
		Robo de Información	1
		Abuso de privilegios	2
INF02	DBFs SIAF	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	1
		Filtraciones de información y accesos no autorizados al sistema	2
		Corrupción de Datos	3
		Robo de Información	1
		Abuso de privilegios	2
INF03	BASE DE DATOS SIGA	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	1
		Filtraciones de información y accesos no autorizados al sistema	2
		Corrupción de Datos	1
		Robo de Información	1
		Abuso de privilegios	1
SW02	GESTOR DE BASE DE DATOS	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3
		Caída del servicio	4
		Saturación del Servicio	2
		Ataque de hackers a las vulnerabilidades de las aplicaciones	1
		Mal Funcionamiento del Sistema	1
SW03	SISTEMA MAD	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2
		Caída del servicio	4
		Saturación del Servicio	3
		Ataque de hackers a las vulnerabilidades de las aplicaciones	1
		Errores de operación de los usuarios	

		Filtraciones de información y accesos no autorizados al sistema	3
		Robo de Información	1
		Mal Funcionamiento del Sistema	2
		Fácil descifrado de las contraseñas de los usuarios por parte de personas inescrupulosas	4
		Acceso de personas ajenas a la institución quienes podrían robar información	4
		Abuso de privilegios	1
SW06	SERVICIO DE DIRECTORIO ACTIVO	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	1
		Caída del servicio	3
		Saturación del Servicio	2
		Ataque de hackers a las vulnerabilidades de las aplicaciones	1
		Acceso no autorizado a la red	1
		Mal Funcionamiento del Sistema	1
		Penetración y propagación de virus en la intranet por mal uso de internet / o memorias extraíbles	1
		Abuso de privilegios	1
SW07	SERVICIO DE DNS	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	1
		Caída del servicio	3
		Saturación del Servicio	2
		Ataque de hackers a las vulnerabilidades de las aplicaciones	1
		Acceso no autorizado a la red	1
		Mal Funcionamiento del Sistema	1
		Penetración y propagación de virus en la intranet por mal uso de internet / o memorias extraíbles	1
		Abuso de privilegios	1
SW08	SISTEMA SIAF	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	4
		Caída del servicio	4
		Saturación del Servicio	4
		Ataque de hackers a las vulnerabilidades de las aplicaciones	1
		Errores de operación de los usuarios	2

		Filtraciones de información y accesos no autorizados al sistema	4
		Robo de Información	1
		Mal Funcionamiento del Sistema	4
		Fácil descifrado de las contraseñas de los usuarios por parte de personas inescrupulosas	4
		Acceso de personas ajenas a la institución quienes podrían robar información	2
		Abuso de privilegios	4
SW09	SISTEMA SIGA	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3
		Caída del servicio	3
		Saturación del Servicio	3
		Ataque de hackers a las vulnerabilidades de las aplicaciones	1
		Errores de operación de los usuarios	4
		Filtraciones de información y accesos no autorizados al sistema	2
		Robo de Información	1
		Mal Funcionamiento del Sistema	3
		Fácil descifrado de las contraseñas de los usuarios por parte de personas inescrupulosas	4
		Acceso de personas ajenas a la institución quienes podrían robar información	4
		Abuso de privilegios	1
SW11	SISTEMA OPERATIVO WINDOWS SERVER 2008 R2	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	1
		Caída del servicio	3
		Saturación del Servicio	2
		Ataque de hackers a las vulnerabilidades de las aplicaciones	1
		Acceso no autorizado a la red	1
		Mal Funcionamiento del Sistema	2
		Infección de software malicioso	1
		Penetración y propagación de virus en la intranet por mal uso de internet / o memorias extraíbles	1
		Abuso de privilegios	1
SW12	ANTIVIRUS	Infección de software malicioso	3
		Penetración y propagación de virus en la intranet por mal uso de internet / o memorias extraíbles	3

		Abuso de privilegios	1
HW03	SERVIDOR DE BASE DE DATOS/MAD/SIGA	Incendios	1
		Falla / Corte de suministro eléctrico	3
		Robo de Equipamiento	1
		Falla de Equipo	1
		Deterioro / Obsolescencia de equipamiento	2
		Manipulación de hardware	2
HW04	SERVIDOR DE DIRECTORIO ACTIVO Y DNS	Incendios	1
		Falla / Corte de suministro eléctrico	3
		Robo de Equipamiento	1
		Falla de Equipo	1
		Deterioro / Obsolescencia de equipamiento	2
		Manipulación de hardware	2
HW05	SERVIDOR SIAF	Incendios	1
		Falla / Corte de suministro eléctrico	3
		Robo de Equipamiento	1
		Falla de Equipo	1
		Deterioro / Obsolescencia de equipamiento	4
		Manipulación de hardware	2
HW06	UPS PARA DATACENTER	Incendios	1
		Fallo UPS principal del Datacenter	1
		Deterioro / Obsolescencia de equipamiento	4
		Manipulación de hardware	1
RED01	CABLEADO ESTRUCTURADO	Interferencia Electromagnética	1
		Deterioro del cableado de red	2
		Acceso no autorizado a la red	2
RED02	FIREWALL	Incendios	1
		Saturación del Servicio	2
		Falla / Corte de suministro eléctrico	3
		Robo de Equipamiento	1
		Ataque de hackers a las vulnerabilidades de las aplicaciones	1
		Falla de Equipo	1
		Deterioro / Obsolescencia de equipamiento	1
		Acceso no autorizado a la red	1
		Manipulación de hardware	2
		Abuso de privilegios	4
RED03	ROUTER ISP	Incendios	1
		Falla / Corte de suministro eléctrico	3

		Robo de Equipamiento	1
		Ataque de hackers a las vulnerabilidades de las aplicaciones	1
		Falla de Equipo	1
		Deterioro /Obsolescencia de equipamiento	1
		Acceso no autorizado a la red	1
		Manipulación de hardware	1
RED04	SERVICIO DE INTERNET	Falla / Corte del servicio de Internet	2
RED05	SWICTH DE ACCESO	Incendios	1
		Saturación del Servicio	1
		Falla / Corte de suministro eléctrico	3
		Robo de Equipamiento	1
		Ataque de hackers a las vulnerabilidades de las aplicaciones	1
		Falla de Equipo	1
		Deterioro / Obsolescencia de equipamiento	4
		Acceso no autorizado a la red	1
		Manipulación de hardware	3
RED05	SWITCH CORE	Incendios	1
		Saturación del Servicio	2
		Falla / Corte de suministro eléctrico	3
		Robo de Equipamiento	1
		Ataque de hackers a las vulnerabilidades de las aplicaciones	1
		Falla de Equipo	3
		Deterioro / Obsolescencia de equipamiento	4
		Acceso no autorizado a la red	1
		Manipulación de hardware	3
PER01	ADMINISTRADOR DE BASE DE DATOS	Renuncia/Ausentismo del personal al centro de labores	1
		Accidentes del personal	1
PER02	ADMINISTRADOR DE REDES Y SERVIDORES	Renuncia/Ausentismo del personal al centro de labores	1
		Accidentes del personal	1
SIT01	AIRE ACONDICIONADO	Incendios	1
		Inundaciones	1
		Falla equipo de aire acondicionado	2
		Falla / Corte de suministro eléctrico	3
		Deterioro / Obsolescencia de equipamiento	2
SIT02	DATACENTER	Incendios	1
		Acceso no autorizado al Datacenter	4

		Inundaciones	1
		Falla / Corte de suministro eléctrico	3
		Deterioro de la infraestructura física	2
SIT03	SISTEMA CONTRA INCENDIOS DEL DATACENTER	Incendios	1
		Inundaciones	1
		Fallo del Sistema Contra Incendios	1
		Deterioro / Obsolescencia de equipamiento	2

Tabla 18: Vinculación de Activos y Amenazas, Valoración de amenazas

La valoración de amenazas nos servirá posteriormente para sacar el nivel de riesgo al que está expuesto un activo de información. Pero antes de ello procederemos con identificar y valorar las vulnerabilidades de cada uno de los activos de información ya identificados.

4.2.4.4. IDENTIFICACIÓN Y VALORACIÓN DE VULNERABILIDADES

Basándonos en la norma NTP-ISO/IEC 27005:2009, tenemos como entradas la lista de amenazas, los activos de información, adicional a ello los controles existentes: Para efectos del presente proyecto no se considera los controles existentes debido a que no existen formalmente, es por tal motivo que antes de elaborar el documento "declaración de aplicabilidad"[24] se realizará una validación; lo que ya se tiene hasta esta etapa son los activos de TI y la lista de amenazas.

La sola presencia de una vulnerabilidad no causa daño por sí misma, dado que es necesario que exista una amenaza presente para explotarla. Una vulnerabilidad que no tiene amenaza puede no requerir de la implementación de un control, pero es recomendable reconocerla y monitorearla para determinar los cambios [4].

A continuación se detallan las vulnerabilidades encontradas en base a entrevistas al personal responsable y a los hallazgos previa inspección visual:

ID	VULNERABILIDAD
V01	Aplicación desactualizada o parchada deficientemente
V02	Ausencia de bitácoras de los sistemas

[24] Declaración de Aplicabilidad: Documento que describe los objetivos de control y los controles que son relevantes y aplicables al Sistema de Gestión de Seguridad de la Información de la Organización.

V03	Ausencia de capacitación en la manipulación de hardware
V04	Ausencia de código fuente
V05	Ausencia de documentación de la implementación y configuración de los servicios que están en producción
V06	Ausencia de equipos de comunicación de respaldo
V07	Ausencia de Grupo Electrógeno
V08	Ausencia de mantenimiento a las instalaciones
V09	Ausencia de mantenimiento periódico a los equipos de comunicaciones
V10	Ausencia de mantenimiento periódico de Servidores
V11	Ausencia de mantenimiento periódico del UPS
V12	Ausencia de mantenimiento y pruebas periódicas al sistema contra incendios del Datacenter
V13	Ausencia de mantenimiento y pruebas periódicas del aire acondicionado del Datacenter
V14	Ausencia de mapeo de red / mapeo de puntos de red
V15	Ausencia de monitoreo de servicios
V16	Ausencia de políticas de confidencialidad de información
V17	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios
V18	Ausencia de políticas y procedimientos para la gestión de respaldos de información (backups)
V19	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW
V20	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software
V21	Ausencia de registros de los ingresos al Datacenter
V22	Ausencia de segregación de funciones
V23	Cables de red sin protección, sin etiquetas y desordenados
V24	Contraseñas de cuentas de usuarios sencillas
V25	Controles de acceso al sistema deficientes
V26	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido
V27	Deficiente control de acceso a la red
V28	Deficiente control de acceso a las instalaciones
V29	Deficiente proceso de copias de seguridad o de respaldo de información (backups)
V30	Falta de políticas para el uso adecuado de aplicativos
V31	Políticas de firewall inadecuadas
V32	Presencia de material inflamable en el ambiente contiguo al Datacenter
V33	Servicio no configurado en alta disponibilidad

V34	Servidores ubicados en el piso
V35	Puertos de Red sin uso y habilitados
V36	Dependencia de un solo proveedor de internet
V37	Dependencia de un solo personal para estas funciones

Tabla 19: Lista de vulnerabilidades identificadas

Luego de identificar e inventariar las vulnerabilidades, estas deben de ser valoradas en relación a la probabilidad que una amenaza explote la vulnerabilidad o debilidad que se identificó para cada activo de información. Es por ello que las siguientes dos tablas muestran primero el criterio de valoración y la relación entre activos de información, amenazas y vulnerabilidades. Luego de ello determinaremos los niveles de riesgo a los que están expuestos los activos de información.

VALOR	VULNERABILIDAD	DESCRIPCIÓN
3	ALTA	Fácil de ser explotar / poca protección
2	MEDIA	Posibilidad de ser explotada
1	BAJA	Difícil de explotar / Existen buenos controles implementados

Tabla 20: Valores que puede tomar la vulnerabilidad

ACTIVO	VULNERABILIDADES	AMENAZAS	FACILIDAD DE EXPLOTACIÓN	
BASE DE DATOS MAD	Ausencia de bitácoras de los sistemas	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2	
	Ausencia de políticas de confidencialidad de información	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2	○
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2	○

	Controles de acceso al sistema deficientes	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2	
	Ausencia de bitácoras de los sistemas	Filtraciones de información y accesos no autorizados al sistema	2	○
	Ausencia de políticas de confidencialidad de información	Filtraciones de información y accesos no autorizados al sistema	3	●
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Filtraciones de información y accesos no autorizados al sistema	3	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Filtraciones de información y accesos no autorizados al sistema	3	●
	Controles de acceso al sistema deficientes	Filtraciones de información y accesos no autorizados al sistema	3	●
	Deficiente proceso de copias de seguridad o de respaldo de información (backups)	Corrupción de Datos	2	
	Ausencia de políticas y procedimientos para la gestión de respaldos de información (backups)	Corrupción de Datos	2	○
	Ausencia de bitácoras de los sistemas	Robo de Información	2	
	Ausencia de políticas de confidencialidad de información	Robo de Información	3	●
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Robo de Información	3	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Robo de Información	3	●
	Controles de acceso al sistema deficientes	Robo de Información	3	●
	Ausencia de bitácoras de los sistemas	Abuso de privilegios	2	○
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Abuso de privilegios	3	●
	Ausencia de políticas de confidencialidad de información	Abuso de privilegios	3	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Abuso de privilegios	3	●
	Controles de acceso al sistema deficientes	Abuso de privilegios	3	●

DBFs SIAF	Ausencia de bitácoras de los sistemas	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	●
	Ausencia de políticas de confidencialidad de información	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2	○
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	●
	Controles de acceso al sistema deficientes	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2	
	Ausencia de bitácoras de los sistemas	Filtraciones de información y accesos no autorizados al sistema	2	○
	Ausencia de políticas de confidencialidad de información	Filtraciones de información y accesos no autorizados al sistema	3	●
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Filtraciones de información y accesos no autorizados al sistema	3	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Filtraciones de información y accesos no autorizados al sistema	3	●
	Controles de acceso al sistema deficientes	Filtraciones de información y accesos no autorizados al sistema	3	●
	Deficiente proceso de copias de seguridad o de respaldo de información (backups)	Corrupción de Datos	2	
	Ausencia de políticas y procedimientos para la gestión de respaldos de información (backups)	Corrupción de Datos	2	○
	Ausencia de bitácoras de los sistemas	Robo de Información	2	
	Ausencia de políticas de confidencialidad de información	Robo de Información	3	●
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Robo de Información	3	●

	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Robo de Información	3	●
	Controles de acceso al sistema deficientes	Robo de Información	3	●
	Ausencia de bitácoras de los sistemas	Abuso de privilegios	2	○
	Ausencia de políticas de confidencialidad de información	Abuso de privilegios	3	●
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Abuso de privilegios	3	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Abuso de privilegios	3	●
	Controles de acceso al sistema deficientes	Abuso de privilegios	3	●
BASE DE DATOS SIGA	Ausencia de bitácoras de los sistemas	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2	
	Ausencia de políticas de confidencialidad de información	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2	○
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2	○
	Controles de acceso al sistema deficientes	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2	
	Ausencia de bitácoras de los sistemas	Filtraciones de información y accesos no autorizados al sistema	2	○
	Ausencia de políticas de confidencialidad de información	Filtraciones de información y accesos no autorizados al sistema	3	●
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Filtraciones de información y accesos no autorizados al sistema	3	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Filtraciones de información y accesos no autorizados al sistema	3	●
	Controles de acceso al sistema deficientes	Filtraciones de información y accesos no autorizados al sistema	3	●

	Deficiente proceso de copias de seguridad o de respaldo de información (backups)	Corrupción de Datos	2	
	Ausencia de políticas y procedimientos para la gestión de respaldos de información (backups)	Corrupción de Datos	2	○
	Ausencia de bitácoras de los sistemas	Robo de Información	2	
	Ausencia de políticas de confidencialidad de información	Robo de Información	3	●
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Robo de Información	3	●
	Ausencia de bitácoras de los sistemas	Abuso de privilegios	2	○
	Ausencia de políticas de confidencialidad de información	Abuso de privilegios	3	●
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Abuso de privilegios	3	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Abuso de privilegios	3	●
	Controles de acceso al sistema deficientes	Abuso de privilegios	3	●
GESTOR DE BASE DE DATOS	Ausencia de bitácoras de los sistemas	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2	
	Ausencia de políticas de confidencialidad de información	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2	○
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2	○
	Controles de acceso al sistema deficientes	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2	
	Servicio no configurado en alta disponibilidad	Caída del servicio	3	●

	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Caída del servicio	3	●
	Ausencia de monitoreo de servicios	Caída del servicio	3	●
	Aplicación desactualizada o parchada deficientemente	Caída del servicio	3	●
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Caída del servicio	3	●
	Ausencia de bitácoras de los sistemas	Ataque de hackers a las vulnerabilidades de las aplicaciones	2	
	Ausencia de monitoreo de servicios	Ataque de hackers a las vulnerabilidades de las aplicaciones	2	○
	Aplicación desactualizada o parchada deficientemente	Ataque de hackers a las vulnerabilidades de las aplicaciones	3	●
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Ataque de hackers a las vulnerabilidades de las aplicaciones	2	○
	Ausencia de bitácoras de los sistemas	Saturación del Servicio	2	
	Servicio no configurado en alta disponibilidad	Saturación del Servicio	3	●
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Saturación del Servicio	3	●
	Ausencia de monitoreo de servicios	Saturación del Servicio	3	●
	Aplicación desactualizada o parchada deficientemente	Saturación del Servicio	2	
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Saturación del Servicio	2	○
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Mal Funcionamiento del Sistema	3	●
	Ausencia de monitoreo de servicios	Mal Funcionamiento del Sistema	2	○

	Aplicación desactualizada o parchada deficientemente	Mal Funcionamiento del Sistema	2	
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Mal Funcionamiento del Sistema	3	●
SISTEMA MAD	Ausencia de bitácoras de los sistemas	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	●
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	●
	Ausencia de bitácoras de los sistemas	Caída del servicio	1	
	Servicio no configurado en alta disponibilidad	Caída del servicio	2	
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Caída del servicio	3	●
	Ausencia de monitoreo de servicios	Caída del servicio	3	●
	Aplicación desactualizada o parchada deficientemente	Caída del servicio	3	●
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Caída del servicio	3	●
	Ausencia de bitácoras de los sistemas	Saturación del Servicio	2	○
	Servicio no configurado en alta disponibilidad	Saturación del Servicio	2	
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Saturación del Servicio	3	●
	Ausencia de monitoreo de servicios	Saturación del Servicio	3	●
	Aplicación desactualizada o parchada deficientemente	Saturación del Servicio	2	○

	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Saturación del Servicio	2	
	Ausencia de bitácoras de los sistemas	Ataque de hackers a las vulnerabilidades de las aplicaciones	2	○
	Aplicación desactualizada o parchada deficientemente	Ataque de hackers a las vulnerabilidades de las aplicaciones	3	●
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Ataque de hackers a las vulnerabilidades de las aplicaciones	2	○
	Falta de políticas para el uso adecuado de aplicativos	Errores de operación de los usuarios	2	
	Ausencia de bitácoras de los sistemas	Filtraciones de información y accesos no autorizados al sistema	2	○
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Filtraciones de información y accesos no autorizados al sistema	3	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Filtraciones de información y accesos no autorizados al sistema	3	●
	Ausencia de bitácoras de los sistemas	Robo de Información	2	
	Ausencia de políticas de confidencialidad de información	Robo de Información	3	●
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Robo de Información	3	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Robo de Información	3	●
	Controles de acceso al sistema deficientes	Robo de Información	3	●
	Ausencia de bitácoras de los sistemas	Mal Funcionamiento del Sistema	2	○
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Mal Funcionamiento del Sistema	3	●
	Ausencia de monitoreo de servicios	Mal Funcionamiento del Sistema	2	○
	Aplicación desactualizada o parchada deficientemente	Mal Funcionamiento del Sistema	2	

	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Mal Funcionamiento del Sistema	3	●
	Ausencia de bitácoras de los sistemas	Fácil descifrado de las contraseñas de los usuarios por parte de personas inescrupulosas	2	
	Contraseñas de cuentas de usuarios sencillas	Fácil descifrado de las contraseñas de los usuarios por parte de personas inescrupulosas	3	●
	Deficiente control de acceso a las instalaciones	Acceso de personas ajenas a la institución quienes podrían robar información	2	
	Ausencia de bitácoras de los sistemas	Abuso de privilegios	2	○
	Ausencia de políticas de confidencialidad de información	Abuso de privilegios	3	●
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Abuso de privilegios	3	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Abuso de privilegios	3	●
	Controles de acceso al sistema deficientes	Abuso de privilegios	3	●
SERVICIO DE DIRECTORIO ACTIVO	Ausencia de bitácoras de los sistemas	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2	
	Ausencia de políticas de confidencialidad de información	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2	○
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2	○
	Controles de acceso al sistema deficientes	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2	
	Ausencia de bitácoras de los sistemas	Caída del servicio	1	
	Servicio no configurado en alta disponibilidad	Caída del servicio	3	●

	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Caída del servicio	3	●
	Ausencia de monitoreo de servicios	Caída del servicio	3	●
	Aplicación desactualizada o parchada deficientemente	Caída del servicio	3	●
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Caída del servicio	3	●
	Ausencia de bitácoras de los sistemas	Saturación del Servicio	2	○
	Servicio no configurado en alta disponibilidad	Saturación del Servicio	3	●
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Saturación del Servicio	3	●
	Ausencia de monitoreo de servicios	Saturación del Servicio	3	●
	Aplicación desactualizada o parchada deficientemente	Saturación del Servicio	2	○
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Saturación del Servicio	2	
	Ausencia de bitácoras de los sistemas	Ataque de hackers a las vulnerabilidades de las aplicaciones	2	○
	Ausencia de monitoreo de servicios	Ataque de hackers a las vulnerabilidades de las aplicaciones	2	
	Aplicación desactualizada o parchada deficientemente	Ataque de hackers a las vulnerabilidades de las aplicaciones	3	●
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Ataque de hackers a las vulnerabilidades de las aplicaciones	2	
	Ausencia de bitácoras de los sistemas	Acceso no autorizado a la red	2	○
	Deficiente control de acceso a la red	Acceso no autorizado a la red	3	●
	Ausencia de monitoreo de servicios	Acceso no autorizado a la red	2	○

