



GOBIERNO REGIONAL  
HUANCAVELICA

# Resolución Gerencial General Regional

Nro. 923 -2016/GOB.REG-HVCA/GGR

Huancavelica, 14 DIC 2016

**VISTO:** El Informe N° 341-2016/GOB.REG.HVCA/GRPPyAT con N° Doc. 259545 y N° Exp. 188498, el Informe N° 503-2016/GOB.REG.HVCA/GRPPyAT-SGDIyII, el Informe N° 180-2016/GOB.REG.HVCA/GRPPyAT-SGDIyII-PYTIC, el Informe N° 081-2016/ GOB.REG.HVCA/GRPPyAT-SGDIyII-drtm, la Carta N° 002-2016/HEC, la Carta N° 008-2016/GOB.REG.HVCA/GRPPyAT-SGDIyII, el Informe N° 080-2016/ GOB.REG.HVCA/GRPPyAT-SGDIyII-drtm, la Carta N° 001-2016/HEC; y,

## CONSIDERANDO:

Que, de conformidad con el Artículo 191° de la Constitución Política del Estado, modificado por Ley N° 27680 – Ley de Reforma Constitucional, del Capítulo XIV, del Título IV, sobre Descentralización, concordante con el Artículo 31° de la Ley N° 27783 – Ley de Bases de la Descentralización, el Artículo 2° de la Ley N° 27867 – Ley Orgánica de Gobiernos Regionales y el Artículo Único de la Ley N° 30305, los Gobiernos Regionales son personas jurídicas que gozan de autonomía política, económica y administrativa en los asuntos de su competencia;

Que, mediante Resolución Gerencial General Regional N° 643-2015/GOB.REG.HVCA/GGR, de fecha 01 de setiembre del 2015, se aprobó el Plan Operativo Anual del PIP: “Mejoramiento de los Servicios de Tecnologías de Información y Comunicación en la Sede Principal y las Direcciones Regionales del Gobierno Regional de Huancavelica”, con código SNIP N° 266096, con un presupuesto total ascendente a S/. 1'559,072.50 (Un millón quinientos cincuenta y nueve mil setenta y dos con 50/100 Soles), cuya ejecución se encuentra a cargo de la Sub Gerencia de Desarrollo Institucional y Tecnologías de Información;

Que, a efectos de estar preparados para afrontar contingencias y desastres diversos, la Sub Gerencia de Desarrollo Institucional y Tecnologías, en el marco del proyecto: “Mejoramiento de los Servicios de Tecnologías de Información y Comunicación en la Sede Principal y las Direcciones Regionales del Gobierno Regional de Huancavelica”, presenta el Plan de Contingencia de Sistemas de Información que servirá como una guía rápida para solucionar los imprevistos y situaciones que afecten el correcto funcionamiento de los activos informáticos identificados a nivel de Data Center de la institución; en tal sentido, amerita su aprobación mediante el presente acto resolutivo;

Estando a lo informado; y,

Con la visación de la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial, Oficina Regional de Asesoría Jurídica y la Secretaría General;

En uso de las atribuciones conferidas por la Constitución política del Perú, Ley N° 27783 - Ley de Bases de la Descentralización, Ley N° 27867 - Ley Orgánica de los Gobiernos Regionales, modificado por la Ley N° 27902.

## SE RESUELVE:

**ARTÍCULO 1°.- APROBAR** el Plan de Contingencia de Sistemas de Información presentado por la Sub Gerencia de Desarrollo Institucional y Tecnologías de la Información en el marco del proyecto: “Mejoramiento de los Servicios de Tecnologías de Información y Comunicación en la Sede Principal y las Direcciones Regionales del Gobierno Regional de Huancavelica”, documento de gestión que en calidad de anexo forma parte integrante de la presente Resolución.

**ARTÍCULO 2°.- ENCARGAR** a la Sub Gerencia de Desarrollo Institucional y Tecnologías de la Información, la implementación, supervisión y ejecución del Plan de Contingencia de Sistemas de Información.





GOBIERNO REGIONAL  
HUANCAVELICA

# Resolución Gerencial General Regional

Nro. 923 -2016/GOB.REG-HVCA/GGR

Huancavelica, 14 DIC 2016

**ARTÍCULO 3°.- NOTIFICAR**, la presente Resolución a los órganos Competentes del Gobierno Regional de Huancavelica, Sub Gerencia de Desarrollo Institucional y Tecnologías de la Información, para los fines pertinentes.