	Ausencia de bitácoras de los sistemas	Mal Funcionamiento del Sistema	2	
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Mal Funcionamiento del Sistema	3	●
	Ausencia de monitoreo de servicios	Mal Funcionamiento del Sistema	2	
	Aplicación desactualizada o parchada deficientemente	Mal Funcionamiento del Sistema	2	○
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Mal Funcionamiento del Sistema	3	●
	Ausencia de bitácoras de los sistemas	Penetración y propagación de virus en la intranet por mal uso de internet / o memorias extraíbles	1	◌
	Ausencia de monitoreo de servicios	Penetración y propagación de virus en la intranet por mal uso de internet / o memorias extraíbles	2	
	Ausencia de bitácoras de los sistemas	Abuso de privilegios	2	○
	Ausencia de políticas de confidencialidad de información	Abuso de privilegios	3	●
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Abuso de privilegios	3	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Abuso de privilegios	3	●
	Controles de acceso al sistema deficientes	Abuso de privilegios	3	●
SERVICIO DE DNS	Ausencia de bitácoras de los sistemas	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2	
	Ausencia de políticas de confidencialidad de información	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2	○
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2	○

	Controles de acceso al sistema deficientes	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2	
	Ausencia de bitácoras de los sistemas	Caída del servicio	1	
	Servicio no configurado en alta disponibilidad	Caída del servicio	3	●
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Caída del servicio	3	●
	Ausencia de monitoreo de servicios	Caída del servicio	3	●
	Aplicación desactualizada o parchada deficientemente	Caída del servicio	3	●
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Caída del servicio	3	●
	Ausencia de bitácoras de los sistemas	Saturación del Servicio	2	○
	Servicio no configurado en alta disponibilidad	Saturación del Servicio	3	●
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Saturación del Servicio	3	●
	Ausencia de monitoreo de servicios	Saturación del Servicio	3	●
	Aplicación desactualizada o parchada deficientemente	Saturación del Servicio	2	○
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Saturación del Servicio	2	
	Ausencia de bitácoras de los sistemas	Ataque de hackers a las vulnerabilidades de las aplicaciones	2	○
	Ausencia de monitoreo de servicios	Ataque de hackers a las vulnerabilidades de las aplicaciones	2	
	Aplicación desactualizada o parchada deficientemente	Ataque de hackers a las vulnerabilidades de las aplicaciones	3	●
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Ataque de hackers a las vulnerabilidades de las aplicaciones	2	

	Ausencia de bitácoras de los sistemas	Acceso no autorizado a la red	2	○
	Deficiente control de acceso a la red	Acceso no autorizado a la red	3	●
	Ausencia de monitoreo de servicios	Acceso no autorizado a la red	2	○
	Ausencia de bitácoras de los sistemas	Mal Funcionamiento del Sistema	2	
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Mal Funcionamiento del Sistema	3	●
	Ausencia de monitoreo de servicios	Mal Funcionamiento del Sistema	2	
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Mal Funcionamiento del Sistema	3	●
	Ausencia de bitácoras de los sistemas	Penetración y propagación de virus en la intranet por mal uso de internet / o memorias extraíbles	1	
	Ausencia de monitoreo de servicios	Penetración y propagación de virus en la intranet por mal uso de internet / o memorias extraíbles	2	○
	Ausencia de bitácoras de los sistemas	Abuso de privilegios	2	
	Ausencia de políticas de confidencialidad de información	Abuso de privilegios	3	●
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Abuso de privilegios	3	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Abuso de privilegios	3	●
	Controles de acceso al sistema deficientes	Abuso de privilegios	3	●
SISTEMA SIAF	Ausencia de bitácoras de los sistemas	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	●
	Ausencia de políticas de confidencialidad de información	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2	
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	●

	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	●
	Controles de acceso al sistema deficientes	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2	○
	Ausencia de bitácoras de los sistemas	Caída del servicio	1	
	Servicio no configurado en alta disponibilidad	Caída del servicio	1	
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Caída del servicio	3	●
	Ausencia de monitoreo de servicios	Caída del servicio	3	●
	Aplicación desactualizada o parchada deficientemente	Caída del servicio	3	●
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Caída del servicio	3	●
	Ausencia de bitácoras de los sistemas	Saturación del Servicio	2	
	Servicio no configurado en alta disponibilidad	Saturación del Servicio	1	
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Saturación del Servicio	3	●
	Ausencia de monitoreo de servicios	Saturación del Servicio	3	●
	Aplicación desactualizada o parchada deficientemente	Saturación del Servicio	2	
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Saturación del Servicio	2	○
	Ausencia de bitácoras de los sistemas	Ataque de hackers a las vulnerabilidades de las aplicaciones	2	
	Ausencia de monitoreo de servicios	Ataque de hackers a las vulnerabilidades de las aplicaciones	2	○

	Aplicación desactualizada o parchada deficientemente	Ataque de hackers a las vulnerabilidades de las aplicaciones	3	●
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Ataque de hackers a las vulnerabilidades de las aplicaciones	2	○
	Falta de políticas para el uso adecuado de aplicativos	Errores de operación de los usuarios	2	
	Ausencia de bitácoras de los sistemas	Filtraciones de información y accesos no autorizados al sistema	2	○
	Ausencia de bitácoras de los sistemas	Robo de Información	2	
	Ausencia de bitácoras de los sistemas	Mal Funcionamiento del Sistema	2	○
	Ausencia de código fuente	Mal Funcionamiento del Sistema	3	●
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Mal Funcionamiento del Sistema	3	●
	Ausencia de monitoreo de servicios	Mal Funcionamiento del Sistema	2	
	Aplicación desactualizada o parchada deficientemente	Mal Funcionamiento del Sistema	2	○
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Mal Funcionamiento del Sistema	3	●
	Ausencia de bitácoras de los sistemas	Fácil descifrado de las contraseñas de los usuarios por parte de personas inescrupulosas	2	○
	Contraseñas de cuentas de usuarios sencillas	Fácil descifrado de las contraseñas de los usuarios por parte de personas inescrupulosas	3	●
	Deficiente control de acceso a las instalaciones	Acceso de personas ajenas a la institución quienes podrían robar información	2	○
	Ausencia de bitácoras de los sistemas	Abuso de privilegios	2	
	Ausencia de políticas de confidencialidad de información	Abuso de privilegios	3	●
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Abuso de privilegios	3	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Abuso de privilegios	3	●

	Controles de acceso al sistema deficientes	Abuso de privilegios	3	●
SISTEMA SIGA	Ausencia de bitácoras de los sistemas	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	●
	Ausencia de políticas de confidencialidad de información	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2	
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	●
	Controles de acceso al sistema deficientes	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2	○
	Ausencia de bitácoras de los sistemas	Caída del servicio	1	
	Servicio no configurado en alta disponibilidad	Caída del servicio	3	●
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Caída del servicio	3	●
	Ausencia de monitoreo de servicios	Caída del servicio	3	●
	Aplicación desactualizada o parchada deficientemente	Caída del servicio	3	●
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Caída del servicio	3	●
	Ausencia de bitácoras de los sistemas	Saturación del Servicio	2	
	Servicio no configurado en alta disponibilidad	Saturación del Servicio	3	●
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Saturación del Servicio	3	●
	Ausencia de monitoreo de servicios	Saturación del Servicio	3	●

	Aplicación desactualizada o parchada deficientemente	Saturación del Servicio	2	
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Saturación del Servicio	2	○
	Ausencia de bitácoras de los sistemas	Ataque de hackers a las vulnerabilidades de las aplicaciones	2	
	Ausencia de monitoreo de servicios	Ataque de hackers a las vulnerabilidades de las aplicaciones	2	○
	Falta de políticas para el uso adecuado de aplicativos	Errores de operación de los usuarios	2	
	Ausencia de bitácoras de los sistemas	Filtraciones de información y accesos no autorizados al sistema	2	○
	Ausencia de bitácoras de los sistemas	Robo de Información	2	
	Ausencia de bitácoras de los sistemas	Mal Funcionamiento del Sistema	2	○
	Ausencia de código fuente	Mal Funcionamiento del Sistema	3	●
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Mal Funcionamiento del Sistema	3	●
	Ausencia de monitoreo de servicios	Mal Funcionamiento del Sistema	2	
	Aplicación desactualizada o parchada deficientemente	Mal Funcionamiento del Sistema	2	○
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Mal Funcionamiento del Sistema	3	●
	Ausencia de bitácoras de los sistemas	Fácil descifrado de las contraseñas de los usuarios por parte de personas inescrupulosas	2	○
	Contraseñas de cuentas de usuarios sencillas	Fácil descifrado de las contraseñas de los usuarios por parte de personas inescrupulosas	3	●
	Deficiente control de acceso a las instalaciones	Acceso de personas ajenas a la institución quienes podrían robar información	2	○
	Ausencia de bitácoras de los sistemas	Abuso de privilegios	2	
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Abuso de privilegios	3	●
	Ausencia de políticas de confidencialidad de información	Abuso de privilegios	3	●

	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Abuso de privilegios	3	●
	Controles de acceso al sistema deficientes	Abuso de privilegios	3	●
SISTEMA OPERATIVO WINDOWS SERVER 2008 R2	Ausencia de bitácoras de los sistemas	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2	○
	Ausencia de políticas de confidencialidad de información	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2	
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2	
	Controles de acceso al sistema deficientes	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2	○
	Ausencia de bitácoras de los sistemas	Caída del servicio	1	
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Caída del servicio	3	●
	Ausencia de monitoreo de servicios	Caída del servicio	3	●
	Aplicación desactualizada o parchada deficientemente	Caída del servicio	3	●
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Caída del servicio	3	●
	Ausencia de bitácoras de los sistemas	Saturación del Servicio	2	○
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Saturación del Servicio	3	●
	Ausencia de monitoreo de servicios	Saturación del Servicio	3	●

	Aplicación desactualizada o parchada deficientemente	Saturación del Servicio	2	
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Saturación del Servicio	2	○
	Ausencia de bitácoras de los sistemas	Ataque de hackers a las vulnerabilidades de las aplicaciones	2	
	Ausencia de monitoreo de servicios	Ataque de hackers a las vulnerabilidades de las aplicaciones	2	○
	Ausencia de bitácoras de los sistemas	Acceso no autorizado a la red	2	
	Deficiente control de acceso a la red	Acceso no autorizado a la red	3	●
	Ausencia de monitoreo de servicios	Acceso no autorizado a la red	2	
	Ausencia de bitácoras de los sistemas	Mal Funcionamiento del Sistema	2	○
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Mal Funcionamiento del Sistema	3	●
	Ausencia de monitoreo de servicios	Mal Funcionamiento del Sistema	2	○
	Ausencia de bitácoras de los sistemas	Infección de software malicioso	2	
	Ausencia de bitácoras de los sistemas	Penetración y propagación de virus en la intranet por mal uso de internet / o memorias extraíbles	1	
	Ausencia de monitoreo de servicios	Penetración y propagación de virus en la intranet por mal uso de internet / o memorias extraíbles	2	
	Ausencia de bitácoras de los sistemas	Abuso de privilegios	2	○
	Ausencia de políticas de confidencialidad de información	Abuso de privilegios	3	●
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Abuso de privilegios	3	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Abuso de privilegios	3	●
	Controles de acceso al sistema deficientes	Abuso de privilegios	3	●
ANTIVIRUS	Ausencia de bitácoras de los sistemas	Infección de software malicioso	2	

	Ausencia de monitoreo de servicios	Infección de software malicioso	3	●
	Ausencia de bitácoras de los sistemas	Penetración y propagación de virus en la intranet por mal uso de internet / o memorias extraíbles	1	
	Ausencia de monitoreo de servicios	Penetración y propagación de virus en la intranet por mal uso de internet / o memorias extraíbles	2	○
	Ausencia de bitácoras de los sistemas	Abuso de privilegios	2	
	Ausencia de políticas de confidencialidad de información	Abuso de privilegios	3	●
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Abuso de privilegios	3	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Abuso de privilegios	3	●
	Controles de acceso al sistema deficientes	Abuso de privilegios	3	●
SERVIDOR DE BASE DE DATOS/MAD/SIGA	Presencia de material inflamable en el ambiente contiguo al Datacenter	Incendios	3	●
	Ausencia de mantenimiento y pruebas periódicas al sistema contra incendios del Datacenter	Incendios	3	●
	Ausencia de Grupo Electrógeno	Falla / Corte de suministro eléctrico	3	●
	Deficiente control de acceso a las instalaciones	Robo de Equipamiento	1	
	Ausencia de mantenimiento periódico de Servidores	Falla de Equipo	2	○
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Falla de Equipo	3	●
	Ausencia de mantenimiento periódico de Servidores	Deterioro / Obsolescencia de equipamiento	2	○
	Servidores ubicados en el piso	Deterioro / Obsolescencia de equipamiento	1	
	Ausencia de mantenimiento a las instalaciones	Deterioro / Obsolescencia de equipamiento	1	
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Deterioro / Obsolescencia de equipamiento	3	●
	Ausencia de capacitación en la manipulación de hardware	Manipulación de hardware	2	○

	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Manipulación de hardware	2	
SERVIDOR DE DIRECTORIO ACTIVO Y DNS	Presencia de material inflamable en el ambiente contiguo al Datacenter	Incendios	3	●
	Ausencia de mantenimiento y pruebas periódicas al sistema contra incendios del Datacenter	Incendios	3	●
	Ausencia de Grupo Electrógeno	Falla / Corte de suministro eléctrico	3	●
	Deficiente control de acceso a las instalaciones	Robo de Equipamiento	1	
	Ausencia de mantenimiento periódico de Servidores	Falla de Equipo	2	○
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Falla de Equipo	3	●
	Ausencia de mantenimiento periódico de Servidores	Deterioro / Obsolescencia de equipamiento	2	○
	Servidores ubicados en el piso	Deterioro / Obsolescencia de equipamiento	1	
	Ausencia de mantenimiento a las instalaciones	Deterioro / Obsolescencia de equipamiento	1	
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Deterioro / Obsolescencia de equipamiento	3	●
	Ausencia de capacitación en la manipulación de hardware	Manipulación de hardware	2	○
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Manipulación de hardware	2	
SERVIDOR SIAF	Presencia de material inflamable en el ambiente contiguo al Datacenter	Incendios	3	●
	Ausencia de mantenimiento y pruebas periódicas al sistema contra incendios del Datacenter	Incendios	3	●
	Ausencia de Grupo Electrógeno	Falla / Corte de suministro eléctrico	3	●
	Deficiente control de acceso a las instalaciones	Robo de Equipamiento	1	
	Ausencia de mantenimiento periódico de Servidores	Falla de Equipo	2	○

	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Falla de Equipo	3	●
	Ausencia de mantenimiento periódico de Servidores	Deterioro / Obsolescencia de equipamiento	2	○
	Servidores ubicados en el piso	Deterioro / Obsolescencia de equipamiento	1	
	Ausencia de mantenimiento a las instalaciones	Deterioro / Obsolescencia de equipamiento	1	
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Deterioro / Obsolescencia de equipamiento	3	●
	Ausencia de capacitación en la manipulación de hardware	Manipulación de hardware	2	○
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Manipulación de hardware	2	
UPS PARA DATACENTER	Presencia de material inflamable en el ambiente contiguo al Datacenter	Incendios	3	●
	Ausencia de mantenimiento y pruebas periódicas al sistema contra incendios del Datacenter	Incendios	3	●
	Ausencia de mantenimiento periódico del UPS	Fallo UPS principal del Datacenter	3	●
	Ausencia de mantenimiento periódico del UPS	Deterioro / Obsolescencia de equipamiento	3	●
	Ausencia de mantenimiento a las instalaciones	Deterioro / Obsolescencia de equipamiento	1	
	Ausencia de capacitación en la manipulación de hardware	Manipulación de hardware	2	
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Manipulación de hardware	2	○
CABLEADO ESTRUCTURADO	Cables de red sin protección, sin etiquetas y desordenados	Interferencia Electromagnética	1	
	Ausencia de mantenimiento periódico a los equipos de comunicaciones	Deterioro del cableado de red	2	○
	Cables de red sin protección, sin etiquetas y desordenados	Deterioro del cableado de red	3	●
	Ausencia de mapeo de red / mapeo de puntos de red	Acceso no autorizado a la red	2	○

	Cables de red sin protección, sin etiquetas y desordenados	Acceso no autorizado a la red	2	
	Deficiente control de acceso a la red	Acceso no autorizado a la red	3	●
	Puertos de Red sin uso y habilitados	Acceso no autorizado a la red	3	●
FIREWALL	Presencia de material inflamable en el ambiente contiguo al Datacenter	Incendios	3	●
	Ausencia de mantenimiento y pruebas periódicas al sistema contra incendios del Datacenter	Incendios	3	●
	Ausencia de bitácoras de los sistemas	Saturación del Servicio	2	○
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Saturación del Servicio	3	●
	Ausencia de Grupo Electrógeno	Falla / Corte de suministro eléctrico	3	●
	Ausencia de equipos de comunicación de respaldo	Robo de Equipamiento	1	
	Deficiente control de acceso a las instalaciones	Robo de Equipamiento	1	
	Ausencia de bitácoras de los sistemas	Ataque de hackers a las vulnerabilidades de las aplicaciones	2	
	Políticas de firewall inadecuadas	Ataque de hackers a las vulnerabilidades de las aplicaciones	2	○
	Ausencia de equipos de comunicación de respaldo	Falla de Equipo	3	●
	Ausencia de mantenimiento periódico a los equipos de comunicaciones	Falla de Equipo	2	○
	Servicio no configurado en alta disponibilidad	Falla de Equipo	3	●
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Falla de Equipo	3	●
	Ausencia de equipos de comunicación de respaldo	Deterioro / Obsolescencia de equipamiento	1	
	Ausencia de mantenimiento periódico a los equipos de comunicaciones	Deterioro / Obsolescencia de equipamiento	2	○
	Servicio no configurado en alta disponibilidad	Deterioro / Obsolescencia de equipamiento	3	●

	Ausencia de mantenimiento a las instalaciones	Deterioro / Obsolescencia de equipamiento	1	
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Deterioro / Obsolescencia de equipamiento	3	●
	Ausencia de bitácoras de los sistemas	Acceso no autorizado a la red	2	○
	Deficiente control de acceso a la red	Acceso no autorizado a la red	3	●
	Ausencia de capacitación en la manipulación de hardware	Manipulación de hardware	2	○
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Manipulación de hardware	2	
	Ausencia de bitácoras de los sistemas	Abuso de privilegios	2	○
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Abuso de privilegios	3	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Abuso de privilegios	3	●
	Controles de acceso al sistema deficientes	Abuso de privilegios	3	●
ROUTER ISP	Presencia de material inflamable en el ambiente contiguo al Datacenter	Incendios	3	●
	Ausencia de mantenimiento y pruebas periódicas al sistema contra incendios del Datacenter	Incendios	3	●
	Ausencia de Grupo Electrógeno	Falla / Corte de suministro eléctrico	3	●
	Ausencia de equipos de comunicación de respaldo	Robo de Equipamiento	1	
	Deficiente control de acceso a las instalaciones	Robo de Equipamiento	1	
	Ausencia de bitácoras de los sistemas	Ataque de hackers a las vulnerabilidades de las aplicaciones	2	
	Ausencia de equipos de comunicación de respaldo	Falla de Equipo	3	●
	Ausencia de mantenimiento periódico a los equipos de comunicaciones	Falla de Equipo	2	

	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Falla de Equipo	3	●
	Ausencia de equipos de comunicación de respaldo	Deterioro / Obsolescencia de equipamiento	1	
	Ausencia de mantenimiento periódico a los equipos de comunicaciones	Deterioro / Obsolescencia de equipamiento	2	○
	Ausencia de mantenimiento a las instalaciones	Deterioro / Obsolescencia de equipamiento	1	
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Deterioro / Obsolescencia de equipamiento	3	●
	Ausencia de bitácoras de los sistemas	Acceso no autorizado a la red	2	
	Deficiente control de acceso a la red	Acceso no autorizado a la red	3	●
	Ausencia de capacitación en la manipulación de hardware	Manipulación de hardware	2	
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Manipulación de hardware	2	○
SERVICIO DE INTERNET	Ausencia de Grupo Electrógeno	Falla / Corte del servicio de Internet	3	●
	Dependencia de un solo proveedor de internet	Falla / Corte del servicio de Internet	2	○
SWICTH DE ACCESO	Presencia de material inflamable en el ambiente contiguo al Datacenter	Incendios	3	●
	Ausencia de mantenimiento y pruebas periódicas al sistema contra incendios del Datacenter	Incendios	3	●
	Ausencia de bitácoras de los sistemas	Saturación del Servicio	2	
	Ausencia de Grupo Electrógeno	Falla / Corte de suministro eléctrico	3	●
	Ausencia de equipos de comunicación de respaldo	Robo de Equipamiento	1	
	Deficiente control de acceso a las instalaciones	Robo de Equipamiento	1	
	Ausencia de bitácoras de los sistemas	Ataque de hackers a las vulnerabilidades de las aplicaciones	2	
	Ausencia de equipos de comunicación de respaldo	Falla de Equipo	1	

	Ausencia de mantenimiento periódico a los equipos de comunicaciones	Falla de Equipo	2	
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Falla de Equipo	3	●
	Ausencia de equipos de comunicación de respaldo	Deterioro / Obsolescencia de equipamiento	1	
	Ausencia de mantenimiento periódico a los equipos de comunicaciones	Deterioro / Obsolescencia de equipamiento	2	○
	Ausencia de mantenimiento a las instalaciones	Deterioro / Obsolescencia de equipamiento	1	
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Deterioro / Obsolescencia de equipamiento	3	●
	Ausencia de bitácoras de los sistemas	Acceso no autorizado a la red	2	
	Deficiente control de acceso a la red	Acceso no autorizado a la red	3	●
	Ausencia de capacitación en la manipulación de hardware	Manipulación de hardware	2	
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Manipulación de hardware	2	○
SWITCH CORE	Presencia de material inflamable en el ambiente contiguo al Datacenter	Incendios	3	●
	Ausencia de mantenimiento y pruebas periódicas al sistema contra incendios del Datacenter	Incendios	3	●
	Ausencia de bitácoras de los sistemas	Saturación del Servicio	2	
	Servicio no configurado en alta disponibilidad	Saturación del Servicio	3	●
	Ausencia de Grupo Electrógeno	Falla / Corte de suministro eléctrico	3	●
	Ausencia de equipos de comunicación de respaldo	Robo de Equipamiento	1	
	Deficiente control de acceso a las instalaciones	Robo de Equipamiento	1	
	Ausencia de bitácoras de los sistemas	Ataque de hackers a las vulnerabilidades de las aplicaciones	2	○

	Ausencia de equipos de comunicación de respaldo	Falla de Equipo	3	●
	Ausencia de mantenimiento periódico a los equipos de comunicaciones	Falla de Equipo	3	●
	Servicio no configurado en alta disponibilidad	Falla de Equipo	3	●
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Falla de Equipo	3	●
	Ausencia de equipos de comunicación de respaldo	Deterioro / Obsolescencia de equipamiento	3	●
	Ausencia de mantenimiento periódico a los equipos de comunicaciones	Deterioro / Obsolescencia de equipamiento	3	●
	Ausencia de mantenimiento a las instalaciones	Deterioro / Obsolescencia de equipamiento	1	
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Deterioro / Obsolescencia de equipamiento	3	●
	Ausencia de bitácoras de los sistemas	Acceso no autorizado a la red	2	
	Deficiente control de acceso a la red	Acceso no autorizado a la red	3	●
	Ausencia de capacitación en la manipulación de hardware	Manipulación de hardware	2	
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Manipulación de hardware	2	○
ADMINISTRADOR DE BASE DE DATOS	Ausencia de segregación de funciones	Renuncia/Ausentismo del personal al centro de labores	2	
	Dependencia de un solo personal para estas funciones	Renuncia/Ausentismo del personal al centro de labores	2	○
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Renuncia/Ausentismo del personal al centro de labores	3	●
	Ausencia de segregación de funciones	Accidentes del personal	2	○
	Dependencia de un solo personal para estas funciones	Accidentes del personal	2	
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Accidentes del personal	2	○

ADMINISTRADOR DE REDES Y SERVIDORES	Ausencia de segregación de funciones	Renuncia/Ausentismo del personal al centro de labores	2	
	Dependencia de un solo personal para estas funciones	Renuncia/Ausentismo del personal al centro de labores	2	○
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Renuncia/Ausentismo del personal al centro de labores	3	●
	Ausencia de segregación de funciones	Accidentes del personal	2	○
	Dependencia de un solo personal para estas funciones	Accidentes del personal	2	
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Accidentes del personal	2	○
AIRE ACONDICIONADO	Presencia de material inflamable en el ambiente contiguo al Datacenter	Incendios	3	●
	Ausencia de mantenimiento y pruebas periódicas al sistema contra incendios del Datacenter	Incendios	3	●
	Ausencia de mantenimiento a las instalaciones	Inundaciones	1	
	Ausencia de mantenimiento y pruebas periódicas del aire acondicionado del Datacenter	Falla equipo de aire acondicionado	2	○
	Ausencia de Grupo Electrógeno	Falla / Corte de suministro eléctrico	1	
	Ausencia de mantenimiento y pruebas periódicas del aire acondicionado del Datacenter	Deterioro / Obsolescencia de equipamiento	2	○
	Ausencia de mantenimiento a las instalaciones	Deterioro / Obsolescencia de equipamiento	1	
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Deterioro / Obsolescencia de equipamiento	3	●
DATACENTER	Presencia de material inflamable en el ambiente contiguo al Datacenter	Incendios	3	●
	Ausencia de mantenimiento y pruebas periódicas al sistema contra incendios del Datacenter	Incendios	3	●
	Ausencia de registros de los ingresos al Datacenter	Acceso no autorizado al Datacenter	2	
	Ausencia de mantenimiento a las instalaciones	Inundaciones	1	

	Ausencia de Grupo Electrógeno	Falla / Corte de suministro eléctrico	3	●
	Ausencia de mantenimiento a las instalaciones	Deterioro de la infraestructura física	1	
SISTEMA CONTRA INCENDIOS DEL DATACENTER	Presencia de material inflamable en el ambiente contiguo al Datacenter	Incendios	3	●
	Ausencia de mantenimiento y pruebas periódicas al sistema contra incendios del Datacenter	Incendios	3	●
	Ausencia de mantenimiento a las instalaciones	Inundaciones	1	
	Ausencia de mantenimiento y pruebas periódicas al sistema contra incendios del Datacenter	Fallo del Sistema Contra Incendios	3	●
	Ausencia de mantenimiento y pruebas periódicas al sistema contra incendios del Datacenter	Deterioro / Obsolescencia de equipamiento	3	●
	Ausencia de mantenimiento a las instalaciones	Deterioro / Obsolescencia de equipamiento	1	
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Deterioro / Obsolescencia de equipamiento	3	●

Tabla 21: Valoración de vulnerabilidades

4.2.4.5. VALORACIÓN DEL RIESGO

Todo el proceso realizado para identificar y valorar los activos de información, amenazas y vulnerabilidades permitirán determinar/identificar los niveles de riesgos a los cuales está expuesto cada activo de información, para que posteriormente se realice el proceso de tratamiento de los riesgos que para el presente proyecto no se realizará, ya que será decisión de la institución implementar los salvaguardas necesarios para reducir el riesgo de los activos de información.

Para determinar el nivel de riesgo de los activos de información nos basaremos en la siguiente tabla, teniendo muy en cuenta los valores de las amenazas Baja (1), Media (2), Alta (3), Muy Alta (4), los valores adoptadas por las vulnerabilidades Baja (1), Media (2), Alta (3); adicional a ello el impacto determinado por la valoración de cada uno de los activos de información.

TABLA DE VALORACIÓN DEL RIESGO													
AMENAZA		BAJA (1)			MEDIA (2)			ALTA (3)			MUY ALTA (4)		
VULNERABILIDAD		B (1)	M (2)	A (3)	B (1)	M (2)	A (3)	B (1)	M (2)	A (3)	B (1)	M (2)	A (3)
IMPACTO	1	1	2	3	2	3	4	3	4	5	4	5	6
	2	2	3	4	3	4	5	4	5	6	5	6	7
	3	3	4	5	4	5	6	5	6	7	6	7	8

Tabla 22: Tabla para determinar los niveles de riesgo de un activo de información

En la tabla siguiente se muestra los resultados del nivel de riesgo por cada Activo de información, relacionando sus amenazas y vulnerabilidades, hay que tener en cuenta en el la identificación y valoración de activos de información ya se realizó un filtro previo donde sólo se consideró de los activos con un valor 3.

ACTIVO	VULNERABILIDADES	AMENAZAS	VAL ACT	VAL AM	VAL VUL	NIVEL RIESGO
BASE DE DATOS MAD	Ausencia de bitácoras de los sistemas	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	1	2	4
	Ausencia de políticas de confidencialidad de información	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	1	2	4
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	1	3	5
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	1	2	4
	Controles de acceso al sistema deficientes	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	1	2	4

	Ausencia de bitácoras de los sistemas	Filtraciones de información y accesos no autorizados al sistema	3	1	2	4
	Ausencia de políticas de confidencialidad de información	Filtraciones de información y accesos no autorizados al sistema	3	1	3	5
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Filtraciones de información y accesos no autorizados al sistema	3	1	3	5
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Filtraciones de información y accesos no autorizados al sistema	3	1	3	5
	Controles de acceso al sistema deficientes	Filtraciones de información y accesos no autorizados al sistema	3	1	3	5
	Deficiente proceso de copias de seguridad o de respaldo de información (backups)	Corrupción de Datos	3	1	2	4
	Ausencia de políticas y procedimientos para la gestión de respaldos de información (backups)	Corrupción de Datos	3	1	2	4
	Ausencia de bitácoras de los sistemas	Robo de Información	3	1	2	4
	Ausencia de políticas de confidencialidad de información	Robo de Información	3	1	3	5
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Robo de Información	3	1	3	5
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Robo de Información	3	1	3	5
	Controles de acceso al sistema deficientes	Robo de Información	3	1	3	5
	Ausencia de bitácoras de los sistemas	Abuso de privilegios	3	2	2	5
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Abuso de privilegios	3	2	3	6

	Ausencia de políticas de confidencialidad de información	Abuso de privilegios	3	2	3	6	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Abuso de privilegios	3	2	3	6	●
	Controles de acceso al sistema deficientes	Abuso de privilegios	3	2	3	6	●
DBFs SIAF	Ausencia de bitácoras de los sistemas	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	1	3	5	
	Ausencia de políticas de confidencialidad de información	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	1	2	4	
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	1	3	5	
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	1	3	5	
	Controles de acceso al sistema deficientes	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	1	2	4	
	Ausencia de bitácoras de los sistemas	Filtraciones de información y accesos no autorizados al sistema	3	2	2	5	
	Ausencia de políticas de confidencialidad de información	Filtraciones de información y accesos no autorizados al sistema	3	2	3	6	●
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Filtraciones de información y accesos no autorizados al sistema	3	2	3	6	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Filtraciones de información y accesos no autorizados al sistema	3	2	3	6	●

	Controles de acceso al sistema deficientes	Filtraciones de información y accesos no autorizados al sistema	3	2	3	6	●
	Deficiente proceso de copias de seguridad o de respaldo de información (backups)	Corrupción de Datos	3	3	2	6	●
	Ausencia de políticas y procedimientos para la gestión de respaldos de información (backups)	Corrupción de Datos	3	3	2	6	●
	Ausencia de bitácoras de los sistemas	Robo de Información	3	1	2	4	
	Ausencia de políticas de confidencialidad de información	Robo de Información	3	1	3	5	
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Robo de Información	3	1	3	5	
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Robo de Información	3	1	3	5	
	Controles de acceso al sistema deficientes	Robo de Información	3	1	3	5	
	Ausencia de bitácoras de los sistemas	Abuso de privilegios	3	2	2	5	
	Ausencia de políticas de confidencialidad de información	Abuso de privilegios	3	2	3	6	●
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Abuso de privilegios	3	2	3	6	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Abuso de privilegios	3	2	3	6	●
	Controles de acceso al sistema deficientes	Abuso de privilegios	3	2	3	6	●
BASE DE DATOS SIGA	Ausencia de bitácoras de los sistemas	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	1	2	4	

	Ausencia de políticas de confidencialidad de información	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	1	2	4
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	1	3	5
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	1	2	4
	Controles de acceso al sistema deficientes	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	1	2	4
	Ausencia de bitácoras de los sistemas	Filtraciones de información y accesos no autorizados al sistema	3	2	2	5
	Ausencia de políticas de confidencialidad de información	Filtraciones de información y accesos no autorizados al sistema	3	2	3	6
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Filtraciones de información y accesos no autorizados al sistema	3	2	3	6
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Filtraciones de información y accesos no autorizados al sistema	3	2	3	6
	Controles de acceso al sistema deficientes	Filtraciones de información y accesos no autorizados al sistema	3	2	3	6
	Deficiente proceso de copias de seguridad o de respaldo de información (backups)	Corrupción de Datos	3	1	2	4
	Ausencia de políticas y procedimientos para la gestión de respaldos de información (backups)	Corrupción de Datos	3	1	2	4
	Ausencia de bitácoras de los sistemas	Robo de Información	3	1	2	4

	Ausencia de políticas de confidencialidad de información	Robo de Información	3	1	3	5	
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Robo de Información	3	1	3	5	
	Ausencia de bitácoras de los sistemas	Abuso de privilegios	3	1	2	4	
	Ausencia de políticas de confidencialidad de información	Abuso de privilegios	3	1	3	5	
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Abuso de privilegios	3	1	3	5	
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Abuso de privilegios	3	1	3	5	
	Controles de acceso al sistema deficientes	Abuso de privilegios	3	1	3	5	
GESTOR DE BASE DE DATOS	Ausencia de bitácoras de los sistemas	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	3	2	6	●
	Ausencia de políticas de confidencialidad de información	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	3	2	6	●
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	3	3	7	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	3	2	6	●
	Controles de acceso al sistema deficientes	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	3	2	6	●
	Servicio no configurado en alta disponibilidad	Caída del servicio	3	4	3	8	●

	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Caída del servicio	3	4	3	8	●
	Ausencia de monitoreo de servicios	Caída del servicio	3	4	3	8	●
	Aplicación desactualizada o parchada deficientemente	Caída del servicio	3	4	3	8	●
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Caída del servicio	3	4	3	8	●
	Ausencia de bitácoras de los sistemas	Ataque de hackers a las vulnerabilidades de las aplicaciones	3	1	2	4	
	Ausencia de monitoreo de servicios	Ataque de hackers a las vulnerabilidades de las aplicaciones	3	1	2	4	
	Aplicación desactualizada o parchada deficientemente	Ataque de hackers a las vulnerabilidades de las aplicaciones	3	1	3	5	
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Ataque de hackers a las vulnerabilidades de las aplicaciones	3	1	2	4	
	Ausencia de bitácoras de los sistemas	Saturación del Servicio	3	2	2	5	
	Servicio no configurado en alta disponibilidad	Saturación del Servicio	3	2	3	6	●
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Saturación del Servicio	3	2	3	6	●
	Ausencia de monitoreo de servicios	Saturación del Servicio	3	2	3	6	●
	Aplicación desactualizada o parchada deficientemente	Saturación del Servicio	3	2	2	5	
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Saturación del Servicio	3	2	2	5	

	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Mal Funcionamiento del Sistema	3	1	3	5	
	Ausencia de monitoreo de servicios	Mal Funcionamiento del Sistema	3	1	2	4	
	Aplicación desactualizada o parchada deficientemente	Mal Funcionamiento del Sistema	3	1	2	4	
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Mal Funcionamiento del Sistema	3	1	3	5	
SISTEMA MAD	Ausencia de bitácoras de los sistemas	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	2	3	6	●
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	2	3	6	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	2	3	6	●
	Ausencia de bitácoras de los sistemas	Caída del servicio	3	4	1	6	●
	Servicio no configurado en alta disponibilidad	Caída del servicio	3	4	2	7	●
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Caída del servicio	3	4	3	8	●
	Ausencia de monitoreo de servicios	Caída del servicio	3	4	3	8	●
	Aplicación desactualizada o parchada deficientemente	Caída del servicio	3	4	3	8	●
	Ausencia de procedimientos estandarizados para actualización de parches	Caída del servicio	3	4	3	8	●

	de seguridad del software						
	Ausencia de bitácoras de los sistemas	Saturación del Servicio	3	3	2	6	●
	Servicio no configurado en alta disponibilidad	Saturación del Servicio	3	3	2	6	●
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Saturación del Servicio	3	3	3	7	●
	Ausencia de monitoreo de servicios	Saturación del Servicio	3	3	3	7	●
	Aplicación desactualizada o parchada deficientemente	Saturación del Servicio	3	3	2	6	●
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Saturación del Servicio	3	3	2	6	●
	Ausencia de bitácoras de los sistemas	Ataque de hackers a las vulnerabilidades de las aplicaciones	3	1	2	4	
	Aplicación desactualizada o parchada deficientemente	Ataque de hackers a las vulnerabilidades de las aplicaciones	3	1	3	5	
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Ataque de hackers a las vulnerabilidades de las aplicaciones	3	1	2	4	
	Falta de políticas para el uso adecuado de aplicativos	Errores de operación de los usuarios	3	3	2	6	●
	Ausencia de bitácoras de los sistemas	Filtraciones de información y accesos no autorizados al sistema	3	3	2	6	●
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Filtraciones de información y accesos no autorizados al sistema	3	3	3	7	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Filtraciones de información y accesos no autorizados al sistema	3	3	3	7	●

	Ausencia de bitácoras de los sistemas	Robo de Información	3	1	2	4
	Ausencia de políticas de confidencialidad de información	Robo de Información	3	1	3	5
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Robo de Información	3	1	3	5
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Robo de Información	3	1	3	5
	Controles de acceso al sistema deficientes	Robo de Información	3	1	3	5
	Ausencia de bitácoras de los sistemas	Mal Funcionamiento del Sistema	3	2	2	5
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Mal Funcionamiento del Sistema	3	2	3	6 ●
	Ausencia de monitoreo de servicios	Mal Funcionamiento del Sistema	3	2	2	5
	Aplicación desactualizada o parchada deficientemente	Mal Funcionamiento del Sistema	3	2	2	5
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Mal Funcionamiento del Sistema	3	2	3	6 ●
	Ausencia de bitácoras de los sistemas	Fácil descifrado de las contraseñas de los usuarios por parte de personas inescrupulosas	3	4	2	7 ●
	Contraseñas de cuentas de usuarios sencillas	Fácil descifrado de las contraseñas de los usuarios por parte de personas inescrupulosas	3	4	3	8 ●
	Deficiente control de acceso a las instalaciones	Acceso de personas ajenas a la institución quienes podrían robar información	3	4	2	7 ●
	Ausencia de bitácoras de los sistemas	Abuso de privilegios	3	1	2	4
	Ausencia de políticas de confidencialidad de información	Abuso de privilegios	3	1	3	5

	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Abuso de privilegios	3	1	3	5	
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Abuso de privilegios	3	1	3	5	
	Controles de acceso al sistema deficientes	Abuso de privilegios	3	1	3	5	
SERVICIO DE DIRECTORIO ACTIVO	Ausencia de bitácoras de los sistemas	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	1	2	4	
	Ausencia de políticas de confidencialidad de información	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	1	2	4	
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	1	3	5	
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	1	2	4	
	Controles de acceso al sistema deficientes	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	1	2	4	
	Ausencia de bitácoras de los sistemas	Caída del servicio	3	3	1	5	
	Servicio no configurado en alta disponibilidad	Caída del servicio	3	3	3	7	●
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Caída del servicio	3	3	3	7	●
	Ausencia de monitoreo de servicios	Caída del servicio	3	3	3	7	●
	Aplicación desactualizada o parchada deficientemente	Caída del servicio	3	3	3	7	●

	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Caída del servicio	3	3	3	7
	Ausencia de bitácoras de los sistemas	Saturación del Servicio	3	2	2	5
	Servicio no configurado en alta disponibilidad	Saturación del Servicio	3	2	3	6
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Saturación del Servicio	3	2	3	6
	Ausencia de monitoreo de servicios	Saturación del Servicio	3	2	3	6
	Aplicación desactualizada o parchada deficientemente	Saturación del Servicio	3	2	2	5
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Saturación del Servicio	3	2	2	5
	Ausencia de bitácoras de los sistemas	Ataque de hackers a las vulnerabilidades de las aplicaciones	3	1	2	4
	Ausencia de monitoreo de servicios	Ataque de hackers a las vulnerabilidades de las aplicaciones	3	1	2	4
	Aplicación desactualizada o parchada deficientemente	Ataque de hackers a las vulnerabilidades de las aplicaciones	3	1	3	5
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Ataque de hackers a las vulnerabilidades de las aplicaciones	3	1	2	4
	Ausencia de bitácoras de los sistemas	Acceso no autorizado a la red	3	1	2	4
	Deficiente control de acceso a la red	Acceso no autorizado a la red	3	1	3	5
	Ausencia de monitoreo de servicios	Acceso no autorizado a la red	3	1	2	4
	Ausencia de bitácoras de los sistemas	Mal Funcionamiento del Sistema	3	1	2	4

	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Mal Funcionamiento del Sistema	3	1	3	5
	Ausencia de monitoreo de servicios	Mal Funcionamiento del Sistema	3	1	2	4
	Aplicación desactualizada o parchada deficientemente	Mal Funcionamiento del Sistema	3	1	2	4
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Mal Funcionamiento del Sistema	3	1	3	5
	Ausencia de bitácoras de los sistemas	Penetración y propagación de virus en la intranet por mal uso de internet / o memorias extraíbles	3	1	1	3
	Ausencia de monitoreo de servicios	Penetración y propagación de virus en la intranet por mal uso de internet / o memorias extraíbles	3	1	2	4
	Ausencia de bitácoras de los sistemas	Abuso de privilegios	3	1	2	4
	Ausencia de políticas de confidencialidad de información	Abuso de privilegios	3	1	3	5
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Abuso de privilegios	3	1	3	5
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Abuso de privilegios	3	1	3	5
	Controles de acceso al sistema deficientes	Abuso de privilegios	3	1	3	5
SERVICIO DE DNS	Ausencia de bitácoras de los sistemas	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	1	2	4
	Ausencia de políticas de confidencialidad de información	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	1	2	4

	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	1	3	5	
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	1	2	4	
	Controles de acceso al sistema deficientes	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	1	2	4	
	Ausencia de bitácoras de los sistemas	Caída del servicio	3	3	1	5	
	Servicio no configurado en alta disponibilidad	Caída del servicio	3	3	3	7	●
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Caída del servicio	3	3	3	7	●
	Ausencia de monitoreo de servicios	Caída del servicio	3	3	3	7	●
	Aplicación desactualizada o parchada deficientemente	Caída del servicio	3	3	3	7	●
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Caída del servicio	3	3	3	7	●
	Ausencia de bitácoras de los sistemas	Saturación del Servicio	3	2	2	5	
	Servicio no configurado en alta disponibilidad	Saturación del Servicio	3	2	3	6	●
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Saturación del Servicio	3	2	3	6	●
	Ausencia de monitoreo de servicios	Saturación del Servicio	3	2	3	6	●
	Aplicación desactualizada o parchada deficientemente	Saturación del Servicio	3	2	2	5	

	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Saturación del Servicio	3	2	2	5
	Ausencia de bitácoras de los sistemas	Ataque de hackers a las vulnerabilidades de las aplicaciones	3	1	2	4
	Ausencia de monitoreo de servicios	Ataque de hackers a las vulnerabilidades de las aplicaciones	3	1	2	4
	Aplicación desactualizada o parchada deficientemente	Ataque de hackers a las vulnerabilidades de las aplicaciones	3	1	3	5
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Ataque de hackers a las vulnerabilidades de las aplicaciones	3	1	2	4
	Ausencia de bitácoras de los sistemas	Acceso no autorizado a la red		1	2	4
	Deficiente control de acceso a la red	Acceso no autorizado a la red	3	1	3	5
	Ausencia de monitoreo de servicios	Acceso no autorizado a la red	3	1	2	4
	Ausencia de bitácoras de los sistemas	Mal Funcionamiento del Sistema	3	1	2	4
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Mal Funcionamiento del Sistema	3	1	3	5
	Ausencia de monitoreo de servicios	Mal Funcionamiento del Sistema	3	1	2	4
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Mal Funcionamiento del Sistema	3	1	3	5
	Ausencia de bitácoras de los sistemas	Penetración y propagación de virus en la intranet por mal uso de internet / o memorias extraíbles	3	1	1	3
	Ausencia de monitoreo de servicios	Penetración y propagación de virus en la intranet por mal uso de internet / o memorias extraíbles	3	1	2	4

	Ausencia de bitácoras de los sistemas	Abuso de privilegios	3	1	2	4	
	Ausencia de políticas de confidencialidad de información	Abuso de privilegios	3	1	3	5	
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Abuso de privilegios	3	1	3	5	
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Abuso de privilegios	3	1	3	5	
	Controles de acceso al sistema deficientes	Abuso de privilegios	3	1	3	5	
SISTEMA SIAF	Ausencia de bitácoras de los sistemas	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	4	3	8	●
	Ausencia de políticas de confidencialidad de información	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	4	2	7	●
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	4	3	8	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	4	3	8	●
	Controles de acceso al sistema deficientes	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	4	2	7	●
	Ausencia de bitácoras de los sistemas	Caída del servicio	3	4	1	6	●
	Servicio no configurado en alta disponibilidad	Caída del servicio	3	4	1	6	●
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Caída del servicio	3	4	3	8	●