**REGÍSTRESE, COMUNÍQUESE Y ARCHÍVESE.**

GOBIERNO REGIONAL HUANCAVELICA

Ing. Grober Enrique Flores Barrera  
GERENTE GENERAL REGIONAL



JCI/cgmc

GOBIERNO REGIONAL DE HUANCAMELICA  
GERENCIA REGIONAL DE PLANEAMIENTO,  
PRESUPUESTO Y ACONDICIONAMIENTO  
TERRITORIAL




*Gobierno Regional*  
**HUANCAMELICA**

SUB GERENCIA DE DESARROLLO  
INSTITUCIONAL Y TECNOLOGÍAS DE LA  
INFORMACIÓN

**PLAN DE CONTINGENCIA DE  
SISTEMAS DE INFORMACIÓN**



Noviembre - 2016

	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

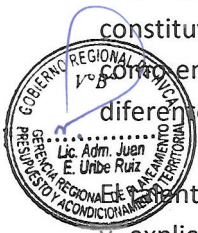
## PRESENTACIÓN


La información es uno de los más importantes activos que posee toda institución la cual se genera en sus acciones y diferentes ámbitos. La Sub Gerencia de Desarrollo Institucional y Tecnologías de la Información, del Gobierno Regional de Huancavelica, consciente de esta premisa podemos advertir que se debe adoptar medidas de seguridad para la información y así mismo estar preparados para poder afrontar contingencias y desastres diversos, ejemplo: virus informáticos, inundaciones, intentos de hacking, cortes de fluido eléctrico, instalaciones eléctricas instaladas a la intemperie, accesos no autorizados, escaso personal profesional y técnico, etc, por lo que el riesgo de sufrir situaciones que perjudiquen el normal desenvolvimiento de las actividades es muy alto, más aún, teniendo el nivel sociocultural y económico, determinan la alta vulnerabilidad a la información generada y/o procesada dentro del Gobierno Regional de Huancavelica.

La Sub Gerencia de Desarrollo Institucional y Tecnologías de la Información, del Gobierno Regional de Huancavelica tiene, entre otros, el propósito de proteger la información y así asegurar su procesamiento y desarrollo de funciones institucionales. En base a ello se presenta el Plan de Contingencia Informático en su primera versión, el cual guarda relación con el marco del Plan Operativo Institucional (POI), diseñado para el desarrollo y ejecución de los objetivos de cada año. La ejecución del Plan de Contingencia Informático permitirá prevenir cualquier problema y/o desastres relacionados con la información técnica, software propietario y hardware, así como suministros informáticos y talento humano, etc.

Al presente, los profesionales y técnicos de la informática tienen como una de sus principales actividades y ocupaciones velar por la seguridad de los sistemas computacionales, que constituyen la base y respaldo a las funciones institucionales realizada a través del tiempo, así como en la actualidad facilitan sobre manera las tareas que se desarrollan en la ejecución de los diferentes procesos administrativos, logísticos, ejecutivos, informativos, entre otros.

El personal de talento humano, responsable del servicio informático están obligados a hacer de conocimiento y explicar con lenguaje entendible a los directivos y/o funcionarios regionales las posibles consecuencias que la seguridad insuficiente o inexistente pueda acarrear; de esta manera proponer y poner a consideración las medidas de seguridad inmediatas y a mediano plazo, que han de tomarse en cuenta para prevenir los desastres que pueda provocar el colapso de los sistemas informáticos.




	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

## Contenido


CAPITULO I .....	5
1. Introducción .....	5
2. ¿Qué es un Sistema de Información? .....	6
3. ¿Qué es un Plan de Contingencia? .....	6
3.1. Características principales de un Plan de Contingencia .....	7
4. Objetivo General.....	7
5. Objetivos Específicos .....	7
6. Base Legal .....	7
7. Alcance.....	8
8. Meta .....	8
9. Marco Teórico.....	8
9.1. Plan de Prevención .....	9
9.2. Plan de Ejecución.....	9
9.3. Plan de Recuperación .....	9
9.4. Plan de Pruebas .....	9
CAPITULO II.....	10
2. PLANIFICACIÓN .....	10
2.1. Diagnóstico .....	10
2.2. Organización .....	12
2.3. Organización del Plan de Contingencia .....	13
2.4. Servicios y/o Bienes Producidos .....	14
2.5. Inventario de Recursos Informáticos.....	15
IDENTIFICACIÓN DE RIESGOS .....	18
3.1. Análisis de Riesgos.....	18
3.1.1. Caracterización y Valoración de los Activos .....	19
Identificación de Activos.....	19
Valoración de Activos Tipo: Aplicaciones Informáticas .....	20
Valoración de Activos Tipo: Servicios .....	21
Valoración de Activos Tipo: Redes de Comunicaciones .....	22
Valoración de Activos Tipo: Equipamiento Informático.....	23
Valoración de Activos Tipo: Equipamiento Auxiliar.....	24



	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

Valoración de Activos Tipo: Instalaciones .....	25
Valoración de Activos Tipo: Personal .....	25
3.1.2. Caracterización y Valoración de los Activos .....	27
Frecuencia de Amenazas .....	27
Degradación de las Amenazas .....	27
Identificación y Valoración de Amenazas Tipo: Aplicaciones Informáticas.....	27
Justificación de Amenazas – Aplicaciones Informáticas.....	28
Identificación y Valoración de Amenazas Tipo: Servicios.....	29
Justificación de Amenazas – Servicios .....	29
Identificación y Valoración de Amenazas Tipo: Redes de Comunicaciones.....	29
Justificación de Amenazas – Redes de Comunicaciones.....	30
Identificación y Valoración de Amenazas Tipo: Desastres Naturales.....	30
Justificación de Amenazas – Desastres Naturales .....	30
Identificación y Valoración de Amenazas Tipo: Equipamiento Auxiliar .....	30
Justificación de Amenazas – Equipamiento Auxiliar.....	30
Identificación y Valoración de Amenazas Tipo: Instalaciones.....	30
Justificación de Amenazas –Instalaciones.....	31
Identificación y Valoración de Amenazas Tipo: Personal.....	31
Justificación de Amenazas –Personal.....	31
3.1.3. Tablas de Amenazas vs Vulnerabilidades .....	31
Desastres Naturales [DesN] .....	31
Errores y fallos no intencionados [E.N] .....	32
Amenazas de origen industrial [Indus.].....	33
Amenazas a Causa de Ataques Intencionados [A_Int.] .....	34
3.1.4. Estimación Del Estado De Riesgo .....	36
Estimación Del Impacto.....	36
Valoración de riesgo en activos de información .....	38
DESARROLLO DE FASES, ACTIVIDADES, ESTRATEGIA, PROGRAMAS Y POLÍTICAS.....	40
RECOMENDACIONES .....	50
CONCLUSIONES.....	51
GLOSARIO DE TERMINOS.....	52
BIBLIGRAFIA.....	54