	Ausencia de monitoreo de servicios	Caída del servicio	3	4	3	8	●
	Aplicación desactualizada o parchada deficientemente	Caída del servicio	3	4	3	8	●
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Caída del servicio	3	4	3	8	●
	Ausencia de bitácoras de los sistemas	Saturación del Servicio	3	4	2	7	●
	Servicio no configurado en alta disponibilidad	Saturación del Servicio	3	4	1	6	●
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Saturación del Servicio	3	4	3	8	●
	Ausencia de monitoreo de servicios	Saturación del Servicio	3	4	3	8	●
	Aplicación desactualizada o parchada deficientemente	Saturación del Servicio	3	4	2	7	●
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Saturación del Servicio	3	4	2	7	●
	Ausencia de bitácoras de los sistemas	Ataque de hackers a las vulnerabilidades de las aplicaciones	3	1	2	4	
	Ausencia de monitoreo de servicios	Ataque de hackers a las vulnerabilidades de las aplicaciones	3	1	2	4	
	Aplicación desactualizada o parchada deficientemente	Ataque de hackers a las vulnerabilidades de las aplicaciones	3	1	3	5	
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Ataque de hackers a las vulnerabilidades de las aplicaciones	3	1	2	4	
	Falta de políticas para el uso adecuado de aplicativos	Errores de operación de los usuarios	3	2	2	5	

Ausencia de bitácoras de los sistemas	Filtraciones de información y accesos no autorizados al sistema	3	4	2	7	●
Ausencia de bitácoras de los sistemas	Robo de Información	3	1	2	4	
Ausencia de bitácoras de los sistemas	Mal Funcionamiento del Sistema	3	4	2	7	●
Ausencia de código fuente	Mal Funcionamiento del Sistema	3	4	3	8	●
Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Mal Funcionamiento del Sistema	3	4	3	8	●
Ausencia de monitoreo de servicios	Mal Funcionamiento del Sistema	3	4	2	7	●
Aplicación desactualizada o parchada deficientemente	Mal Funcionamiento del Sistema	3	4	2	7	●
Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Mal Funcionamiento del Sistema	3	4	3	8	●
Ausencia de bitácoras de los sistemas	Fácil descifrado de las contraseñas de los usuarios por parte de personas inescrupulosas	3	4	2	7	●
Contraseñas de cuentas de usuarios sencillas	Fácil descifrado de las contraseñas de los usuarios por parte de personas inescrupulosas	3	4	3	8	●
Deficiente control de acceso a las instalaciones	Acceso de personas ajenas a la institución quienes podrían robar información	3	2	2	5	
Ausencia de bitácoras de los sistemas	Abuso de privilegios	3	4	2	7	●
Ausencia de políticas de confidencialidad de información	Abuso de privilegios	3	4	3	8	●
Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Abuso de privilegios	3	4	3	8	●
Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Abuso de privilegios	3	4	3	8	●

	Controles de acceso al sistema deficientes	Abuso de privilegios	3	4	3	8	●
SISTEMA SIGA	Ausencia de bitácoras de los sistemas	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	3	3	7	●
	Ausencia de políticas de confidencialidad de información	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	3	2	6	●
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	3	3	7	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	3	3	7	●
	Controles de acceso al sistema deficientes	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	3	2	6	●
	Ausencia de bitácoras de los sistemas	Caída del servicio	3	3	1	5	
	Servicio no configurado en alta disponibilidad	Caída del servicio	3	3	3	7	●
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Caída del servicio	3	3	3	7	●
	Ausencia de monitoreo de servicios	Caída del servicio	3	3	3	7	●
	Aplicación desactualizada o parchada deficientemente	Caída del servicio	3	3	3	7	●
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Caída del servicio	3	3	3	7	●
	Ausencia de bitácoras de los sistemas	Saturación del Servicio	3	3	2	6	●

Servicio no configurado en alta disponibilidad	Saturación del Servicio	3	3	3	7	●
Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Saturación del Servicio	3	3	3	7	●
Ausencia de monitoreo de servicios	Saturación del Servicio	3	3	3	7	●
Aplicación desactualizada o parchada deficientemente	Saturación del Servicio	3	3	2	6	●
Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Saturación del Servicio	3	3	2	6	●
Ausencia de bitácoras de los sistemas	Ataque de hackers a las vulnerabilidades de las aplicaciones	3	1	2	4	
Ausencia de monitoreo de servicios	Ataque de hackers a las vulnerabilidades de las aplicaciones	3	1	2	4	
Falta de políticas para el uso adecuado de aplicativos	Errores de operación de los usuarios	3	4	2	7	●
Ausencia de bitácoras de los sistemas	Filtraciones de información y accesos no autorizados al sistema	3	2	2	5	
Ausencia de bitácoras de los sistemas	Robo de Información	3	1	2	4	
Ausencia de bitácoras de los sistemas	Mal Funcionamiento del Sistema	3	3	2	6	●
Ausencia de código fuente	Mal Funcionamiento del Sistema	3	3	3	7	●
Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Mal Funcionamiento del Sistema	3	3	3	7	●
Ausencia de monitoreo de servicios	Mal Funcionamiento del Sistema	3	3	2	6	●
Aplicación desactualizada o parchada deficientemente	Mal Funcionamiento del Sistema	3	3	2	6	●

	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Mal Funcionamiento del Sistema	3	3	3	7	●
	Ausencia de bitácoras de los sistemas	Fácil descifrado de las contraseñas de los usuarios por parte de personas inescrupulosas	3	4	2	7	●
	Contraseñas de cuentas de usuarios sencillas	Fácil descifrado de las contraseñas de los usuarios por parte de personas inescrupulosas	3	4	3	8	●
	Deficiente control de acceso a las instalaciones	Acceso de personas ajenas a la institución quienes podrían robar información	3	4	2	7	●
	Ausencia de bitácoras de los sistemas	Abuso de privilegios	3	1	2	4	
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Abuso de privilegios	3	1	3	5	
	Ausencia de políticas de confidencialidad de información	Abuso de privilegios	3	1	3	5	
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Abuso de privilegios	3	1	3	5	
	Controles de acceso al sistema deficientes	Abuso de privilegios	3	1	3	5	
SISTEMA OPERATIVO WINDOWS SERVER 2008 R2	Ausencia de bitácoras de los sistemas	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	1	2	4	
	Ausencia de políticas de confidencialidad de información	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	1	2	4	
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	1	3	5	

	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	1	2	4	
	Controles de acceso al sistema deficientes	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	1	2	4	
	Ausencia de bitácoras de los sistemas	Caída del servicio	3	3	1	5	
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Caída del servicio	3	3	3	7	●
	Ausencia de monitoreo de servicios	Caída del servicio	3	3	3	7	●
	Aplicación desactualizada o parchada deficientemente	Caída del servicio	3	3	3	7	●
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Caída del servicio	3	3	3	7	●
	Ausencia de bitácoras de los sistemas	Saturación del Servicio	3	2	2	5	
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Saturación del Servicio	3	2	3	6	●
	Ausencia de monitoreo de servicios	Saturación del Servicio		2	3	6	●
	Aplicación desactualizada o parchada deficientemente	Saturación del Servicio	3	2	2	5	
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Saturación del Servicio	3	2	2	5	
	Ausencia de bitácoras de los sistemas	Ataque de hackers a las vulnerabilidades de las aplicaciones	3	1	2	4	

	Ausencia de monitoreo de servicios	Ataque de hackers a las vulnerabilidades de las aplicaciones	3	1	2	4	
	Ausencia de bitácoras de los sistemas	Acceso no autorizado a la red	3	1	2	4	
	Deficiente control de acceso a la red	Acceso no autorizado a la red	3	1	3	5	
	Ausencia de monitoreo de servicios	Acceso no autorizado a la red	3	1	2	4	
	Ausencia de bitácoras de los sistemas	Mal Funcionamiento del Sistema	3	2	2	5	
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Mal Funcionamiento del Sistema	3	2	3	6	●
	Ausencia de monitoreo de servicios	Mal Funcionamiento del Sistema	3	2	2	5	
	Ausencia de bitácoras de los sistemas	Infección de software malicioso	3	1	2	4	
	Ausencia de bitácoras de los sistemas	Penetración y propagación de virus en la intranet por mal uso de internet / o memorias extraíbles	3	1	1	3	○
	Ausencia de monitoreo de servicios	Penetración y propagación de virus en la intranet por mal uso de internet / o memorias extraíbles	3	1	2	4	
	Ausencia de bitácoras de los sistemas	Abuso de privilegios	3	1	2	4	
	Ausencia de políticas de confidencialidad de información	Abuso de privilegios	3	1	3	5	
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Abuso de privilegios	3	1	3	5	
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Abuso de privilegios	3	1	3	5	
	Controles de acceso al sistema deficientes	Abuso de privilegios	3	1	3	5	
ANTIVIRUS	Ausencia de bitácoras de los sistemas	Infección de software malicioso	3	3	2	6	●
	Ausencia de monitoreo de servicios	Infección de software malicioso	3	3	3	7	●

	Ausencia de bitácoras de los sistemas	Penetración y propagación de virus en la intranet por mal uso de internet / o memorias extraíbles	3	3	1	5	
	Ausencia de monitoreo de servicios	Penetración y propagación de virus en la intranet por mal uso de internet / o memorias extraíbles	3	3	2	6	●
	Ausencia de bitácoras de los sistemas	Abuso de privilegios	3	1	2	4	
	Ausencia de políticas de confidencialidad de información	Abuso de privilegios	3	1	3	5	
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Abuso de privilegios	3	1	3	5	
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Abuso de privilegios	3	1	3	5	
	Controles de acceso al sistema deficientes	Abuso de privilegios	3	1	3	5	
SERVIDOR DE BASE DE DATOS/MAD/SIGA	Presencia de material inflamable en el ambiente contiguo al Datacenter	Incendios	3	1	3	5	
	Ausencia de mantenimiento y pruebas periódicas al sistema contra incendios del Datacenter	Incendios	3	1	3	5	
	Ausencia de Grupo Electrógeno	Falla / Corte de suministro eléctrico	3	3	3	7	●
	Deficiente control de acceso a las instalaciones	Robo de Equipamiento	3	1	1	3	
	Ausencia de mantenimiento periódico de Servidores	Falla de Equipo	3	1	2	4	
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Falla de Equipo	3	1	3	5	
	Ausencia de mantenimiento periódico de Servidores	Deterioro / Obsolescencia de equipamiento	3	2	2	5	
	Servidores ubicados en el piso	Deterioro / Obsolescencia de equipamiento	3	2	1	4	

	Ausencia de mantenimiento a las instalaciones	Deterioro / Obsolescencia de equipamiento	3	2	1	4
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Deterioro / Obsolescencia de equipamiento	3	2	3	6 ●
	Ausencia de capacitación en la manipulación de hardware	Manipulación de hardware	3	2	2	5
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Manipulación de hardware	3	2	2	5
SERVIDOR DE DIRECTORIO ACTIVO Y DNS	Presencia de material inflamable en el ambiente contiguo al Datacenter	Incendios	3	1	3	5
	Ausencia de mantenimiento y pruebas periódicas al sistema contra incendios del Datacenter	Incendios	3	1	3	5
	Ausencia de Grupo Electrógeno	Falla / Corte de suministro eléctrico	3	3	3	7 ●
	Deficiente control de acceso a las instalaciones	Robo de Equipamiento	3	1	1	3
	Ausencia de mantenimiento periódico de Servidores	Falla de Equipo	3	1	2	4
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Falla de Equipo	3	1	3	5
	Ausencia de mantenimiento periódico de Servidores	Deterioro / Obsolescencia de equipamiento	3	2	2	5
	Servidores ubicados en el piso	Deterioro / Obsolescencia de equipamiento	3	2	1	4
	Ausencia de mantenimiento a las instalaciones	Deterioro / Obsolescencia de equipamiento	3	2	1	4
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Deterioro / Obsolescencia de equipamiento	3	2	3	6 ●

	Ausencia de capacitación en la manipulación de hardware	Manipulación de hardware	3	2	2	5	
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Manipulación de hardware	3	2	2	5	
SERVIDOR SIAF	Presencia de material inflamable en el ambiente contiguo al Datacenter	Incendios	3	1	3	5	
	Ausencia de mantenimiento y pruebas periódicas al sistema contra incendios del Datacenter	Incendios	3	1	3	5	
	Ausencia de Grupo Electrógeno	Falla / Corte de suministro eléctrico		3	3	7	●
	Deficiente control de acceso a las instalaciones	Robo de Equipamiento	3	1	1	3	
	Ausencia de mantenimiento periódico de Servidores	Falla de Equipo	3	1	2	4	
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Falla de Equipo	3	1	3	5	
	Ausencia de mantenimiento periódico de Servidores	Deterioro / Obsolescencia de equipamiento	3	4	2	7	●
	Servidores ubicados en el piso	Deterioro / Obsolescencia de equipamiento	3	4	1	6	●
	Ausencia de mantenimiento a las instalaciones	Deterioro / Obsolescencia de equipamiento	3	4	1	6	●
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Deterioro / Obsolescencia de equipamiento	3	4	3	8	●
	Ausencia de capacitación en la manipulación de hardware	Manipulación de hardware	3	2	2	5	
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Manipulación de hardware	3	2	2	5	

UPS PARA DATACENTER	Presencia de material inflamable en el ambiente contiguo al Datacenter	Incendios	3	1	3	5	
	Ausencia de mantenimiento y pruebas periódicas al sistema contra incendios del Datacenter	Incendios	3	1	3	5	
	Ausencia de mantenimiento periódico del UPS	Fallo UPS principal del Datacenter	3	1	3	5	
	Ausencia de mantenimiento periódico del UPS	Deterioro / Obsolescencia de equipamiento	3	4	3	8	●
	Ausencia de mantenimiento a las instalaciones	Deterioro / Obsolescencia de equipamiento	3	4	1	6	●
	Ausencia de capacitación en la manipulación de hardware	Manipulación de hardware	3	1	2	4	
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Manipulación de hardware	3	1	2	4	
CABLEADO ESTRUCTURADO	Cables de red sin protección, sin etiquetas y desordenados	Interferencia Electromagnética	3	1	1	3	
	Ausencia de mantenimiento periódico a los equipos de comunicaciones	Deterioro del cableado de red	3	2	2	5	
	Cables de red sin protección, sin etiquetas y desordenados	Deterioro del cableado de red	3	2	3	6	●
	Ausencia de mapeo de red / mapeo de puntos de red	Acceso no autorizado a la red	3	2	2	5	
	Cables de red sin protección, sin etiquetas y desordenados	Acceso no autorizado a la red	3	2	2	5	
	Deficiente control de acceso a la red	Acceso no autorizado a la red	3	2	3	6	●
	Puertos de Red sin uso y habilitados	Acceso no autorizado a la red	3	2	3	6	●
FIREWALL	Presencia de material inflamable en el ambiente contiguo al Datacenter	Incendios	3	1	3	5	

	Ausencia de mantenimiento y pruebas periódicas al sistema contra incendios del Datacenter	Incendios	3	1	3	5	
	Ausencia de bitácoras de los sistemas	Saturación del Servicio	3	2	2	5	
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Saturación del Servicio	3	2	3	6	●
	Ausencia de Grupo Electrógeno	Falla / Corte de suministro eléctrico	3	3	3	7	●
	Ausencia de equipos de comunicación de respaldo	Robo de Equipamiento	3	1	1	3	
	Deficiente control de acceso a las instalaciones	Robo de Equipamiento	3	1	1	3	○
	Ausencia de bitácoras de los sistemas	Ataque de hackers a las vulnerabilidades de las aplicaciones	3	1	2	4	
	Políticas de firewall inadecuadas	Ataque de hackers a las vulnerabilidades de las aplicaciones	3	1	2	4	
	Ausencia de equipos de comunicación de respaldo	Falla de Equipo	3	1	3	5	
	Ausencia de mantenimiento periódico a los equipos de comunicaciones	Falla de Equipo	3	1	2	4	
	Servicio no configurado en alta disponibilidad	Falla de Equipo	3	1	3	5	
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Falla de Equipo	3	1	3	5	
	Ausencia de equipos de comunicación de respaldo	Deterioro / Obsolescencia de equipamiento	3	1	1	3	
	Ausencia de mantenimiento periódico a los equipos de comunicaciones	Deterioro / Obsolescencia de equipamiento	3	1	2	4	
	Servicio no configurado en alta disponibilidad	Deterioro / Obsolescencia de equipamiento	3	1	3	5	
	Ausencia de mantenimiento a las instalaciones	Deterioro / Obsolescencia de equipamiento	3	1	1	3	○

	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Deterioro / Obsolescencia de equipamiento	3	1	3	5	
	Ausencia de bitácoras de los sistemas	Acceso no autorizado a la red	3	1	2	4	
	Deficiente control de acceso a la red	Acceso no autorizado a la red	3	1	3	5	
	Ausencia de capacitación en la manipulación de hardware	Manipulación de hardware	3	2	2	5	
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Manipulación de hardware	3	2	2	5	
	Ausencia de bitácoras de los sistemas	Abuso de privilegios	3	4	2	7	●
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Abuso de privilegios	3	4	3	8	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Abuso de privilegios	3	4	3	8	●
	Controles de acceso al sistema deficientes	Abuso de privilegios	3	4	3	8	●
ROUTER ISP	Presencia de material inflamable en el ambiente contiguo al Datacenter	Incendios	3	1	3	5	
	Ausencia de mantenimiento y pruebas periódicas al sistema contra incendios del Datacenter	Incendios	3	1	3	5	
	Ausencia de Grupo Electrógeno	Falla / Corte de suministro eléctrico	3	3	3	7	●
	Ausencia de equipos de comunicación de respaldo	Robo de Equipamiento	3	1	1	3	
	Deficiente control de acceso a las instalaciones	Robo de Equipamiento	3	1	1	3	○
	Ausencia de bitácoras de los sistemas	Ataque de hackers a las vulnerabilidades de las aplicaciones	3	1	2	4	
	Ausencia de equipos de comunicación de respaldo	Falla de Equipo	3	1	3	5	

	Ausencia de mantenimiento periódico a los equipos de comunicaciones	Falla de Equipo	3	1	2	4
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Falla de Equipo	3	1	3	5
	Ausencia de equipos de comunicación de respaldo	Deterioro / Obsolescencia de equipamiento	3	1	1	3
	Ausencia de mantenimiento periódico a los equipos de comunicaciones	Deterioro / Obsolescencia de equipamiento	3	1	2	4
	Ausencia de mantenimiento a las instalaciones	Deterioro / Obsolescencia de equipamiento	3	1	1	3
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Deterioro / Obsolescencia de equipamiento	3	1	3	5
	Ausencia de bitácoras de los sistemas	Acceso no autorizado a la red	3	1	2	4
	Deficiente control de acceso a la red	Acceso no autorizado a la red	3	1	3	5
	Ausencia de capacitación en la manipulación de hardware	Manipulación de hardware	3	1	2	4
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Manipulación de hardware	3	1	2	4
SERVICIO DE INTERNET	Ausencia de Grupo Electrógeno	Falla / Corte del servicio de Internet	3	2	3	6
	Dependencia de un solo proveedor de internet	Falla / Corte del servicio de Internet	3	2	2	5
SWICTH DE ACCESO	Presencia de material inflamable en el ambiente contiguo al Datacenter	Incendios	3	1	3	5
	Ausencia de mantenimiento y pruebas periódicas al sistema contra incendios del Datacenter	Incendios	3	1	3	5
	Ausencia de bitácoras de los sistemas	Saturación del Servicio	3	1	2	4

	Ausencia de Grupo Electrógeno	Falla / Corte de suministro eléctrico	3	3	3	7	●
	Ausencia de equipos de comunicación de respaldo	Robo de Equipamiento	3	1	1	3	
	Deficiente control de acceso a las instalaciones	Robo de Equipamiento	3	1	1	3	○
	Ausencia de bitácoras de los sistemas	Ataque de hackers a las vulnerabilidades de las aplicaciones	3	1	2	4	
	Ausencia de equipos de comunicación de respaldo	Falla de Equipo	3	1	1	3	○
	Ausencia de mantenimiento periódico a los equipos de comunicaciones	Falla de Equipo	3	1	2	4	
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Falla de Equipo	3	1	3	5	
	Ausencia de equipos de comunicación de respaldo	Deterioro / Obsolescencia de equipamiento	3	4	1	6	●
	Ausencia de mantenimiento periódico a los equipos de comunicaciones	Deterioro / Obsolescencia de equipamiento	3	4	2	7	●
	Ausencia de mantenimiento a las instalaciones	Deterioro / Obsolescencia de equipamiento	3	4	1	6	●
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Deterioro / Obsolescencia de equipamiento	3	4	3	8	●
	Ausencia de bitácoras de los sistemas	Acceso no autorizado a la red	3	1	2	4	
	Deficiente control de acceso a la red	Acceso no autorizado a la red	3	1	3	5	
	Ausencia de capacitación en la manipulación de hardware	Manipulación de hardware	3	3	2	6	●
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Manipulación de hardware	3	3	2	6	●
SWITCH CORE	Presencia de material inflamable en el ambiente contiguo al Datacenter	Incendios	3	1	3	5	

Ausencia de mantenimiento y pruebas periódicas al sistema contra incendios del Datacenter	Incendios	3	1	3	5	
Ausencia de bitácoras de los sistemas	Saturación del Servicio	3	2	2	5	
Servicio no configurado en alta disponibilidad	Saturación del Servicio	3	2	3	6	●
Ausencia de Grupo Electrógeno	Falla / Corte de suministro eléctrico	3	3	3	7	●
Ausencia de equipos de comunicación de respaldo	Robo de Equipamiento	3	1	1	3	○
Deficiente control de acceso a las instalaciones	Robo de Equipamiento	3	1	1	3	
Ausencia de bitácoras de los sistemas	Ataque de hackers a las vulnerabilidades de las aplicaciones	3	1	2	4	
Ausencia de equipos de comunicación de respaldo	Falla de Equipo	3	3	3	7	●
Ausencia de mantenimiento periódico a los equipos de comunicaciones	Falla de Equipo	3	3	3	7	●
Servicio no configurado en alta disponibilidad	Falla de Equipo	3	3	3	7	●
Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Falla de Equipo	3	3	3	7	●
Ausencia de equipos de comunicación de respaldo	Deterioro / Obsolescencia de equipamiento	3	4	3	8	●
Ausencia de mantenimiento periódico a los equipos de comunicaciones	Deterioro / Obsolescencia de equipamiento	3	4	3	8	●
Ausencia de mantenimiento a las instalaciones	Deterioro / Obsolescencia de equipamiento	3	4	1	6	●
Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Deterioro / Obsolescencia de equipamiento	3	4	3	8	●
Ausencia de bitácoras de los sistemas	Acceso no autorizado a la red	3	1	2	4	
Deficiente control de acceso a la red	Acceso no autorizado a la red	3	1	3	5	

	Ausencia de capacitación en la manipulación de hardware	Manipulación de hardware	3	3	2	6	●
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Manipulación de hardware	3	3	2	6	●
ADMINISTRADOR DE BASE DE DATOS	Ausencia de segregación de funciones	Renuncia/Ausentismo del personal al centro de labores	3	1	2	4	
	Dependencia de un solo personal para estas funciones	Renuncia/Ausentismo del personal al centro de labores	3	1	2	4	
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Renuncia/Ausentismo del personal al centro de labores	3	1	3	5	
	Ausencia de segregación de funciones	Accidentes del personal	3	1	2	4	
	Dependencia de un solo personal para estas funciones	Accidentes del personal	3	1	2	4	
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Accidentes del personal	3	1	2	4	
ADMINISTRADOR DE REDES Y SERVIDORES	Ausencia de segregación de funciones	Renuncia/Ausentismo del personal al centro de labores	3	1	2	4	
	Dependencia de un solo personal para estas funciones	Renuncia/Ausentismo del personal al centro de labores	3	1	2	4	
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Renuncia/Ausentismo del personal al centro de labores	3	1	3	5	
	Ausencia de segregación de funciones	Accidentes del personal	3	1	2	4	
	Dependencia de un solo personal para estas funciones	Accidentes del personal	3	1	2	4	

	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Accidentes del personal	3	1	2	4	
AIRE ACONDICIONADO	Presencia de material inflamable en el ambiente contiguo al Datacenter	Incendios	3	1	3	5	
	Ausencia de mantenimiento y pruebas periódicas al sistema contra incendios del Datacenter	Incendios	3	1	3	5	
	Ausencia de mantenimiento a las instalaciones	Inundaciones	3	1	1	3	
	Ausencia de mantenimiento y pruebas periódicas del aire acondicionado del Datacenter	Falla equipo de aire acondicionado	3	2	2	5	
	Ausencia de Grupo Electrógeno	Falla / Corte de suministro eléctrico	3	3	1	5	
	Ausencia de mantenimiento y pruebas periódicas del aire acondicionado del Datacenter	Deterioro / Obsolescencia de equipamiento	3	2	2	5	
	Ausencia de mantenimiento a las instalaciones	Deterioro / Obsolescencia de equipamiento	3	2	1	4	
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Deterioro / Obsolescencia de equipamiento	3	2	3	6	●
DATACENTER	Presencia de material inflamable en el ambiente contiguo al Datacenter	Incendios	3	1	3	5	
	Ausencia de mantenimiento y pruebas periódicas al sistema contra incendios del Datacenter	Incendios	3	1	3	5	
	Ausencia de registros de los ingresos al Datacenter	Acceso no autorizado al Datacenter	3	4	2	7	●
	Ausencia de mantenimiento a las instalaciones	Inundaciones	3	1	1	3	○

	Ausencia de Grupo Electrógeno	Falla / Corte de suministro eléctrico	3	3	3	7 ●
	Ausencia de mantenimiento a las instalaciones	Deterioro de la infraestructura física	3	2	1	4
SISTEMA CONTRA INCENDIOS DEL DATACENTER	Presencia de material inflamable en el ambiente contiguo al Datacenter	Incendios	3	1	3	5
	Ausencia de mantenimiento y pruebas periódicas al sistema contra incendios del Datacenter	Incendios	3	1	3	5
	Ausencia de mantenimiento a las instalaciones	Inundaciones	3	1	1	3
	Ausencia de mantenimiento y pruebas periódicas al sistema contra incendios del Datacenter	Fallo del Sistema Contra Incendios	3	1	3	5
	Ausencia de mantenimiento y pruebas periódicas al sistema contra incendios del Datacenter	Deterioro / Obsolescencia de equipamiento	3	2	3	6 ●
	Ausencia de mantenimiento a las instalaciones	Deterioro / Obsolescencia de equipamiento	3	2	1	4
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Deterioro / Obsolescencia de equipamiento	3	2	3	6 ●

Tabla 23: Valoración de Riesgos de los activos de información – Ref. ISO 27005

Luego de realizar la valoración de riesgos, sólo se tendrán en cuenta los riesgos que tengan la categoría de riesgo al como se muestra en el siguiente cuadro:

NIVEL DE RIESGO	RANGO
Bajo	De 1 a 3
Medio	De 4 a 5
Alto	De 6 a 8

Tabla 24: Leyenda Valoración de Riesgos - Ref. ISO 27005

Continuando con el proceso metodológico del análisis de riesgos vamos a enfocarnos en los riesgos con nivel alto o los que tienen valores 6, 7 y 8; esto permitirá centrarnos en los riesgos más saltantes para cada activo de información.

ACTIVO	VULNERABILIDADES	AMENAZAS	VAL ACT	VAL AM	VAL VUL	NIVEL RIESGO
BASE DE DATOS MAD	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Abuso de privilegios	3	2	3	6 ●
	Ausencia de políticas de confidencialidad de información	Abuso de privilegios	3	2	3	6 ●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Abuso de privilegios	3	2	3	6 ●
	Controles de acceso al sistema deficientes	Abuso de privilegios	3	2	3	6 ●
DBFs SIAF	Ausencia de políticas de confidencialidad de información	Filtraciones de información y accesos no autorizados al sistema	3	2	3	6 ●
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Filtraciones de información y accesos no autorizados al sistema	3	2	3	6 ●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Filtraciones de información y accesos no autorizados al sistema	3	2	3	6 ●
	Controles de acceso al sistema deficientes	Filtraciones de información y accesos no autorizados al sistema	3	2	3	6 ●
	Deficiente proceso de copias de seguridad o de respaldo de información (backups)	Corrupción de Datos	3	3	2	6 ●
	Ausencia de políticas y procedimientos para la gestión de respaldos de información (backups)	Corrupción de Datos	3	3	2	6 ●
	Ausencia de políticas de confidencialidad de información	Abuso de privilegios	3	2	3	6 ●

	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Abuso de privilegios	3	2	3	6	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Abuso de privilegios	3	2	3	6	●
	Controles de acceso al sistema deficientes	Abuso de privilegios	3	2	3	6	●
BASE DE DATOS SIGA	Ausencia de políticas de confidencialidad de información	Filtraciones de información y accesos no autorizados al sistema	3	2	3	6	●
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Filtraciones de información y accesos no autorizados al sistema	3	2	3	6	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Filtraciones de información y accesos no autorizados al sistema	3	2	3	6	●
	Controles de acceso al sistema deficientes	Filtraciones de información y accesos no autorizados al sistema	3	2	3	6	●
GESTOR DE BASE DE DATOS	Ausencia de bitácoras de los sistemas	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	3	2	6	●
	Ausencia de políticas de confidencialidad de información	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	3	2	6	●
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	3	3	7	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	3	2	6	●
	Controles de acceso al sistema deficientes	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	3	2	6	●

	Servicio no configurado en alta disponibilidad	Caída del servicio	3	4	3	8	●
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Caída del servicio	3	4	3	8	●
	Ausencia de monitoreo de servicios	Caída del servicio	3	4	3	8	●
	Aplicación desactualizada o parchada deficientemente	Caída del servicio	3	4	3	8	●
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Caída del servicio	3	4	3	8	●
	Servicio no configurado en alta disponibilidad	Saturación del Servicio	3	2	3	6	●
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Saturación del Servicio	3	2	3	6	●
	Ausencia de monitoreo de servicios	Saturación del Servicio	3	2	3	6	●
SISTEMA MAD	Ausencia de bitácoras de los sistemas	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	2	3	6	●
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	2	3	6	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	2	3	6	●
	Ausencia de bitácoras de los sistemas	Caída del servicio	3	4	1	6	●
	Servicio no configurado en alta disponibilidad	Caída del servicio	3	4	2	7	●

	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Caída del servicio	3	4	3	8	●
	Ausencia de monitoreo de servicios	Caída del servicio	3	4	3	8	●
	Aplicación desactualizada o parchada deficientemente	Caída del servicio	3	4	3	8	●
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Caída del servicio	3	4	3	8	●
	Ausencia de bitácoras de los sistemas	Saturación del Servicio	3	3	2	6	●
	Servicio no configurado en alta disponibilidad	Saturación del Servicio	3	3	2	6	●
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Saturación del Servicio	3	3	3	7	●
	Ausencia de monitoreo de servicios	Saturación del Servicio	3	3	3	7	●
	Aplicación desactualizada o parchada deficientemente	Saturación del Servicio	3	3	2	6	●
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Saturación del Servicio	3	3	2	6	●
	Falta de políticas para el uso adecuado de aplicativos	Errores de operación de los usuarios	3	3	2	6	●
	Ausencia de bitácoras de los sistemas	Filtraciones de información y accesos no autorizados al sistema	3	3	2	6	●
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Filtraciones de información y accesos no autorizados al sistema	3	3	3	7	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Filtraciones de información y accesos no autorizados al sistema	3	3	3	7	●

	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Mal Funcionamiento del Sistema	3	2	3	6	●
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Mal Funcionamiento del Sistema	3	2	3	6	●
	Ausencia de bitácoras de los sistemas	Fácil descifrado de las contraseñas de los usuarios por parte de personas inescrupulosas	3	4	2	7	●
	Contraseñas de cuentas de usuarios sencillas	Fácil descifrado de las contraseñas de los usuarios por parte de personas inescrupulosas	3	4	3	8	●
	Deficiente control de acceso a las instalaciones	Acceso de personas ajenas a la institución quienes podrían robar información	3	4	2	7	●
	Servicio no configurado en alta disponibilidad	Caída del servicio	3	3	3	7	●
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Caída del servicio	3	3	3	7	●
	Ausencia de monitoreo de servicios	Caída del servicio	3	3	3	7	●
SERVICIO DE DIRECTORIO ACTIVO	Aplicación desactualizada o parchada deficientemente	Caída del servicio	3	3	3	7	●
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Caída del servicio	3	3	3	7	●
	Servicio no configurado en alta disponibilidad	Saturación del Servicio	3	2	3	6	●
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Saturación del Servicio	3	2	3	6	●

SERVICIO DE DNS	Ausencia de monitoreo de servicios	Saturación del Servicio	3	2	3	6	●
	Servicio no configurado en alta disponibilidad	Caída del servicio	3	3	3	7	●
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Caída del servicio	3	3	3	7	●
	Ausencia de monitoreo de servicios	Caída del servicio	3	3	3	7	●
	Aplicación desactualizada o parchada deficientemente	Caída del servicio	3	3	3	7	●
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Caída del servicio	3	3	3	7	●
	Servicio no configurado en alta disponibilidad	Saturación del Servicio	3	2	3	6	●
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Saturación del Servicio	3	2	3	6	●
	Ausencia de monitoreo de servicios	Saturación del Servicio	3	2	3	6	●
SISTEMA SIAF	Ausencia de bitácoras de los sistemas	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	4	3	8	●
	Ausencia de políticas de confidencialidad de información	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	4	2	7	●
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	4	3	8	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	4	3	8	●

	Controles de acceso al sistema deficientes	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	4	2	7	●
	Ausencia de bitácoras de los sistemas	Caída del servicio	3	4	1	6	●
	Servicio no configurado en alta disponibilidad	Caída del servicio	3	4	1	6	●
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Caída del servicio	3	4	3	8	●
	Ausencia de monitoreo de servicios	Caída del servicio	3	4	3	8	●
	Aplicación desactualizada o parchada deficientemente	Caída del servicio	3	4	3	8	●
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Caída del servicio	3	4	3	8	●
	Ausencia de bitácoras de los sistemas	Saturación del Servicio	3	4	2	7	●
	Servicio no configurado en alta disponibilidad	Saturación del Servicio	3	4	1	6	●
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Saturación del Servicio	3	4	3	8	●
	Ausencia de monitoreo de servicios	Saturación del Servicio	3	4	3	8	●
	Aplicación desactualizada o parchada deficientemente	Saturación del Servicio	3	4	2	7	●
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Saturación del Servicio	3	4	2	7	●
	Ausencia de bitácoras de los sistemas	Filtraciones de información y accesos no autorizados al sistema	3	4	2	7	●
	Ausencia de bitácoras de los sistemas	Mal Funcionamiento del Sistema	3	4	2	7	●

	Ausencia de código fuente	Mal Funcionamiento del Sistema	3	4	3	8	●
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Mal Funcionamiento del Sistema	3	4	3	8	●
	Ausencia de monitoreo de servicios	Mal Funcionamiento del Sistema	3	4	2	7	●
	Aplicación desactualizada o parchada deficientemente	Mal Funcionamiento del Sistema	3	4	2	7	●
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Mal Funcionamiento del Sistema	3	4	3	8	●
	Ausencia de bitácoras de los sistemas	Fácil descifrado de las contraseñas de los usuarios por parte de personas inescrupulosas	3	4	2	7	●
	Contraseñas de cuentas de usuarios sencillas	Fácil descifrado de las contraseñas de los usuarios por parte de personas inescrupulosas	3	4	3	8	●
	Ausencia de bitácoras de los sistemas	Abuso de privilegios	3	4	2	7	●
	Ausencia de políticas de confidencialidad de información	Abuso de privilegios	3	4	3	8	●
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Abuso de privilegios	3	4	3	8	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Abuso de privilegios	3	4	3	8	●
	Controles de acceso al sistema deficientes	Abuso de privilegios	3	4	3	8	●
SISTEMA SIGA	Ausencia de bitácoras de los sistemas	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	3	3	7	●
	Ausencia de políticas de confidencialidad de información	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de	3	3	2	6	●

		acceso al sistema				
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	3	3	7
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	3	3	7
	Controles de acceso al sistema deficientes	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	3	2	6
	Servicio no configurado en alta disponibilidad	Caída del servicio	3	3	3	7
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Caída del servicio	3	3	3	7
	Ausencia de monitoreo de servicios	Caída del servicio	3	3	3	7
	Aplicación desactualizada o parchada deficientemente	Caída del servicio	3	3	3	7
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Caída del servicio	3	3	3	7
	Ausencia de bitácoras de los sistemas	Saturación del Servicio	3	3	2	6
	Servicio no configurado en alta disponibilidad	Saturación del Servicio	3	3	3	7
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Saturación del Servicio	3	3	3	7
	Ausencia de monitoreo de servicios	Saturación del Servicio	3	3	3	7
	Aplicación desactualizada o parchada deficientemente	Saturación del Servicio	3	3	2	6

	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Saturación del Servicio	3	3	2	6	●
	Falta de políticas para el uso adecuado de aplicativos	Errores de operación de los usuarios	3	4	2	7	●
	Ausencia de bitácoras de los sistemas	Mal Funcionamiento del Sistema	3	3	2	6	●
	Ausencia de código fuente	Mal Funcionamiento del Sistema	3	3	3	7	●
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Mal Funcionamiento del Sistema	3	3	3	7	●
	Ausencia de monitoreo de servicios	Mal Funcionamiento del Sistema	3	3	2	6	●
	Aplicación desactualizada o parchada deficientemente	Mal Funcionamiento del Sistema	3	3	2	6	●
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Mal Funcionamiento del Sistema	3	3	3	7	●
	Ausencia de bitácoras de los sistemas	Fácil descifrado de las contraseñas de los usuarios por parte de personas inescrupulosas	3	4	2	7	●
	Contraseñas de cuentas de usuarios sencillas	Fácil descifrado de las contraseñas de los usuarios por parte de personas inescrupulosas	3	4	3	8	●
	Deficiente control de acceso a las instalaciones	Acceso de personas ajenas a la institución quienes podrían robar información	3	4	2	7	●
SISTEMA OPERATIVO WINDOWS SERVER 2008 R2	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Caída del servicio	3	3	3	7	●
	Ausencia de monitoreo de servicios	Caída del servicio	3	3	3	7	●

	Aplicación desactualizada o parchada deficientemente	Caída del servicio	3	3	3	7
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Caída del servicio	3	3	3	7
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Saturación del Servicio	3	2	3	6
	Ausencia de monitoreo de servicios	Saturación del Servicio		2	3	6
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Mal Funcionamiento del Sistema	3	2	3	6
ANTIVIRUS	Ausencia de bitácoras de los sistemas	Infección de software malicioso	3	3	2	6
	Ausencia de monitoreo de servicios	Infección de software malicioso	3	3	3	7
	Ausencia de monitoreo de servicios	Penetración y propagación de virus en la intranet por mal uso de internet / o memorias extraíbles	3	3	2	6
SERVIDOR DE BASE DE DATOS/MAD/SIGA	Ausencia de Grupo Electrógeno	Falla / Corte de suministro eléctrico	3	3	3	7
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Deterioro / Obsolescencia de equipamiento	3	2	3	6
SERVIDOR DE DIRECTORIO ACTIVO Y DNS	Ausencia de Grupo Electrógeno	Falla / Corte de suministro eléctrico	3	3	3	7
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Deterioro / Obsolescencia de equipamiento	3	2	3	6

SERVIDOR SIAF	Ausencia de Grupo Electrógeno	Falla / Corte de suministro eléctrico		3	3	7	●
	Ausencia de mantenimiento periódico de Servidores	Deterioro / Obsolescencia de equipamiento	3	4	2	7	●
	Servidores ubicados en el piso	Deterioro / Obsolescencia de equipamiento	3	4	1	6	●
	Ausencia de mantenimiento a las instalaciones	Deterioro / Obsolescencia de equipamiento	3	4	1	6	●
UPS PARA DATACENTER	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Deterioro / Obsolescencia de equipamiento	3	4	3	8	●
	Ausencia de mantenimiento periódico del UPS	Deterioro / Obsolescencia de equipamiento	3	4	3	8	●
	Ausencia de mantenimiento a las instalaciones	Deterioro / Obsolescencia de equipamiento	3	4	1	6	●
CABLEADO ESTRUCTURADO	Cables de red sin protección, sin etiquetas y desordenados	Deterioro del cableado de red	3	2	3	6	●
	Deficiente control de acceso a la red	Acceso no autorizado a la red	3	2	3	6	●
	Puertos de Red sin uso y habilitados	Acceso no autorizado a la red	3	2	3	6	●
FIREWALL	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Saturación del Servicio	3	2	3	6	●
	Ausencia de Grupo Electrógeno	Falla / Corte de suministro eléctrico	3	3	3	7	●
	Ausencia de bitácoras de los sistemas	Abuso de privilegios	3	4	2	7	●
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Abuso de privilegios	3	4	3	8	●
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Abuso de privilegios	3	4	3	8	●
	Controles de acceso al sistema deficientes	Abuso de privilegios	3	4	3	8	●
ROUTER ISP	Ausencia de Grupo Electrógeno	Falla / Corte de suministro eléctrico	3	3	3	7	●
SERVICIO DE INTERNET	Ausencia de Grupo Electrógeno	Falla / Corte del servicio de Internet	3	2	3	6	●

	Ausencia de Grupo Electrógeno	Falla / Corte de suministro eléctrico	3	3	3	7	
	Ausencia de equipos de comunicación de respaldo	Deterioro / Obsolescencia de equipamiento	3	4	1	6	
	Ausencia de mantenimiento periódico a los equipos de comunicaciones	Deterioro / Obsolescencia de equipamiento	3	4	2	7	
	Ausencia de mantenimiento a las instalaciones	Deterioro / Obsolescencia de equipamiento	3	4	1	6	
SWICTH DE ACCESO	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Deterioro / Obsolescencia de equipamiento	3	4	3	8	
	Ausencia de capacitación en la manipulación de hardware	Manipulación de hardware	3	3	2	6	
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Manipulación de hardware	3	3	2	6	
	Servicio no configurado en alta disponibilidad	Saturación del Servicio	3	2	3	6	
	Ausencia de Grupo Electrógeno	Falla / Corte de suministro eléctrico	3	3	3	7	
	Ausencia de equipos de comunicación de respaldo	Falla de Equipo	3	3	3	7	
	Ausencia de mantenimiento periódico a los equipos de comunicaciones	Falla de Equipo	3	3	3	7	
	Servicio no configurado en alta disponibilidad	Falla de Equipo	3	3	3	7	
SWITCH CORE	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Falla de Equipo	3	3	3	7	
	Ausencia de equipos de comunicación de respaldo	Deterioro / Obsolescencia de equipamiento	3	4	3	8	
	Ausencia de mantenimiento periódico a los equipos de comunicaciones	Deterioro / Obsolescencia de equipamiento	3	4	3	8	
	Ausencia de mantenimiento a las instalaciones	Deterioro / Obsolescencia de equipamiento	3	4	1	6	

	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Deterioro / Obsolescencia de equipamiento	3	4	3	8	●
	Ausencia de capacitación en la manipulación de hardware	Manipulación de hardware	3	3	2	6	●
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Manipulación de hardware	3	3	2	6	●
AIRE ACONDICIONADO	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Deterioro / Obsolescencia de equipamiento	3	2	3	6	●
DATACENTER	Ausencia de registros de los ingresos al Datacenter	Acceso no autorizado al Datacenter	3	4	2	7	●
	Ausencia de Grupo Electrógeno	Falla / Corte de suministro eléctrico	3	3	3	7	●
SISTEMA CONTRA INCENDIOS DEL DATACENTER	Ausencia de mantenimiento y pruebas periódicas al sistema contra incendios del Datacenter	Deterioro / Obsolescencia de equipamiento	3	2	3	6	●
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Deterioro / Obsolescencia de equipamiento	3	2	3	6	●

Tabla 25: Riesgos Depurados

Hasta este punto de a culminado con la valoración de activos de información, amenazas, vulnerabilidades; para concluir con definir los niveles de riesgos, y priorizar los que tienen un nivel alto.

4.2.4.6. IDENTIFIACIÓN DE CONTROLES ASOCIADOS A LOS RIESGOS IDENTIFICADOS

En apartados anteriores se comentó que la norma hace referencia o contempla 11 dominios, 39 objetivos de control y 133 controles. Los riesgos identificados los relacionamos con estos controles, los cuales deberían ser implementados por el área del Centro de Información y Sistemas del Gobierno

Regional de Cajamarca. En el cuadro siguiente se detalla los controles identificados.