	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

ANEXOS..... 55

FORMATOS ..... 55

CATÁLOGOS DE ACTIVOS: MAGERIT VERSIÓN 3.0 ..... 58

1. [D] Datos / Información ..... 58

2. [S] Servicios..... 58

3. [SW] Software - Aplicaciones informáticas ..... 59

4. [HW] Equipamiento informático (hardware) ..... 59

5. [COM] Redes de comunicaciones..... 60

6. [AUX] Equipamiento auxiliar ..... 60


7. [L] Instalaciones..... 61

8. [P] Personal..... 61

CRITERIOS DE VALORACIÓN ..... 62

ESCALA ESTÁNDAR ..... 62



	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

## CAPITULO I

### DEFINICIONES Y ALCANCES

#### 1. Introducción

Es conocido que toda organización es vulnerable a las fallas o caídas de los sistemas informáticos poniendo en riesgo el normal funcionamiento de las diversas actividades que realiza una empresa o institución de servicios, como es el caso del Gobierno Regional de Huancavelica, ya que la paralización de los servicios informáticos internos y externos originada por la falta de prevención, generaría gran malestar en todos los usuarios externos, empleados y funcionarios regionales confundidos por no poder controlar el servicio informático regional.

El tiempo siempre es corlo para resolver sorpresivos y diversos problemas informáticos, más aun teniendo en cuenta que no se cuenta con un Plan de Contingencias; es por eso que desde este lugar y como formulador de este proyecto se exige su implementación al 100%, siendo la Sub Gerencia de Desarrollo Institucional y Tecnologías de la Información la responsable de gestionar su implantación, supervisar y controlar su ejecución, cabe señalar que el presente Plan de Contingencias deberá ser aprobado con la Resolución correspondiente, lo cual legalizará su ejecución.

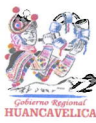
Con la elaboración del presente Plan de Contingencia de Sistemas de Información, la Sub Gerencia de Desarrollo Institucional y Tecnologías de la Información busca contribuir al buen desarrollo de Plan Operativo informático POI y otras actividades pertinentes. Entre los principales sistemas que procesan información digitalizada tenemos: Planillas de Remuneraciones (SUP) de empleados, Obreros, CAS, Pensionistas, Consejeros, Escalafón y Legajos, SIGA, SIAF, SISGEDO, PCSistel, Control de Cheques, Portal Web Institucional, Portal de Transparencia Estándar - PTE, Sistema de Descargas (normas regionales, documentos de gestión, adquisiciones y contrataciones, proyectos de inversión, información presupuestal y financiera, audiencias y rendición de cuentas, entre otros), etc.

Debe tener en cuenta que el riesgo del problema no se limita únicamente a los sistemas de información internos que contiene los equipos de la Sub Gerencia de Desarrollo Institucional y Tecnologías de la Información, sino también a otros equipos de cómputo operativos en otras áreas, muchas de las cuales dependen de la información y datos proporcionada por el público contribuyente, proveedores o de la Gerencia General Regional. Con el fin de que las áreas usuarias continúen operando a pesar de que algunos sistemas informáticos puedan presentar deficiencias, se elabora este Plan de Contingencias para que la comisión correspondiente pueda supervisar la vigencia del mismo obteniendo soluciones de emergencia rápidas.

Toda vez que las diversas áreas usuarias del GORE Huancavelica, procesan información computarizada se encuentran desarrollando acciones para dar cumplimiento a la ejecución del Plan Operativo Institucional, sin embargo es posible, que en algunos casos no respondan a lo





	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

planeado ni concluyan oportunamente las tareas o metas establecidas a consecuencias de los desastres que podrían presentarse, justificación suficiente que amerita la elaboración del presente Plan de Contingencias en su primera versión.

Todo sistema de información utiliza como materia prima los datos, los cuales se almacena, procesa y transforma para obtener como resultado final información, la cual será suministrada a los diferentes usuarios del sistema, existiendo además un proceso de retroalimentación o "feedback" (Retroalimentación), en la cual se ha de valorar si la información obtenida se adecua a lo esperado.

## 2. ¿Qué es un Sistema de Información?

Un sistema de información es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo. Dichos elementos formarán parte de alguna de las siguientes categorías: Personas; Datos; Actividades o técnicas de trabajo; Recursos materiales en general (generalmente recursos informáticos y de comunicación, aunque no necesariamente).