ACTIVO	VULNERABILIDADES	AMENAZAS	RIESGO	CONTROLES IDENTIFICADOS
BASE DE DATOS MAD	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Abuso de privilegios	Robo de información y posible de divulgación	11.2. Gestión de Acceso de Usuarios
	Ausencia de políticas de confidencialidad de información	Abuso de privilegios	Robo de información y posible de divulgación por parte del personal	A.6.1.5. Acuerdos de Confidencialidad
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Abuso de privilegios	Robo de información y po	A.11.1.1. Política de control de Accesos
	Controles de acceso al sistema deficientes	Abuso de privilegios	Robo de información y posible de divulgación	11.2. Gestión de Acceso de Usuarios
DBFs SIAF	Ausencia de políticas de confidencialidad de información	Filtraciones de información y accesos no autorizados al sistema	Robo de información y posible de divulgación por parte del personal	A.6.1.5. Acuerdos de Confidencialidad
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Filtraciones de información y accesos no autorizados al sistema	Robo de información y posible de divulgación	11.2. Gestión de Acceso de Usuarios
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Filtraciones de información y accesos no autorizados al sistema	Robo de información y posible de divulgación por parte del personal	A.11.1.1. Política de control de Accesos
	Controles de acceso al sistema deficientes	Filtraciones de información y accesos no autorizados al sistema	Robo de información y posible de divulgación	11.2. Gestión de Acceso de Usuarios

	Deficiente proceso de copias de seguridad o de respaldo de información (backups)	Corrupción de Datos	Pérdida de información	A.10.5.1. Recuperación de la información
	Ausencia de políticas y procedimientos para la gestión de respaldos de información (backups)	Corrupción de Datos	Pérdida de información	A.10.5.1. Recuperación de la información
	Ausencia de políticas de confidencialidad de información	Abuso de privilegios	Robo de información y posible de divulgación por parte del personal	A.6.1.5. Acuerdos de Confidencialidad
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Abuso de privilegios	Robo de información y posible de divulgación	11.2. Gestión de Acceso de Usuarios
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Abuso de privilegios	Robo de información y posible de divulgación por parte del personal	A.11.1.1. Política de control de Accesos
	Controles de acceso al sistema deficientes	Abuso de privilegios	Robo de información y posible de divulgación	11.2. Gestión de Acceso de Usuarios
BASE DE DATOS SIGA	Ausencia de políticas de confidencialidad de información	Filtraciones de información y accesos no autorizados al sistema	Robo de información y posible de divulgación por parte del personal	A.6.1.5. Acuerdos de Confidencialidad
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Filtraciones de información y accesos no autorizados al sistema	Robo de información y posible de divulgación	11.2. Gestión de Acceso de Usuarios
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Filtraciones de información y accesos no autorizados al sistema	Robo de información y posible de divulgación por parte del personal	A.11.1.1. Política de control de Accesos
	Controles de acceso al sistema deficientes	Filtraciones de información y accesos no autorizados al sistema	Robo de información y posible de divulgación	11.2. Gestión de Acceso de Usuarios

GESTOR DE BASE DE DATOS	Ausencia de bitácoras de los sistemas	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	No tener logs de acceso al sistema	A.10.10.2 Uso del sistema de monitoreo A.11.1.1. Política de control de Accesos
	Ausencia de políticas de confidencialidad de información	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	Robo de información y posible de divulgación por parte del personal	A.6.1.5. Acuerdos de Confidencialidad
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	Robo de información y posible de divulgación	11.2. Gestión de Acceso de Usuarios
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	Robo de información y posible de divulgación por parte del personal	A.11.1.1. Política de control de Accesos
	Controles de acceso al sistema deficientes	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	Robo de información y posible de divulgación	11.2. Gestión de Acceso de Usuarios
	Servicio no configurado en alta disponibilidad	Caída del servicio	Demoras para restaurar el servicio	A.14.1.3. Desarrollando e implementando planes de continuidad que incluyen la seguridad de la información.
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Caída del servicio	Demoras para la solución de problemas de configuración	A.12.4.1. Control del software en producción
	Ausencia de monitoreo de servicios	Caída del servicio	No detectar caída del servicio proactivamente	A.10.3.1. Gestión de la capacidad
	Aplicación desactualizada o parchada deficientemente	Caída del servicio	No disponibilidad de las Bases de Datos	A.12.5.1. Procedimientos de control de cambios

	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Caída del servicio	No disponibilidad del servicio	A.10.3.2. Aceptación del Sistema
	Servicio no configurado en alta disponibilidad	Saturación del Servicio	Demoras en el procesamiento de datos	A.14.1.3. Desarrollando e implementando planes de continuidad que incluyen la seguridad de la información.
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Saturación del Servicio	Demoras para la solución de problemas de configuración	A.12.4.1. Control del software en producción
	Ausencia de monitoreo de servicios	Saturación del Servicio	No detectar caída del servicio proactivamente	A.10.3.1. Gestión de la capacidad
SISTEMA MAD	Ausencia de bitácoras de los sistemas	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	No tener logs de acceso al sistema	A.10.10.2 Uso del sistema de monitoreo A.11.1.1. Política de control de Accesos
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	Robo de información y posible de divulgación	11.2. Gestión de Acceso de Usuarios
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	Robo de información y posible de divulgación por parte del personal	A.11.1.1. Política de control de Accesos
	Ausencia de bitácoras de los sistemas	Caída del servicio	No tener logs y alertas del funcionamiento del sistema	A.10.10.2 Uso del sistema de monitoreo A.10.3.1. Gestión de la capacidad
	Servicio no configurado en alta disponibilidad	Caída del servicio	Demoras para restaurar el servicio	A.14.1.3. Desarrollando e implementando planes de continuidad que incluyen la seguridad de la información.

	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Caída del servicio	Demoras para la solución de problemas de configuración	A.12.4.1. Control del software en producción
	Ausencia de monitoreo de servicios	Caída del servicio	No detectar caída del servicio proactivamente	A.10.3.1. Gestión de la capacidad
	Aplicación desactualizada o parchada deficientemente	Caída del servicio	No disponibilidad del Sistema MAD	A.12.5.1. Procedimientos de control de cambios
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Caída del servicio	No disponibilidad del servicio	A.10.3.2. Aceptación del Sistema
	Ausencia de bitácoras de los sistemas	Saturación del Servicio	No tener logs y alertas del funcionamiento del sistema	A.10.10.2 Uso del sistema de monitoreo A.10.3.1. Gestión de la capacidad
	Servicio no configurado en alta disponibilidad	Saturación del Servicio	Demoras en el procesamiento de datos	A.14.1.3. Desarrollando e implementando planes de continuidad que incluyen la seguridad de la información.
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Saturación del Servicio	Demoras para la solución de problemas de configuración	A.12.4.1. Control del software en producción
	Ausencia de monitoreo de servicios	Saturación del Servicio	No detectar caída del servicio proactivamente	A.10.3.1. Gestión de la capacidad
	Aplicación desactualizada o parchada deficientemente	Saturación del Servicio	Sistema MAD lento	A.12.5.1. Procedimientos de control de cambios
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Saturación del Servicio	Demoras en el procesamiento de datos	A.10.3.2. Aceptación del Sistema
	Falta de políticas para el uso adecuado de aplicativos	Errores de operación de los usuarios	Errores en el ingreso de datos al sistema	A.8.2.2. Concientización, educación y entrenamiento en la seguridad de la información

	Ausencia de bitácoras de los sistemas	Filtraciones de información y accesos no autorizados al sistema	No tener logs de acceso al sistema	A.10.10.2 Uso del sistema de monitoreo A.11.5.1. Procedimientos seguros de conexión
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Filtraciones de información y accesos no autorizados al sistema	Robo de información y posible de divulgación	11.2. Gestión de Acceso de Usuarios
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Filtraciones de información y accesos no autorizados al sistema	Robo de información y posible de divulgación por parte del personal	A.11.1.1. Política de control de Accesos
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Mal Funcionamiento del Sistema	Demoras para la solución de problemas de configuración	A.12.4.1. Control del software en producción
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Mal Funcionamiento del Sistema	Errores de funcionamiento del servicio	A.10.3.2. Aceptación del Sistema
	Ausencia de bitácoras de los sistemas	Fácil descifrado de las contraseñas de los usuarios por parte de personas inescrupulosas	No tener logs de acceso al sistema	A.10.10.2 Uso del sistema de monitoreo A.11.5.3. Sistema de Gestión de contraseñas
	Contraseñas de cuentas de usuarios sencillas	Fácil descifrado de las contraseñas de los usuarios por parte de personas inescrupulosas	Descifrado de contraseñas y acceso a los sistemas para robo de información	A.11.3.1. Uso de contraseñas
	Deficiente control de acceso a las instalaciones	Acceso de personas ajenas a la institución quienes podrían robar información	Robo de información por personas ajenas a la institución	9.1.2. Controles físicos de entradas
SERVICIO DE DIRECTORIO ACTIVO	Servicio no configurado en alta disponibilidad	Caída del servicio	Demoras para restaurar el servicio	A.14.1.3. Desarrollando e implementando planes de continuidad que incluyen la seguridad de la información.
	Ausencia de documentación de la implementación y configuración de los servicios que están en	Caída del servicio	Demoras para la solución de problemas de configuración	A.12.4.1. Control del software en producción

	producción			
	Ausencia de monitoreo de servicios	Caída del servicio	No detectar caída del servicio proactivamente	A.10.3.1. Gestión de la capacidad
	Aplicación desactualizada o parchada deficientemente	Caída del servicio	No disponibilidad de los servicios red	A.12.5.1. Procedimientos de control de cambios
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Caída del servicio	No disponibilidad del servicio	A.10.3.2. Aceptación del Sistema
	Servicio no configurado en alta disponibilidad	Saturación del Servicio	Demoras en el procesamiento de peticiones al servicio de directorio activo	A.14.1.3. Desarrollando e implementando planes de continuidad que incluyen la seguridad de la información.
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Saturación del Servicio	Demoras para la solución de problemas de configuración	A.12.4.1. Control del software en producción
	Ausencia de monitoreo de servicios	Saturación del Servicio	No detectar caída del servicio proactivamente	A.10.3.1. Gestión de la capacidad
SERVICIO DE DNS	Servicio no configurado en alta disponibilidad	Caída del servicio	Demoras para restaurar el servicio	A.14.1.3. Desarrollando e implementando planes de continuidad que incluyen la seguridad de la información.
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Caída del servicio	Demoras para la solución de problemas de configuración	A.12.4.1. Control del software en producción
	Ausencia de monitoreo de servicios	Caída del servicio	No detectar caída del servicio proactivamente	A.10.3.1. Gestión de la capacidad

	Aplicación desactualizada o parchada deficientemente	Caída del servicio	No disponibilidad del servicio DNS y demoras de acceso a los servicios de red e internet	A.12.5.1. Procedimientos de control de cambios
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Caída del servicio	No disponibilidad del servicio	A.10.3.2. Aceptación del Sistema
	Servicio no configurado en alta disponibilidad	Saturación del Servicio	Demoras en los servicios de red e internet	A.14.1.3. Desarrollando e implementando planes de continuidad que incluyen la seguridad de la información.
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Saturación del Servicio	Demoras para la solución de problemas de configuración	A.12.4.1. Control del software en producción
	Ausencia de monitoreo de servicios	Saturación del Servicio	No detectar caída del servicio proactivamente	A.10.3.1. Gestión de la capacidad
SISTEMA SIAF	Ausencia de bitácoras de los sistemas	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	No tener logs de acceso al sistema	A.10.10.2 Uso del sistema de monitoreo A.11.1.1. Política de control de Accesos
	Ausencia de políticas de confidencialidad de información	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	Robo de información y posible de divulgación por parte del personal	A.6.1.5. Acuerdos de Confidencialidad
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	Robo de información y posible de divulgación	11.2. Gestión de Acceso de Usuarios
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	Robo de información y posible de divulgación por parte del personal	A.11.1.1. Política de control de Accesos

	Controles de acceso al sistema deficientes	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	Robo de información y posible de divulgación	11.2. Gestión de Acceso de Usuarios
	Ausencia de bitácoras de los sistemas	Caída del servicio	No tener logs y alertas del funcionamiento del sistema	A.10.10.2 Uso del sistema de monitoreo A.10.3.1. Gestión de la capacidad
	Servicio no configurado en alta disponibilidad	Caída del servicio	Demoras para restaurar el servicio	A.14.1.3. Desarrollando e implementando planes de continuidad que incluyen la seguridad de la información.
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Caída del servicio	Demoras para la solución de problemas de configuración	A.12.4.1. Control del software en producción
	Ausencia de monitoreo de servicios	Caída del servicio	No detectar caída del servicio proactivamente	A.10.3.1. Gestión de la capacidad
	Aplicación desactualizada o parchada deficientemente	Caída del servicio	No disponibilidad del sistema SIAF	A.12.5.1. Procedimientos de control de cambios
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Caída del servicio	No disponibilidad del servicio	A.10.3.2. Aceptación del Sistema
	Ausencia de bitácoras de los sistemas	Saturación del Servicio	No tener logs y alertas del funcionamiento del sistema	A.10.10.2 Uso del sistema de monitoreo A.10.3.1. Gestión de la capacidad
	Servicio no configurado en alta disponibilidad	Saturación del Servicio	Demoras en el procesamiento de datos	A.14.1.3. Desarrollando e implementando planes de continuidad que incluyen la seguridad de la información.
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Saturación del Servicio	Demoras para la solución de problemas de configuración	A.12.4.1. Control del software en producción
	Ausencia de monitoreo de servicios	Saturación del Servicio	No detectar caída del servicio proactivamente	A.10.3.1. Gestión de la capacidad

	Aplicación desactualizada o parchada deficientemente	Saturación del Servicio	Acceso lento al sistema SIAF	A.12.5.1. Procedimientos de control de cambios
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Saturación del Servicio	Demoras en el procesamiento de datos	A.10.3.2. Aceptación del Sistema
	Ausencia de bitácoras de los sistemas	Filtraciones de información y accesos no autorizados al sistema	No tener logs de acceso al sistema	A.10.10.2 Uso del sistema de monitoreo A.11.5.1. Procedimientos seguros de conexión
	Ausencia de bitácoras de los sistemas	Mal Funcionamiento del Sistema	No tener logs y alertas del funcionamiento del sistema	A.10.10.2 Uso del sistema de monitoreo A.10.3.1. Gestión de la capacidad
	Ausencia de código fuente	Mal Funcionamiento del Sistema	Demoras para resolver inconsistencias de funcionamiento del sistema	10.3.2. Aceptación del Sistema
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Mal Funcionamiento del Sistema	Demoras para la solución de problemas de configuración	A.12.4.1. Control del software en producción
	Ausencia de monitoreo de servicios	Mal Funcionamiento del Sistema	No detectar caída del servicio proactivamente	A.10.3.1. Gestión de la capacidad
	Aplicación desactualizada o parchada deficientemente	Mal Funcionamiento del Sistema	Errores funcionales del sistema y demoras en el procesamiento de datos	A.12.5.1. Procedimientos de control de cambios
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Mal Funcionamiento del Sistema	Errores de funcionamiento del servicio	A.10.3.2. Aceptación del Sistema
	Ausencia de bitácoras de los sistemas	Fácil descifrado de las contraseñas de los usuarios por parte de personas inescrupulosas	No tener logs de acceso al sistema	A.10.10.2 Uso del sistema de monitoreo A.11.5.3. Sistema de Gestión de contraseñas

	Contraseñas de cuentas de usuarios sencillas	Fácil descifrado de las contraseñas de los usuarios por parte de personas inescrupulosas	Descifrado de contraseñas y acceso a los sistemas para robo de información	A.11.3.1. Uso de contraseñas
	Ausencia de bitácoras de los sistemas	Abuso de privilegios	No tener logs de acceso al sistema	A.10.10.2 Uso del sistema de monitoreo A.11.2.2. Gestión de Privilegios
	Ausencia de políticas de confidencialidad de información	Abuso de privilegios	Robo de información y posible de divulgación por parte del personal	A.6.1.5. Acuerdos de Confidencialidad
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Abuso de privilegios	Robo de información y posible de divulgación	11.2. Gestión de Acceso de Usuarios
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Abuso de privilegios	Robo de información y posible de divulgación por parte del personal	A.11.1.1. Política de control de Accesos
	Controles de acceso al sistema deficientes	Abuso de privilegios	Robo de información y posible de divulgación	11.2. Gestión de Acceso de Usuarios
SISTEMA SIGA	Ausencia de bitácoras de los sistemas	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	No tener logs de acceso al sistema	A.10.10.2 Uso del sistema de monitoreo A.11.1.1. Política de control de Accesos
	Ausencia de políticas de confidencialidad de información	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	Robo de información y posible de divulgación por parte del personal	A.6.1.5. Acuerdos de Confidencialidad
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	Robo de información y posible de divulgación	11.2. Gestión de Acceso de Usuarios

Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	Robo de información y posible de divulgación por parte del personal	A.11.1.1. Política de control de Accesos
Controles de acceso al sistema deficientes	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	Robo de información y posible de divulgación	11.2. Gestión de Acceso de Usuarios
Servicio no configurado en alta disponibilidad	Caída del servicio	Demoras para restaurar el servicio	A.14.1.3. Desarrollando e implementando planes de continuidad que incluyen la seguridad de la información.
Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Caída del servicio	Demoras para la solución de problemas de configuración	A.12.4.1. Control del software en producción
Ausencia de monitoreo de servicios	Caída del servicio	No detectar caída del servicio proactivamente	A.10.3.1. Gestión de la capacidad
Aplicación desactualizada o parchada deficientemente	Caída del servicio	No disponibilidad del sistema SIGA	A.12.5.1. Procedimientos de control de cambios
Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Caída del servicio	No disponibilidad del servicio	A.10.3.2. Aceptación del Sistema
Ausencia de bitácoras de los sistemas	Saturación del Servicio	No tener logs y alertas del funcionamiento del sistema	A.10.10.2 Uso del sistema de monitoreo A.10.3.1. Gestión de la capacidad
Servicio no configurado en alta disponibilidad	Saturación del Servicio	Demoras en el procesamiento de datos	A.14.1.3. Desarrollando e implementando planes de continuidad que incluyen la seguridad de la información.
Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Saturación del Servicio	Demoras para la solución de problemas de configuración	A.12.4.1. Control del software en producción

	Ausencia de monitoreo de servicios	Saturación del Servicio	No detectar caída del servicio proactivamente	A.10.3.1. Gestión de la capacidad
	Aplicación desactualizada o parchada deficientemente	Saturación del Servicio	Acceso al sistema SIGA lento	A.12.5.1. Procedimientos de control de cambios
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Saturación del Servicio	Demoras en el procesamiento de datos	A.10.3.2. Aceptación del Sistema
	Falta de políticas para el uso adecuado de aplicativos	Errores de operación de los usuarios	Errores en el ingreso de datos al sistema	A.8.2.2. Concientización, educación y entrenamiento en la seguridad de la información
	Ausencia de bitácoras de los sistemas	Mal Funcionamiento del Sistema	No tener logs y alertas del funcionamiento del sistema	A.10.10.2 Uso del sistema de monitoreo A.10.3.1. Gestión de la capacidad
	Ausencia de código fuente	Mal Funcionamiento del Sistema	Demoras para resolver inconsistencias de funcionamiento del sistema	10.3.2. Aceptación del Sistema
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Mal Funcionamiento del Sistema	Demoras para la solución de problemas de configuración	A.12.4.1. Control del software en producción
	Ausencia de monitoreo de servicios	Mal Funcionamiento del Sistema	No detectar caída del servicio proactivamente	A.10.3.1. Gestión de la capacidad
	Aplicación desactualizada o parchada deficientemente	Mal Funcionamiento del Sistema	Errores funcionales del sistema y demoras en el procesamiento de datos	A.12.5.1. Procedimientos de control de cambios
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Mal Funcionamiento del Sistema	Errores de funcionamiento del servicio	A.10.3.2. Aceptación del Sistema

	Ausencia de bitácoras de los sistemas	Fácil descifrado de las contraseñas de los usuarios por parte de personas inescrupulosas	No tener logs de acceso al sistema	A.10.10.2 Uso del sistema de monitoreo A.11.5.3. Sistema de Gestión de contraseñas
	Contraseñas de cuentas de usuarios sencillas	Fácil descifrado de las contraseñas de los usuarios por parte de personas inescrupulosas	Descifrado de contraseñas y acceso a los sistemas para robo de información	A.11.3.1. Uso de contraseñas
	Deficiente control de acceso a las instalaciones	Acceso de personas ajenas a la institución quienes podrían robar información	Robo de información por personas ajenas a la institución	9.1.2. Controles físicos de entradas
SISTEMA OPERATIVO WINDOWS SERVER 2008 R2	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Caída del servicio	Demoras para la solución de problemas de configuración	A.12.4.1. Control del software en producción
	Ausencia de monitoreo de servicios	Caída del servicio	No detectar caída del servicio proactivamente	A.10.3.1. Gestión de la capacidad
	Aplicación desactualizada o parchada deficientemente	Caída del servicio	No disponibilidad del sistema operativo y los servicios instalados	A.12.5.1. Procedimientos de control de cambios
	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	Caída del servicio	No disponibilidad del servicio	A.10.3.2. Aceptación del Sistema
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Saturación del Servicio	Demoras para la solución de problemas de configuración	A.12.4.1. Control del software en producción
	Ausencia de monitoreo de servicios	Saturación del Servicio	No detectar problemas con el servicio proactivamente	A.10.3.1. Gestión de la capacidad
	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Mal Funcionamiento del Sistema	Demoras para la solución de problemas de configuración	A.12.4.1. Control del software en producción

ANTIVIRUS	Ausencia de bitácoras de los sistemas	Infección de software malicioso	No tener logs y alertas del de infección	A.10.10.2 Uso del sistema de monitoreo A.10.4.1. Controles contra software malicioso
	Ausencia de monitoreo de servicios	Infección de software malicioso	Infección de software malicioso en la red	A.10.4.1. Controles contra software malicioso
	Ausencia de monitoreo de servicios	Penetración y propagación de virus en la intranet por mal uso de internet / o memorias extraíbles	Infección de software malicioso en la red	A.10.4.1. Controles contra software malicioso
SERVIDOR DE BASE DE DATOS/MAD/SIGA	Ausencia de Grupo Electrógeno	Falla / Corte de suministro eléctrico	No disponibilidad del servicio de base de datos/servicio MAD y servicio SIGA	A.9.2.2. Suministro eléctrico
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Deterioro / Obsolescencia de equipamiento	Equipo averiado y no disponibilidad de bases de datos / MAD / SIGA	A.9.2.4. Mantenimiento de Equipos
	Ausencia de mantenimiento a las instalaciones	Deterioro / Obsolescencia de equipamiento	Equipo averiado	A.9.1.4. Protección contra amenazas externas y ambientales
	Ausencia de mantenimiento periódico de Servidores	Deterioro / Obsolescencia de equipamiento	Equipo averiado y no disponibilidad de bases de datos / MAD / SIGA	A.9.2.4. Mantenimiento de equipos
SERVIDOR DE DIRECTORIO ACTIVO Y DNS	Ausencia de Grupo Electrógeno	Falla / Corte de suministro eléctrico	No disponibilidad del servicio de directorio activo y acceso a servicios de redes	A.9.2.2. Suministro eléctrico
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Deterioro / Obsolescencia de equipamiento	Equipo averiado y no disponibilidad de servicios de red	A.9.2.4. Mantenimiento de Equipos
	Ausencia de mantenimiento a las instalaciones	Deterioro / Obsolescencia de equipamiento	Equipo averiado	A.9.1.4. Protección contra amenazas externas y ambientales