Un Sistema Informático utiliza ordenadores para almacenar los datos de una organización y ponerlos a disposición de su personal. Pueden ser tan simples como en el que una persona tiene una computadora e introduce datos, los datos pueden ser registros simples como ventas diarias, se produce una entrada por cada venta.

Sin embargo, la mayor parte de los sistemas son más complejos que el enunciado anteriormente. Normalmente una organización tiene más de un sistema de computadoras para soportar las diferentes funciones de la organización, ya sean de ventas, recursos humanos, contabilidad, producción, inventario, etc.

Los sistemas de información tienen muchas cosas en común. La mayoría de ellos están formados por personas, equipos y procedimientos. Al conjugar una serie de elementos como personas y computadoras se hace imprescindible tomar medidas que nos permitan una continuidad en la operatividad de los sistemas para no ver afectados los objetivos de las mismas y no perder la inversión de costos y tiempo.

## ¿Qué es un Plan de Contingencia?

Un Plan de Contingencias es una herramienta estratégica planificada con una serie de procedimientos que nos facilitan u orientan a tener una solución alternativa y nos permite restituir rápidamente los servicios de la organización ante la eventualidad que pueda paralizar los servicios, ya sea de forma parcial o total, es decir, un plan que le permite a su negocio u organización, seguir operando, aunque sea de forma limitada.

	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN GOBIERNO REGIONAL DE HUANCAMELICA	Fecha: Noviembre 2016 Versión:1.0

### 3.1. Características principales de un Plan de Contingencia

- 3.1.1.**Amplio:** Porque considera a todos los componentes de los procesos de una Institución u organización.
- 3.1.2.**Abierto en el tiempo:** Para dar respuesta permanente a cualquier tipo de incidencias.
- 3.1.3.**Participativo:** Porque se pretende que intervenga todos los agentes, instituciones o agrupaciones que estén implicados de una u otra forma en el servicio.
- 3.1.4.**Eminentemente práctico:** Ya que fija objetivos concretos y establece los medios y los plazos.

La vigencia del plan será hasta que los procesos a los que suple estén nuevamente operativos.

### 4. Objetivo General

Contar con un Plan de Contingencias actualizado, que permita la continuidad en los procedimientos informáticos de la Sub Gerencia de Desarrollo Institucional y Tecnologías de la Información, así como disminuir las fallas y eventos inesperados; con el propósito de asegurar y restaurar los equipos e información con las menores pérdidas posibles en forma rápida, eficiente y oportuna; buscando la mejora de la calidad en los servicios que brinda la SGOIyTI.

### 5. Objetivos Específicos

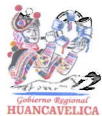
- a) Identificar amenazas de orden natural, operacional o exógeno asociadas a los sistemas informáticos del GRH que puedan afectar eventualmente su normal funcionamiento.
- b) Estimar los riesgos a partir de la valoración de las amenazas identificadas y la vulnerabilidad propias de los sistemas informáticos del GRH ante diferentes contingencias que pueden presentarse.
- c) Generar un plan de respuesta que articule diferentes estrategias definidas por procedimientos, recursos e instrumentos necesarios para la prevención, control y atención de los riesgos identificados.
- d) Establecer un manual de procedimientos formales que indique las acciones a seguir para afrontar con éxito un incidente o emergencia, de tal manera que cause el menor impacto.
- e) Generar una documentación práctica y actualizada que garantice al GORE Huancavelica la continuidad de las operaciones de los sistemas informáticos sin sufrir paralizaciones o pérdidas relevantes.
- f) Contar con personal debidamente capacitado y organizado para afrontar adecuadamente las contingencias que puedan presentarse en las actividades del GORE Huancavelica.



### 6. Base Legal

- a) Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado.
- b) Ley N° 30096, Ley de Delitos Informáticos.
- c) Ley N° 30171, Ley que modifica la Ley N° 30096.
- d) Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública.
- e) RM N° 004-2016-PCM, Aprueban el uso obligatorio de la Norma Técnica Peruana "ISO NTP/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de



	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

Gestión de Seguridad de la Información. Requisitos 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.

- f) DL. N° 601, Ley de Organización y Funciones del INEI.
- g) DS. N° 018-91-PMC, Reglamento de Organización y Funciones del INEI.
- h) RJ N° 340-94-INEI, Normas Técnicas para el procesamiento y respaldo de la información que se procesa en entidades del Estado.
- i) RJ. N° 076-95-INEI, Recomendaciones Técnicas para la seguridad e integridad de la información que se procesa en la administración pública.
- j) RJ N° 090-95-INEI, Recomendaciones Técnicas para la protección física de los equipos y medios de procesamiento de la información en la administración pública.
- k) RJ N° 140-95-INEI, Recomendaciones Técnicas para la Organización y Gestión de los Servicios Informáticos para la Administración Pública.
- l) RJ N° 229-95-INEI, Recomendaciones Técnicas para la Elaboración de Planes de Sistemas de Información en la Administración Pública

## 7. Alcance

La Implementación del Plan de Contingencia de Sistemas de Información - PCSI, incluye los elementos referidos a los aplicativos informáticos, equipos, infraestructura, personal, servicios y otros, direccionado a minimizar eventuales riesgos ante situaciones adversas que atentan contra el normal funcionamiento de los servicios de la sede central del GORE Huancavelica.

## 8. Meta

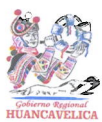
Potenciar el nivel informático de la Sub Gerencia de Desarrollo Institucional y Tecnologías de la Información (SGDIyTI) del GORE Huancavelica, y además las funciones cotidianas informáticas, haciéndolas seguras y consistentes, logrando con ello su buen desarrollo y la optimización de resultados

### Marco Teórico

El Plan de Contingencia de Sistemas de Información - PCSI, es un documento que reúne un conjunto de procedimientos alternativos para facilitar el normal funcionamiento de las tecnologías de Información y de Comunicaciones - TIC's de la sede central del GORE Huancavelica, cuando alguno de sus servicios se ha afectado negativamente por causa de algún incidente interno o externo a la organización.

El Plan de Contingencia permite minimizar las consecuencias en caso de incidente con el fin de reanudar las operaciones en el menor tiempo posible en forma eficiente y oportuna.

El término "incidente" en este contexto será entendido como la interrupción de las condiciones normales de operación en cualquier proceso informático en la sede central del GORE Huancavelica.

	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016 Versión:1.0

### 9.1. Plan de Prevención

Es el conjunto de acciones, decisiones y comprobaciones orientadas a prevenir la presencia de un evento con el propósito de disminuir y mitigar la probabilidad de ocurrencia del mismo en los factores identificados en el presente plan.

El plan de prevención es la parte principal del Plan de Contingencia Informático porque permite aminorar y atenuar la probabilidad de ocurrencia de un estado de contingencia.

### 9.2. Plan de Ejecución

Es el conjunto detallado de acciones a realizar en el momento que se presenta el incidente de contingencia y que activa un mecanismo alterno que permitirá reemplazar a la actividad normal cuando este no se encuentra disponible.

Las acciones descritas dentro del plan de ejecución deben ser completamente claras y definidas de forma tal que sean de conocimiento y entendimiento inequívoco del personal involucrado en atender la contingencia.

### 9.3. Plan de Recuperación

Es el conjunto de acciones que tienen por objetivo restablecer oportunamente la capacidad de las operaciones, procesos y recursos del servicio que fueron afectados por un evento de contingencia.


Todo Plan de Contingencia Informático debe tener un carácter recursivo que permita retroalimentar y mejorar continuamente los planes en cada una de las etapas descritas, logrando así tener un documento dinámico.

### 9.4. Plan de Pruebas

El Plan de Pruebas, será presentado a la Gerencia General Regional del GORE Huancavelica, para su aprobación previa a su implementación. El resultado de las pruebas efectuadas será presentado igualmente para su conformidad.

Las pruebas relacionadas a este plan, debe ser programada en el segundo semestre del siguiente año con el fin de evaluar la preparación de la organización ante la ocurrencia de un siniestro y realizar los ajustes necesarios.



	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

## CAPITULO II

### DESARROLLO DE LAS FASES METODOLÓGICAS, ACTIVIDADES, ESTRATÉGIAS, PROGRAMAS Y POLÍTICAS

#### 1. Marco metodológico

Los planes de contingencia se organizan para que las instituciones y empresas puedan prevenir fallas o accidentes en sus operaciones diarias y les permita seguir activas, en la provisión de servicios o productos, en el caso de que algún componente sufra cualquier tipo de problemas que condicione el correcto funcionamiento de sus equipos tecnológicos, aplicaciones informáticas y otros sistemas críticos, lo cual indica que la Sub Gerencia de Desarrollo Institucional y Tecnologías de la Información está involucrada en el tema.

Debemos de tener presente que mucho dependerá de la infraestructura de la institución y de los servicios que ésta ofrezca para determinar un modelo de desarrollo de plan, no existe un modelo único para todos, lo que se intenta es dar los puntos más importantes a tener en cuenta.

La metodología empicada para el desarrollo y aplicación del plan de contingencias de los sistemas de información, ha sido desarrollada por el INEI, en base a la experiencia lograda en el desarrollo de planes de contingencia del año 2000. Asimismo, este plan en particular se apoya en la metodología Magerit versión 3, para realizar el análisis de riesgos del Gobierno Regional de Huancavelica, en temas referentes a los sistemas de información con los que cuenta en la actualidad.

La presente metodología se desarrollará por fases de la siguiente manera:




#### Análisis Interno:

##### FORTALEZAS

- a. Cuenta con personal con experiencia en las funciones informáticas y con experiencia en la administración pública.
- b. Trabajo en equipo.
- c. Personal motivado e Identificado con la institución.
- d. Apoyo de la Alta Dirección para ejecutar proyectos de modernización del Gobierno Regional de Huancavelica.
- e. Portal de Transparencia posicionado como uno de los Portales Webs más Transparentes a nivel nacional lo cual mejora la imagen institucional.
- f. Posibilidad de asumir funciones para desarrollar aplicaciones distribuidas en las diferentes plataformas en con la capacidad de trabajar en equipo con las diferentes unidades orgánicas de la institución



	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

## DEBILIDADES

- No existe sistemas de información integrados en el Gobierno Regional de Huancavelica.
- Falta de una adecuada infraestructura física del Área de Informática tomando en cuentas normas técnicas, y estándares de seguridad.
- Escasos recursos presupuestales para la obtención de hardware, software, herramientas, mobiliario, etc.
- No existe programas de capacitación especializado para el personal informático promovidos por la Institución.
- Las unidades orgánicas de la institución se encuentran ubicados en diferentes locales de la ciudad, siendo alguno de ellos alquilados.
- Falta de seguridad eléctrica de los locales del Gobierno Regional (inexistencia de pararrayos, pozo a tierra y sistema de puesta a tierra sin mantenimiento).
- No se cuenta con un sistema de gestión de seguridad de información, lo cual pone en riesgo información relevante de la entidad.
- Compra y recepción de equipos informáticos que no cumplen con las características y especificaciones técnicas necesarias debido a que no se toma en cuenta la opinión del área de informática para la adquisición y recepción de éstos.