	Ausencia de mantenimiento periódico de Servidores	Deterioro / Obsolescencia de equipamiento	Equipo averiado y no disponibilidad de servicios de red	A.9.2.4. Mantenimiento de equipos
SERVIDOR SIAF	Ausencia de Grupo Electrógeno	Falla / Corte de suministro eléctrico	No disponiblidad de acceso al sistema SIAF	A.9.2.2. Suministro eléctrico
	Ausencia de mantenimiento periódico de Servidores	Deterioro / Obsolescencia de equipamiento	Equipo averiado y no disponibilidad de acceso al sistema SIAF	A.9.2.4. Mantenimiento de equipos
	Servidores ubicados en el piso	Deterioro / Obsolescencia de equipamiento	Servidores inoperativos	A.9.2.1. Ubicación y protección de equipos
	Ausencia de mantenimiento a las instalaciones	Deterioro / Obsolescencia de equipamiento	Equipo averiado	A.9.1.4. Protección contra amenazas externas y ambientales
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Deterioro / Obsolescencia de equipamiento	Equipo averiado y no disponibilidad de acceso al sistema SIAF	A.9.2.4. Mantenimiento de Equipos
UPS PARA DATACENTER	Ausencia de mantenimiento periódico del UPS	Deterioro / Obsolescencia de equipamiento	Equipo averiado y no disponibilidad de acceso a servicios de red y sistemas	A.9.2.4. Mantenimiento de equipos
	Ausencia de mantenimiento a las instalaciones	Deterioro / Obsolescencia de equipamiento	Equipo averiado	A.9.1.4. Protección contra amenazas externas y ambientales
CABLEADO ESTRUCTURADO	Cables de red sin protección, sin etiquetas y desordenados	Deterioro del cableado de red	Cableado de red deteriorado e inservible	A.9.2.3. Seguridad del cableado
	Deficiente control de acceso a la red	Acceso no autorizado a la red	Acceso a la red por personas inescrupulosas y con la posibilidad de robar información	A.10.6.1. Controles de Red
	Puertos de Red sin uso y habilitados	Acceso no autorizado a la red	Acceso a la red por personas inescrupulosas y con la posibilidad de robar información	A.9.2.3. Seguridad del cableado

FIREWALL	Ausencia de documentación de la implementación y configuración de los servicios que están en producción	Saturación del Servicio	Demoras para la solución de problemas de configuración	A.12.4.1. Control del software en producción
	Ausencia de Grupo Electrógeno	Falla / Corte de suministro eléctrico	No disponibilidad de servicios de redes y sistemas en la sede regional	A.9.2.2. Suministro eléctrico
	Ausencia de bitácoras de los sistemas	Abuso de privilegios	No tener logs de acceso al sistema	A.10.10.2 Uso del sistema de monitoreo A.11.2.2. Gestión de Privilegios
	Cuentas de acceso activas de personas cuyo vínculo laboral con el GRC ha concluido	Abuso de privilegios	Dar accesos remotos para acceso y robo de información	11.2. Gestión de Acceso de Usuarios
	Ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	Abuso de privilegios	Cambios de configuraciones que afecten la seguridad de la red	A.11.1.1. Política de control de Accesos
	Controles de acceso al sistema deficientes	Abuso de privilegios	Cambios de configuraciones que afecten la seguridad de la red	11.2. Gestión de Acceso de Usuarios
ROUTER ISP	Ausencia de Grupo Electrógeno	Falla / Corte de suministro eléctrico	No disponibilidad de servicio de internet en la sede regional	A.9.2.2. Suministro eléctrico
SERVICIO DE INTERNET	Ausencia de Grupo Electrógeno	Falla / Corte de suministro eléctrico	No disponibilidad de servicio de internet en la sede regional	A.9.2.2. Suministro eléctrico
SWICTH DE ACCESO	Ausencia de Grupo Electrógeno	Falla / Corte de suministro eléctrico	No disponibilidad de servicios de redes y sistemas en ciertas ubicaciones	A.9.2.2. Suministro eléctrico

	Ausencia de equipos de comunicación de respaldo	Deterioro / Obsolescencia de equipamiento	Demoras en reemplazo de equipo averiado y problemas para acceder a los servicios de red y sistemas de ciertas áreas del GRC	A.14.1.3. Desarrollando e implementando planes de continuidad que incluyen la seguridad de la información.
	Ausencia de mantenimiento periódico a los equipos de comunicaciones	Deterioro / Obsolescencia de equipamiento	Equipo averiado y no acceso a servicios de red y sistemas de ciertas áreas del GRC	A.9.2.4. Mantenimiento de equipos
	Ausencia de mantenimiento periódico a los equipos de comunicaciones	Falla de Equipo	Equipo averiado y no acceso a servicios de red y sistemas de ciertas áreas del GRC	A.9.2.4. Mantenimiento de equipos
	Ausencia de mantenimiento a las instalaciones	Deterioro / Obsolescencia de equipamiento	Equipo averiado	A.9.1.4. Protección contra amenazas externas y ambientales
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Deterioro / Obsolescencia de equipamiento	Equipo averiado	A.9.2.4. Mantenimiento de Equipos
	Ausencia de capacitación en la manipulación de hardware	Manipulación de hardware	Deterioro / Inoperatividad de del equipo	A.8.2.2. Concientización, educación y entrenamiento en la seguridad de la información
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Manipulación de hardware	Equipo averiado	A.9.2.4. Mantenimiento de Equipos
SWITCH CORE	Servicio no configurado en alta disponibilidad	Saturación del Servicio	Demoras en el acceso a servicios de red	A.14.1.3. Desarrollando e implementando planes de continuidad que incluyen la seguridad de la información.

	Ausencia de Grupo Electrógeno	Falla / Corte de suministro eléctrico	No disponibilidad de servicios de redes y sistemas en la sede regional	A.9.2.2. Suministro eléctrico
	Ausencia de equipos de comunicación de respaldo	Falla de Equipo	Demoras en reemplazo de equipo averiado y problemas para acceder a los servicios de red y sistemas en la sede del GRC	A.14.1.3. Desarrollando e implementando planes de continuidad que incluyen la seguridad de la información.
	Ausencia de mantenimiento periódico a los equipos de comunicaciones	Falla de Equipo	Equipo averiado y no acceso a servicios de red y sistemas en la sede del GRC	A.9.2.4. Mantenimiento de equipos
	Servicio no configurado en alta disponibilidad	Falla de Equipo	Demoras para restaurar los servicios de red de la sede del GRC	A.14.1.3. Desarrollando e implementando planes de continuidad que incluyen la seguridad de la información.
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Falla de Equipo	Equipo averiado	A.9.2.4. Mantenimiento de Equipos
	Ausencia de equipos de comunicación de respaldo	Deterioro / Obsolescencia de equipamiento	Demoras en reemplazo de equipo averiado y problemas para acceder a los servicios de red y sistemas en la sede del GRC	A.14.1.3. Desarrollando e implementando planes de continuidad que incluyen la seguridad de la información.
	Ausencia de mantenimiento periódico a los equipos de comunicaciones	Deterioro / Obsolescencia de equipamiento	Equipo averiado y no acceso a servicios de red y sistemas en la sede del GRC	A.9.2.4. Mantenimiento de equipos
	Ausencia de mantenimiento a las instalaciones	Deterioro / Obsolescencia de equipamiento	Equipo averiado	A.9.1.4. Protección contra amenazas externas y ambientales

	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Deterioro / Obsolescencia de equipamiento	Equipo averiado	A.9.2.4. Mantenimiento de Equipos
	Ausencia de capacitación en la manipulación de hardware	Manipulación de hardware	Deterioro / Inoperatividad de del equipo	A.8.2.2. Concientización, educación y entrenamiento en la seguridad de la información
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Manipulación de hardware	Equipo averiado	A.9.2.4. Mantenimiento de Equipos
AIRE ACONDICIONADO	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Deterioro / Obsolescencia de equipamiento	Equipo averiado	A.9.2.4. Mantenimiento de Equipos
DATACENTER	Ausencia de registros de los ingresos al datacenter	Acceso no autorizado al Datacenter	Manipulación de Hardware y/o manipulación/cambio de cables de red	9.1.2. Controles físicos de entradas
	Ausencia de Grupo Electrógeno	Falla / Corte de suministro eléctrico	No disponibilidad de servicios de redes y sistemas en la sede regional	A.9.2.2. Suministro eléctrico
SISTEMA CONTRA INCENDIOS DEL DATACENTER	Ausencia de mantenimiento y pruebas periódicas al sistema contra incendios del Datacenter	Deterioro / Obsolescencia de equipamiento	Equipo averiado	A.9.2.4. Mantenimiento de equipos
	Ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	Deterioro / Obsolescencia de equipamiento	Equipo averiado	A.9.2.4. Mantenimiento de equipos

Tabla 26: Identificación de Controles ISO 27001 / ISO 17799 asociados a los riesgos

CONCLUSIONES Y RECOMENDACIONES

En este capítulo se presentarán las conclusiones y recomendaciones que permitan llevar a cabo un trabajo adecuado para la implementación de controles y se adapten a la NTP-ISO/IEC 27001:2008

4.3. CONCLUSIONES

- El proyecto contempló la identificación de macro procesos, y dentro de ellos centrarse en el más importante "Gestión de Proyectos de Inversión Pública"
- El proceso metodológico utilizado en el presente proyecto se ha basado en la norma técnica peruana NTP-ISO/IEC 27005:2009, la cual es contemplada por la Oficina Nacional de Gobierno Electrónico e Informática.
- Durante el desarrollo del proyecto se ha identificado los activos de información de TI más importantes relacionados a la "Gestión de Proyectos de Inversión Pública", permitiendo tener un inventario actualizado de activos de TI que dan soporte al proceso. Adicional a ello se ha realizado la valoración de cada uno de ellos teniendo en cuenta características como integridad, confidencialidad y disponibilidad (pilares de la seguridad de la información)
- Se ha obtenido la lista de amenazas y vulnerabilidades; y sus valoraciones para cada activo de información (sólo activos con valoración alta)
- En función a la combinación de activos de TI, amenazas y vulnerabilidades se ha identificado los riesgos de cada activo de TI.
- Finalmente se ha identificado los controles ha implementar por cada riesgo identificado, con el fin de proteger los activos de TI con el fin de asegurar la continuidad del negocio.
- Es evidente que realizar un análisis de riesgos orientado a la Seguridad de la Información es complejo; por tal a mayor alcance de un proyecto como estos conllevará a utilizar más recursos humanos y económicos.
- El presente trabajo sirve de referencia para futuros trabajos, los niveles de riesgos no son estáticos en el tiempo, se necesita revisiones periódicas para

verificar si han sido mitigados o se tiene aún que realizar acciones correctivas para reducir el riesgo (riesgo residual).

4.4. RECOMENDACIONES

- En el presente proyecto se tomó como alcance la sede del Gobierno Regional de Cajamarca, y se recomienda que para próximos trabajos se considere a todas las Direcciones Regionales y dependencias rindentes de la institución.
- La metodología utilizada en este proyecto toma como referencia la norma técnica peruana NTP-ISO/IEC 27005:2009; pero posteriormente los responsables de la implementación del SGSI deberán de definir que metodología que se adapta mejor a sus requerimientos.
- El proceso de análisis de riesgos es constante, el modelo PDCA es un proceso circular que permite la mejora continua, es por ello que se recomienda realizar la revisión y actualización de los riesgos y controles basados en las normas técnicas peruanas basadas en seguridad de la información.
- Para iniciar con la implementación de un SGSI, es necesario concientizar a la alta dirección en la importancia y la exigencia por parte de la ONGEI en la implementación del SGSI en el Gobierno Regional de Cajamarca, haciendo prevalecer los beneficios de contar con un SGSI.
- Es importante conformar un comité de Seguridad de la Información el cual debe de ser multidisciplinario, dentro de este comité se debe de incluir a miembros clave de la alta gerencia (tomadores de decisiones) que apoyen en la implementación de un SGSI.
- Es importante concientizar y capacitar al personal del área de TI del Gobierno Regional de Cajamarca en temas de Seguridad de la Información, y ellos impartir el conocimiento a los colaboradores de la institución para ir creando una cultura organizacional basada en seguridad de la información.

BIBLIOGRAFÍA

[1] Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, «MAGERIT 3.0 - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Guía de Técnicas,» Madrid, 2012.

[2] Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, «MAGERIT 3.0 - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Catálogo de Elementos,» Madrid, 2012.

[3] Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, «MAGERIT 3.0 - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Método,» Madrid, 2012.

[4] Comité Técnico de Normalización de Codificación e Intercambio Electrónico de Datos, «EDI. Tecnología de la información. Técnicas de seguridad. Gestión del riesgo en seguridad de la información NTP-ISO/IEC 27005:2009,» Lima, 2009.

[5] Comité Técnico de Normalización de Codificación e Intercambio Electrónico de Datos, «Técnicas de seguridad. Directrices para la implementación de un sistema de gestión de la seguridad de la información NTP-ISO/IEC 27003:2012,» Lima, 2012.

[6] Comité Técnico de Normalización de Codificación e Intercambio Electrónico de Datos, «EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información NTP-ISO/IEC 17799:2007,» Lima, 2007.

[7] Comité Técnico de Normalización de Codificación e Intercambio Electrónico de Datos, «EDI. Tecnología de la información. Técnicas de seguridad.Sistemas de gestión de seguridad de la información. Requisitos NTP-ISO/IEC 27001:2008,» Lima, 2008.

[8] Information Systems Audit and Control Association, «ISACA,» [En línea]. Available: http://www.isaca.org/COBIT/Documents/COBIT5-Framework-Spanish.pdf. [Último acceso: 20 06 2013].

[9] A. López Neira, «El Portal de ISO 27001 en español,» [En línea]. Available: www.iso27000.es.

[10] INTECO-CERT, «Curso de Sistemas de Gestión de la Seguridad de la Información degún la norma UNE-ISO/IEC 27000,» 06 2010. [En línea]. Available: www.inteco.es. [Último acceso: 2013].

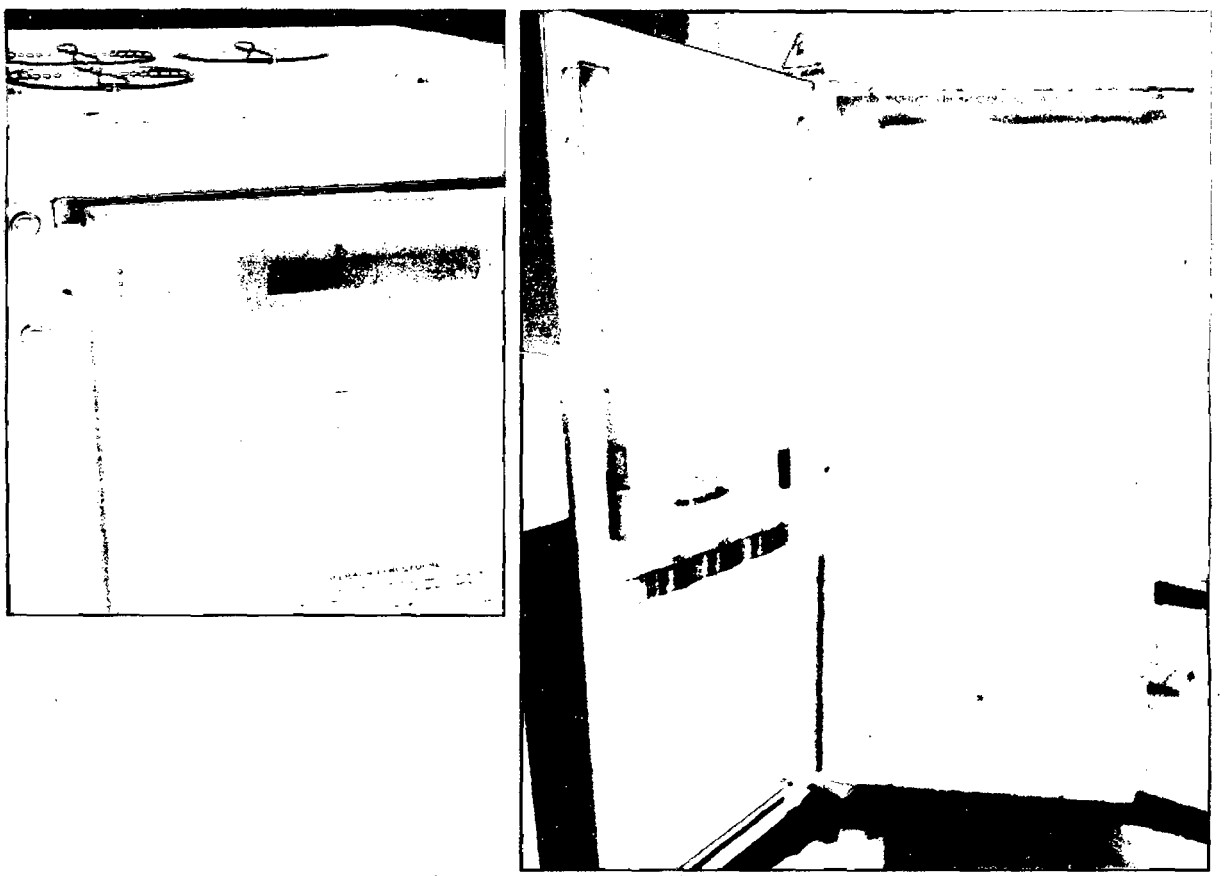
[11] The IT Services Experts, «ITIL-Gestión de Servicios TI,» [En línea]. Available: itil.osiatis.es. [Último acceso: 18 06 2013].

[12] Gobierno Regional de Cajamarca, «Gobierno Regional de Cajamarca,» [En línea]. Available: www.regioncajamarca.gob.pe.

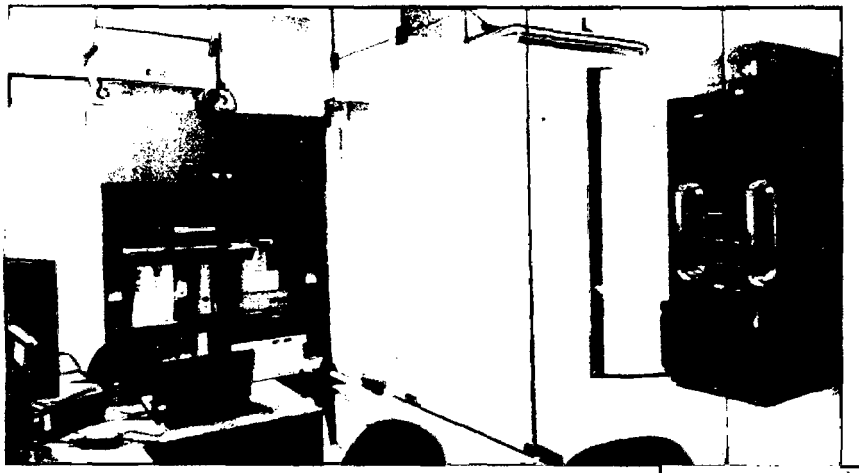
[13] Ministerio de Economía y Finanzas, «Ministerio de Economía y Finanzas,» [En línea]. Available: www.mef.gob.pe.