## Análisis Externo:

### AMENAZAS


- Cambios permanentes y acelerados en las Tecnología de Información y Comunicación, que provocan el desfase acelerado de los equipos.
- Los altos costos de software y de hardware.
- No existe políticas claras en materia de informática por parte del Gobierno Central, para el desarrollo de sistemas de información integrales en los Gobiernos Regionales.

### OPORTUNIDADES

- Demanda potencial y creciente de los usuarios de la entidad a los servicios informáticos, sistemas de información, asistencia y soporte técnico.
- El Gobierno Regional de Huancavelica es una institución ya consolidada por lo que la informática y las soluciones tecnológicas deben empezar a mantenerse alineadas a la visión de ésta.
- Surgimiento de programas y software de uso libre.
- Posibilidad del desarrollo e implementación en la Página Web para brindar servicios de consultas en línea.
- Crecimiento de uso de las herramientas de Tecnologías de la Información y las Comunicación para consultas y gestiones en línea de nuestro portal web, la cual nos exige a mejorar nuestros sistemas de gestión interna a fin de atender mayores exigencias a la población.





	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

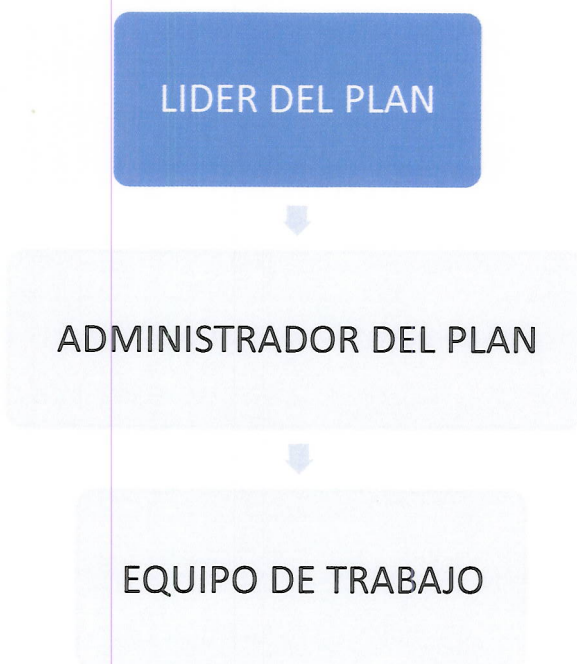
### 2.3. Organización del Plan de Contingencia

Uno de los aspectos que evidencia un carácter formal y serio en toda la entidad es que ésta se encuentre siempre preparada para afrontar cualquier evento de contingencia o dificultades en general y que le permitan poder superarlos por lo menos de manera transitoria mientras dure dicho evento.

Es necesario entonces que la definición de un Plan de Contingencia informático deba hacerse de manera formal y responsable de tal forma que involucre en mayor o menor medida a toda la entidad en el Plan de Prevención, Ejecución y Recuperación, pero definiendo un grupo responsable para su elaboración, validación y mantenimiento.

Por lo que se propone la siguiente organización según la estructura siguiente:

#### 2.3.1. Talento Humano



#### Líder del Plan:

- Sub Gerente de Desarrollo Institucional y Tecnologías de la Información.

#### Administrador del Plan:


- Jefe del Área de Tecnologías de la Información.

#### Equipo de Trabajo:

- Área de Tecnologías de la Información.
- Área de Soporte Técnico.





	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

- Dirección Regional de Administración.
- Otras áreas si amerita el caso.

#### A. DEL LÍDER DEL PLAN

- Dirigir el desarrollo integral del plan, así como verificar el cumplimiento de las actividades encargadas al Administrador del Plan y cada uno de los responsables del Equipo de Trabajo.

#### B. DEL ADMINISTRADOR DEL PLAN

- Desarrollar el Plan de Trabajo establecido
- Asignar los responsables, así como las prioridades para el desarrollo de las tareas.
- Organizar el proyecto y orientar al equipo de trabajo.
- Establecer coordinaciones entre el Equipo de trabajo, el Líder del Proyecto y las demás Unidades Orgánicas involucradas.
- Verificar y efectuar el seguimiento para que el proyecto sea expresado en documentos formales y de fácil entendimiento.
- Identificar los problemas, desarrollar las soluciones y recomendar aquellas acciones específicas.
- Controlar el avance del proyecto.
- Informar al Líder del Proyecto, los avances y ocurrencias durante el cumplimiento de las tareas de los responsables.

#### C. DEL EQUIPO DE TRABAJO


- Ejecutar las acciones encargadas y especificadas en el cronograma o plan de trabajo, cumpliendo los plazos señalados a fin de no alterar el cumplimiento de las demás tareas.
- Comunicar oportunamente al Administrador del Plan, sobre los avances de las tareas asignadas, así como las dificultades encontradas y la identificación de los riesgos.
- Identificar sobre aspectos operativos no contemplados en el Cronograma de actividades.

Ejecutar las acciones correctivas del caso, coordinando su implementación con el Administrador del Plan.

#### 2.4. Servicios y/o Bienes Producidos

EL Gobierno Regional de Huancavelica a través de la Sub Gerencia de Desarrollo Institucional, brinda servicios informáticos para usuarios internos y externos. Dentro de los servicios internos tenemos los sistemas SIGA, SIAF, SUP, SISGEDO, Control de Cheques, Controlador de Dominio, etc; y como servicios externos el portal web institucional.



	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

## 2.5. Inventario de Recursos Informáticos

### Servidores en el Gobierno Regional de Huancavelica Sede Central y Gerencias Sub Regionales

DESCRIPCIÓN	CANTIDAD
Servidor de Base de Datos	7
Servidor Firewall/Proxy	6
Servidor Web	3
Servidor de Correo Electrónico	1
Servidor de Dominio	2
Servidor Firewall Frontal	1
Servidor de telefonía IP	3
Servidor SIGA	1
Servidor SIAF	1
Servidor firewall/VPN	1
Servidor SUP	1
<b>TOTAL</b>	<b>27</b>


### Equipamiento Informático en el Gobierno Regional de Huancavelica Sede Central

Tipo	CANTIDAD
Computadoras de escritorio	420
Computadoras portátiles	252
<b>TOTAL</b>	<b>672</b>

### Impresoras en el Gobierno Regional de Huancavelica Sede Central

TIPO	CANTIDAD
Multifuncionales	83
Inyección a tinta	22
Matriciales	18
Láser	120
Plotter	12
<b>TOTAL</b>	<b>255</b>




	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

**Otros equipos en el Gobierno Regional de Huancavelica**  
**Sede Central**


DESCRIPCION	CANTIDAD
Proyectores multimedia	107
<b>TOTAL</b>	<b>107</b>

**Software en el Gobierno Regional de Huancavelica**

Nombre	Edición	Versión	Cantidad
<b>SERVIDORES</b>			
Microsoft Windows Server 2008	Standard	2008 Release 2	12
Microsoft Windows Server 2008	Enterprise	2008 Release 2	2
Microsoft Windows Server 2008	Estándar	2008	1
Microsoft Windows Server 2008	Standard	2008	1
Microsoft Windows Server 2008	Estándar	2008	1
Microsoft Windows Server 2003	Estándar	2003	1
Microsoft Windows Server 2003	Small Bussines	2003	1
Microsoft Windows Server 2003	Estándar	2003	1
Exchange Server	Standard	2010	1
Forefront Threat Management Gateway-Per Processor	Standard	2010	2
<b>SISTEMAS OPERATIVOS DE ESCRITORIO</b>			
Microsoft Windows	Profesional	8	74
Microsoft Windows	single	8	214
Microsoft Windows	Professional	7	502
Microsoft Windows	Home Basic	7	72
Microsoft Windows	Starter	7	40
Microsoft Windows	Enterprise	7	200
Microsoft Windows	Bussines	Vista	76
Microsoft Windows	Home Basic	Vista	64
Microsoft Windows	Home Basic	Vista	26
Microsoft Windows	Home Edition	Vista	9
Microsoft Windows	Home Premiun	Vista	3
Microsoft Windows	Ultimate	Vista	1
Microsoft Windows *	Starter	Vista	200
Microsoft Windows	Home Edition	XP	6
Microsoft Windows	Professional	XP	103
Microsoft Windows	-	Millenium	3
Microsoft Windows	Sec Edicion	98	2

	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

OFIMATICA				
Microsoft Office	Hogar y Empresa	2016		1
Microsoft Office	Hogar y Empresa	2013		128
Microsoft Office	Estudiante	2013		262
Microsoft Office *	Professional	Plus 2010		200
Microsoft Office	Standard	2010		4
Microsoft Office	Hogar y Pequeña Empresa	2010		15
Microsoft Office	Professional	2010		3
Microsoft Office	Home	2007		2
Microsoft Office	Small Bussines	2007		245
Microsoft Office	Hogar y Estudiantes	2007		13
Microsoft Office	Basic	2007		5
Microsoft Office	Standard	2007		150
Microsoft Office	Office SB Edition With BCM	2003		1
Microsoft Office Outlook	-	2003		1
Adobe Acrobat	Estándar	5		1
BASE DE DATOS				
SQL Server-1 Processor	Standard	2008 Release 2		1
SQL Server-1 Processor	Standard	2008		1
ANTIVIRUS				
NOD32 Antivirus	ESET NOD32 Antivirus	5		700
LICENCIAS DE ACCESO PARA CLIENTES				
Exchange Server CAL Device CAL	Standard	2007		500
Microsoft Windows Small Bussines Server CAL	-	2003		15
Windows Remote Desktop Services - User CAL	-	2008 Release 2		20
Windows Server - Device CAL	-	2008		20
Windows Server - User CAL	-	2008		820
OTROS				
DIREC-CAD	Full	2009		5
DLT-CAD	Full	2006		1
DLT-CAD	Lite	2006		5
DRS-CAD	-	2		1
FDCGRD	-	1.01		1
WINFDC	Llave fisica SSD5411-32Bits Rainbow	2.02		4
Melisa	Cooperativa	2.0		1
Clarisa	Cooperativa	1.0		1
TCMS	No Indica	2.2		8
* Licencias adquiridas para Centros Educativos				<b>4752</b>