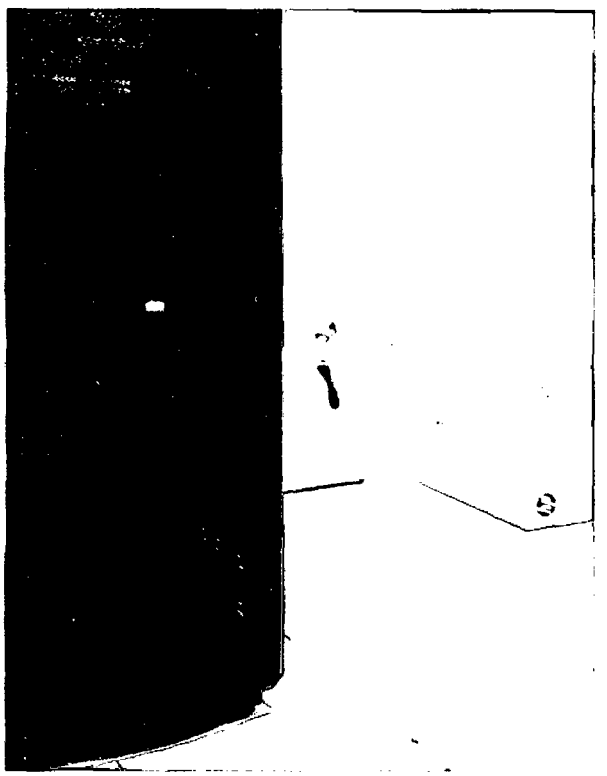
ANEXOS

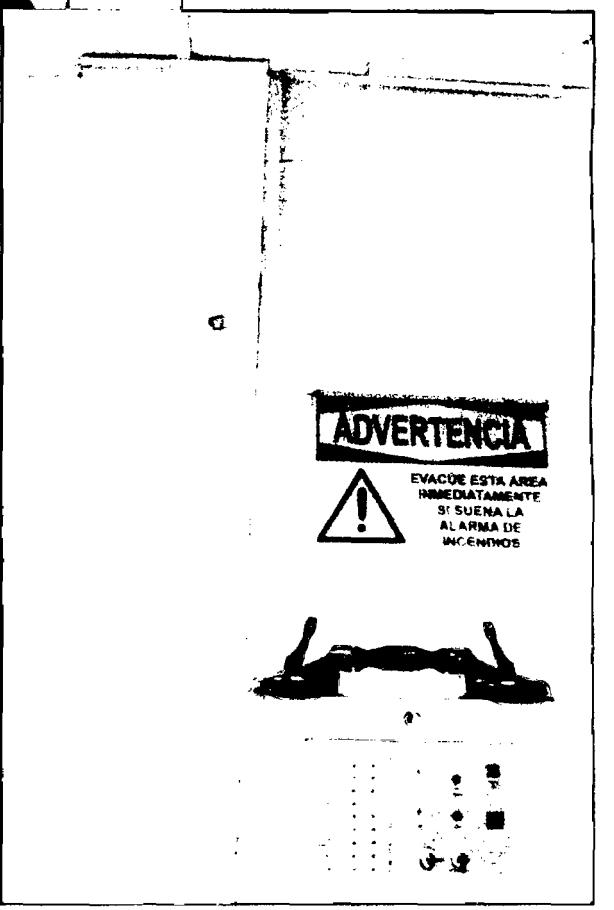
1.1. ALGUNAS EVIDENCIAS PARA DETERMINAR VALORACIÓN DE AMENAZAS Y VULNERABILIDADES



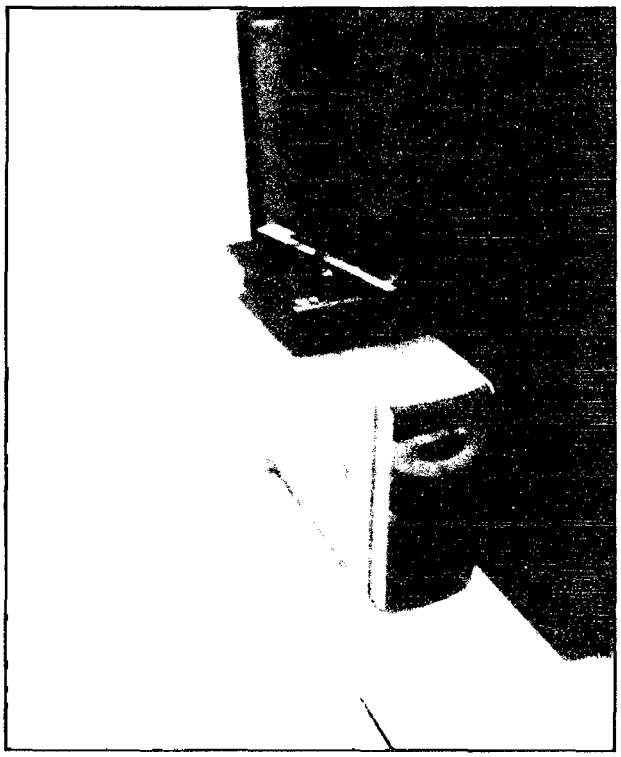
Falta de mantenimiento - UPS Datacenter





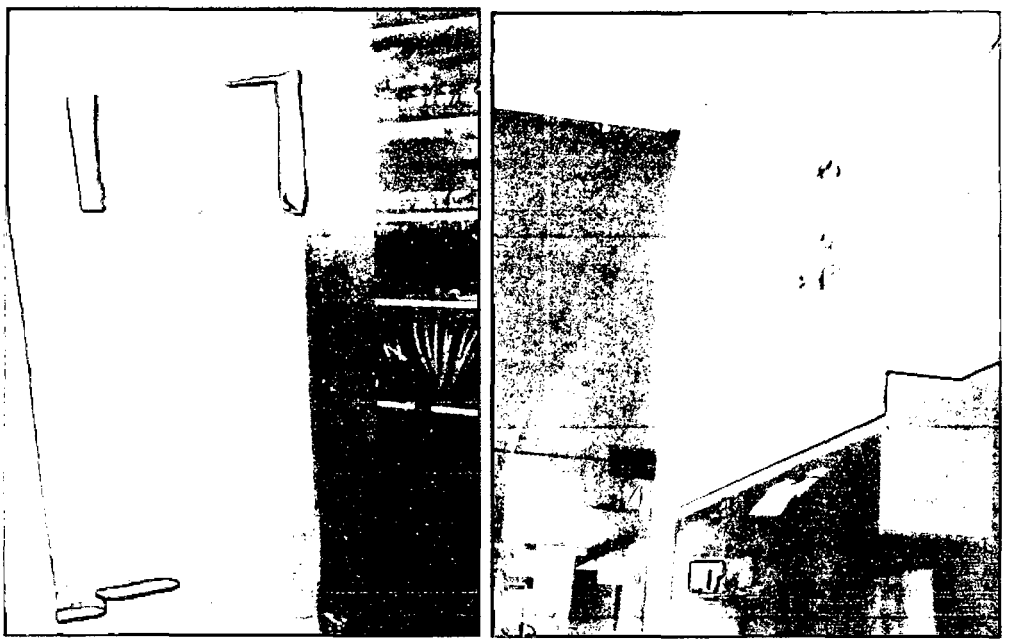


Datacenter – Material Inflamable – Humedad en paredes

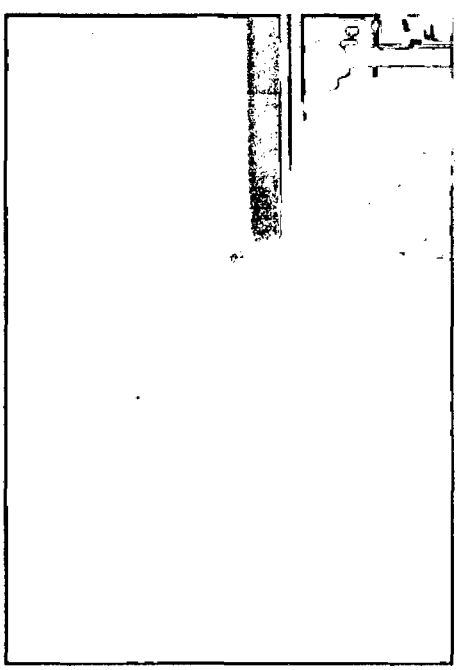


Servidores en el Piso

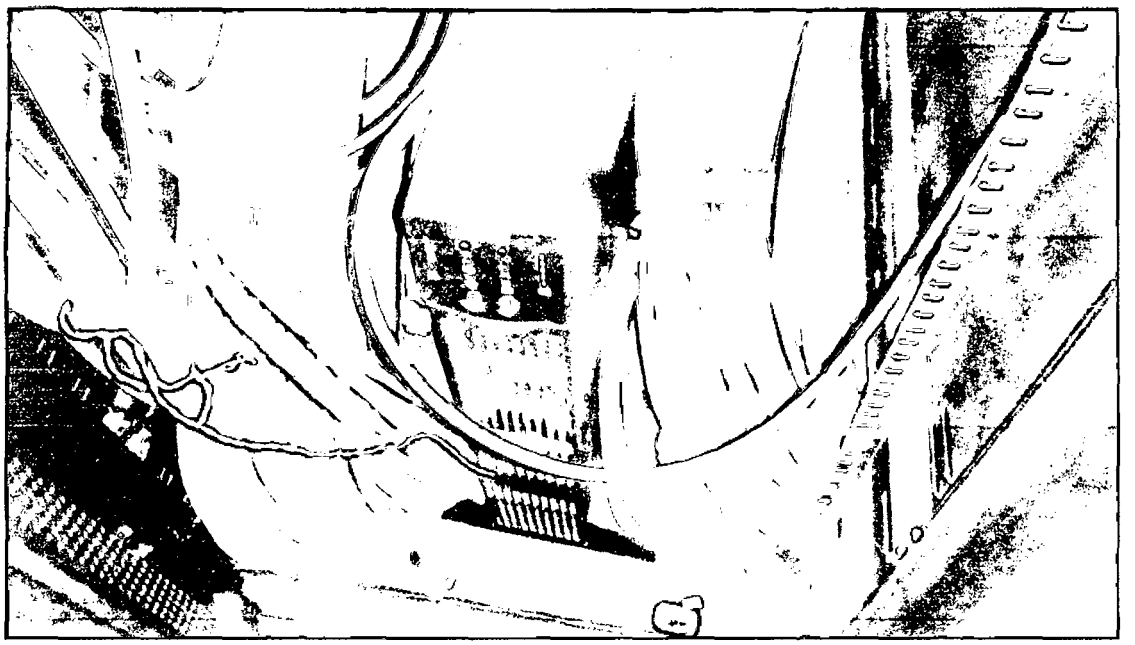
Cableado de red desordenado y sin protección



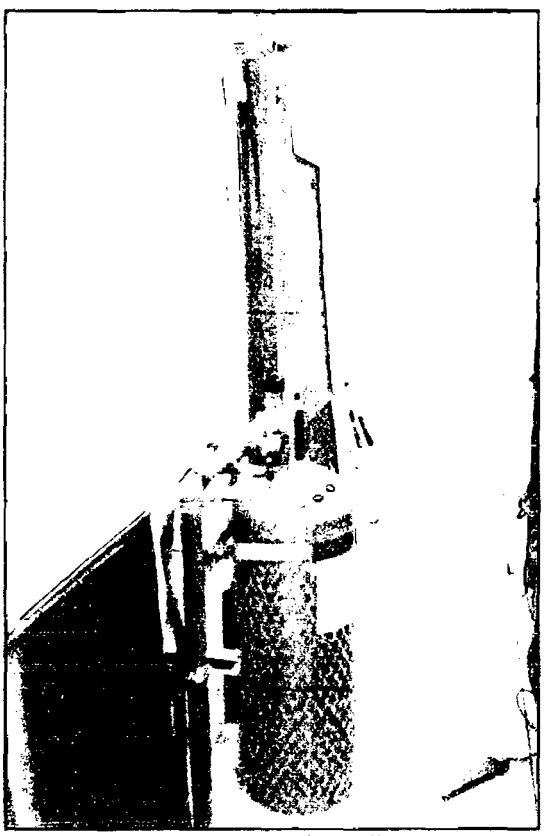
Ausencia de mantenimiento a las instalaciones



Puntos de Red sin uso, activos (pasadizo del GRC)



Ausencia de mantenimiento a equipos



Sistema contra incendios

1.2. MAPEANDO OBJETIVOS DE CONTROL DE COBIT 4.1 – ITIL V 3 – ISO 27002

El siguiente cuadro se visualiza el mapeo para relacionar objetivos de control de COBIT, ITIL e ISO 27002. Sólo es un extracto de algunos objetivos de control. Para más detalle pueden visitar la URL www.isaca.org

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
4.1 Evaluando riesgos de seguridad	4.0 Evaluación y tratamiento de riesgos	• PO9.4 Evaluación de riesgos de TI	• PO9 Evaluar y gestionar los riesgos de TI	
4.2 Tratamiento de los riesgos de seguridad			• PO9 Evaluar y gestionar los riesgos de TI	
5.1 Políticas de seguridad de la información	5.0 Política de seguridad			
5.1.1 Documento de la política de seguridad de información		• PO6.1 Política y entorno de control de TI • PO6.2 Riesgo corporativo y marco de referencia del control interno de TI • PO6.3 Gestión de políticas de TI • PO6.5 Comunicación de los objetivos y la dirección de TI • DS5.2 Plan de seguridad de TI • DS5.3 Gestión de identidad • ME2.1 Monitoreo del marco de trabajo de control interno	• PO6 Comunicar las aspiraciones y la dirección de la gerencia • DS5 Garantizar la seguridad de los sistemas • ME2 Monitorear y evaluar el control interno	• SS 6.4 Cultura organizacional • ST 5.1 Gestión de las comunicaciones y el compromiso • SO 3.6 Comunicaciones • SO 4.5 Gestión de accesos • SD 4.6.4 Políticas, principios y conceptos básicos • SD 4.6.5.1 Controles de seguridad (cobertura de alto nivel, sin detalle)

Alineando Cobit 4.1, ITIL v3 e ISO 27002 en beneficio del negocio
Fuente: http://www.isaca.org/Knowledge-Center/Research/Documents/Alineando-COBIT-4-1-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa_res_Spa_0108.pdf

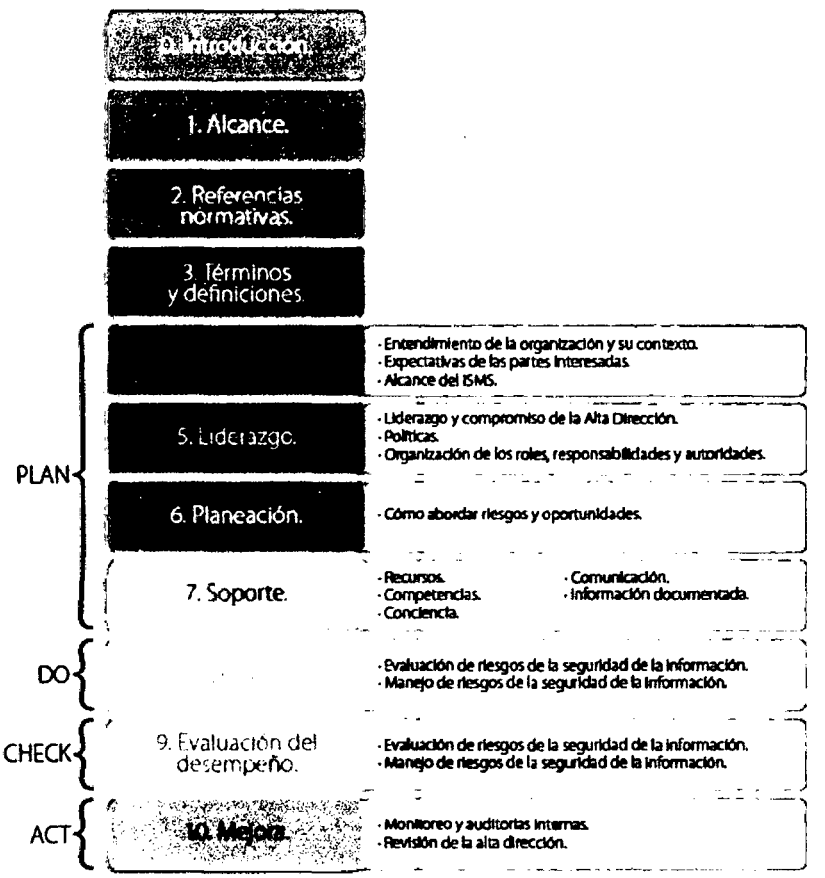
1.3. INTRODUCCIÓN ISO/IEC-27001:2013

En Marzo del presente año, la BSI ha dado a conocer el borrador de la norma ISO/IEC-27001:2013 donde ya se aprecian algunos cambios significativos a tener en cuenta para el futuro.

Las modificaciones más significativas encontradas están en la estructura y el contenido de los controles que conforman el anexo A, incrementándose de 11

dominios a 14 y reduciendo en número de controles de 133 a 113 (donde algunos controles se han fusionado, otros se han excluido, y otros nuevos incorporados).

La nueva estructura de la ISO/IEC 27001:2013



Estructura ISO27001:2013
Fuente: http://www.magazcitum.com.mx

Descripción de las principales secciones

0. Introducción

El cambio más significativo en todo el apartado fue la eliminación de la sección "Enfoque del proceso" que contenía la versión 2005, en donde se describía el modelo PDCA, corazón del Sistema de Gestión de Seguridad de la Información

(SGSI). Además de la ya mencionada alineación con el Anexo SL de la ISO/IEC, sección 1.

1. Alcance

En esta sección se establece la obligatoriedad de cumplir con los requisitos especificados en los capítulos 4 a 10 del documento, para poder obtener la conformidad de cumplimiento y certificarse.

2. Referencias normativas

El estándar ISO-27002 ya no es una referencia normativa para ISO-27001:2013, aunque continúa considerándose necesario en el desarrollo de la declaración de aplicabilidad (SOA, por sus siglas en inglés).
El estándar ISO 27000:2013 se convierte en una referencia normativa obligatoria y única, ya que contiene todos los nuevos términos y definiciones.

3. Términos y definiciones

Los términos y definiciones que se manejaban en 27001:2005 los trasladaron y agruparon en la sección 3 de ISO 27000:2013 "Fundamentos y vocabulario" (lo cual se llevará a cabo en todos los documentos que forman parte de esta familia), con el objetivo de contar con una sola guía de términos y definiciones que sea consistente.

4. Contexto de la organización

Esta cláusula hace hincapié en identificar los problemas externos e internos que rodean a la organización.

- Instituye los requerimientos para definir el contexto del SGSI sin importar el tipo de organización y su alcance.
- Introduce una nueva figura (las partes interesadas) como un elemento primordial para la definición del alcance del SGSI.
- Establece la prioridad de identificar y definir formalmente las necesidades de las partes interesadas con relación a la seguridad de la información y sus expectativas con relación al SGSI, pues esto determinará las políticas de

seguridad de la información y los objetivos a seguir para el proceso de gestión de riesgos.

5. Liderazgo

Ajusta la relación y responsabilidades de la Alta Dirección respecto al SGSI, destacando de manera puntual cómo debe demostrar su compromiso, por ejemplo:

- Garantizando que los objetivos del SGSI y "La política de seguridad de la información", anteriormente definida como "Política del SGSI", estén alineados con los objetivos del negocio.
- Garantizando la disponibilidad de los recursos para la implementación del SGSI (económicos, tecnológicos, etcétera).
- Garantizando que los roles y responsabilidades claves para la seguridad de la información se asignen y se comuniquen adecuadamente.

6. Planeación

Esta es una nueva sección enfocada en la definición de los objetivos de seguridad como un todo, los cuales deben ser claros y se debe contar con planes específicos para alcanzarlos.

Se presentan grandes cambios en el proceso de evaluación de riesgos:

- El proceso para la evaluación de riesgos ya no está enfocado en los activos, las vulnerabilidades y las amenazas.
- Esta metodología se enfoca en el objetivo de identificar los riesgos asociados con la pérdida de la confidencialidad, integridad y disponibilidad de la información.
- El nivel de riesgo se determina con base en la probabilidad de ocurrencia del riesgo y las consecuencias generadas (impacto), si el riesgo se materializa.
- Se ha eliminado el término "Propietario del activo" y se adopta el término "Propietario del riesgo".
- Los requerimientos del SOA no sufrieron transformaciones significativas.

7. Soporte

Marca los requerimientos de soporte para el establecimiento, implementación y mejora del SGSI, que incluye:

- Recursos
- Personal competente
- Conciencia y comunicación de las partes interesadas

Se incluye una nueva definición "información documentada" que sustituye a los términos "documentos" y "registros"; abarca el proceso de documentar, controlar, mantener y conservar la documentación correspondiente al SGSI.

El proceso de revisión se enfoca en el contenido de los documentos y no en la existencia de un determinado conjunto de estos.

8. Operación

Establece los requerimientos para medir el funcionamiento del SGSI, las expectativas de la Alta Dirección y su realimentación sobre estas, así como el cumplimiento con el del estándar.

Además, plantea que la organización debe planear y controlar las operaciones y requerimientos de seguridad, erigiendo como el pilar de este proceso la ejecución de evaluaciones de riesgos de seguridad de la información de manera periódica por medio de un programa previamente elegido.

Los activos, vulnerabilidades y amenazas ya no son la base de la evaluación de riesgos. Solo se requiere para identificar los riesgos asociados con la confidencialidad, integridad y disponibilidad.

9. Evaluación del desempeño

La base para identificar y medir la efectividad y desempeño del SGSI continúan siendo las auditorías internas y las revisiones del SGSI.

Se debe considerar para estas revisiones el estado de los planes de acción para atender no conformidades anteriores y se establece la necesidad de definir quién y cuándo se deben realizar estas evaluaciones así como quién debe analizar la información recolectada.

10. Mejora

El principal elemento del proceso de mejora son las no-conformidades identificadas, las cuales tienen que contabilizarse y compararse con las acciones correctivas para asegurar que no se repitan y que las acciones correctivas sean efectivas.

Aquí se observa uno de los cambios más importantes porque las medidas preventivas se fusionarán con la evaluación y tratamiento del riesgo, algo más natural e intuitivo que permite enfrentar los riesgos y las oportunidades con base en cuándo estos se identifican y cómo se tratan. Además, se distingue entre las correcciones que se ejecutan como una respuesta directa a una "no conformidad", en oposición a las acciones correctoras que se realizan para eliminar la causa de la no conformidad.

Anexos

El "Anexo A – Referencia de objetivos y controles" continúa formando parte de este estándar, pero los anexos "B" y "C" se han eliminado.

Sin ser intención de este artículo brindar una descripción completa de los cambios efectuados, se detallan algunos de los principales:

- El número de dominios del anexo aumenta de 11 a 14, de esta manera, donde algunos controles se incluían de forma "artificial" en ciertas áreas donde no encajaban perfectamente, ahora se organizan mejor.

Figura Dominios Anexo "A" de ISO 27001:2013
Fuente: http://www.magazcitum.com.mx

1.4. DEFINICIONES

ACTIVO: Algo que presenta valor para la organización.

AMENAZA: Causa potencial de un incidente no deseado que puede resultar en daño al sistema u organización.

ANÁLISIS DEL RIESGO: Uso sistemático de información para identificar y estimar el riesgo.

CONTROL: Herramienta de la gestión del riesgo, incluido políticas, pautas, estructuras organizacionales, que pueden ser de naturaleza administrativa, técnica, gerencial o legal. El término también es usado como sinónimo de salvaguarda o contramedida.

CONFIDENCIALIDAD: Garantizar que la información sea accesible únicamente para quienes tengan acceso autorizado.

DISPONIBILIDAD: Garantizar que los usuarios autorizados tengan acceso a la información y activos asociados cuando sea necesario.

GESTIÓN DEL RIESGO: Actividades coordinadas para dirigir y controlar el riesgo.

IMPACTO: Consecuencia sobre un activo de la materialización de una amenaza.

INTEGRIDAD: Salvaguardar la exactitud e integridad de la información y activos asociados.

RIESGO: Es la posibilidad de pérdida, o daño, o disminución de la posibilidad de beneficios; causada por factores que pueden

afectar adversamente la realización de objetivos de una organización

RIESGO RESIDUAL: Riesgo remanente después de un tratamiento del riesgo.

TRANSFERENCIA DEL RIESGO: Compartir con otra de las partes la pérdida o la ganancia de un riesgo.

VULNERABILIDAD: es una debilidad de un bien o de un control, que puede ser aprovechada por una o más amenazas. Se trata de una característica negativa del bien, también conocido como activo o recurso de información, o de un control que se implementó sobre él, que lo hace vulnerable. En efecto esa vulnerabilidad es susceptible de ser aprovechada y varía de acuerdo con los cambios en las condiciones que dieron origen a su existencia o a las acciones que se tomen con el fin de evitar su explotación o aprovechamiento.

METODOLOGÍA: La metodología hace referencia al conjunto de procedimientos racionales utilizados para alcanzar una gama de objetivos que rigen en una investigación científica, una exposición doctrinal o tareas que requieran habilidades, conocimientos o cuidados específicos.