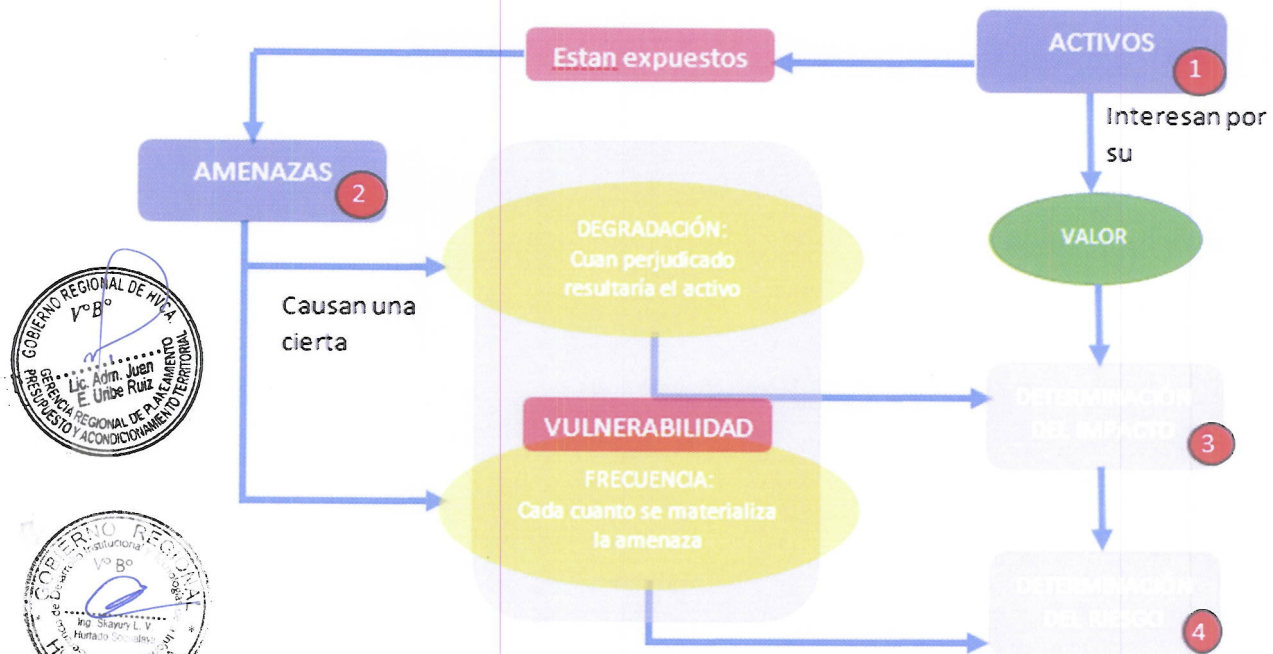
	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

### Conectividad en el Gobierno Regional de Huancavelica


Nombre	Descripción	Cantidad
Switch	3Com 48 Puertos	09
Switch	3Com 24 Puertos	11
Switch	HP 24 Puertos	03
Switch	HP 48 Puertos	03
Switch	D-LINK 28 Puertos	28
Switch	HP poe 24 Puertos	01
Access Point	3Com Access Point 7760	01
Access Point	3Com OfficeConnect®	02
Switch	3Com Switch 4200G 24 Puertos	01
<b>TOTAL</b>		<b>59</b>

## 3. IDENTIFICACIÓN DE RIESGOS

### 3.1. Análisis de Riesgos



Al igual que cualquier organización y/o empresa, el Gobierno Regional de Huancavelica, está expuesta a múltiples riesgos razón por la cual debe considerar y dar importancia a los cambios o alteraciones que lleguen a afectar los activos informáticos evitando acciones negativas al normal funcionamiento.

	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAMELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

Este es la parte crítica y quizás la razón de ser de MAGERIT versión 3.0, es que ofrece un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones para de esta forma implementar las medidas de control más adecuadas que permitan tener los riesgos mitigados. Además de esto, cuenta con todo un documento que reúne técnicas y ejemplos de cómo realizar el análisis de riesgos. Además, es que esta metodología concuerda con la Norma ISO 27005 para la gestión de riesgos.

### 3.1.1. Caracterización y Valoración de los Activos


#### Identificación de Activos.

Los activos presentes en el gobierno regional de Huancavelica, son identificados y clasificados tomando como base el Libro II de la metodología MAGERIT versión 3, en donde nos presenta el catálogo de elementos (Ver Anexo A):

Tabla 01: Activos de información

TIPO	NOMBRE DEL ACTIVO
<b>SOFTWARE - APLICACIONES INFORMATICAS</b>	1. [SIAF] Sistema Integrado de Administración Financiera 2. [SIGA] Sistema Integrado de Gestión Logística 3. [SIGGEDO] Sistema de Gestión Documentaria 4. [SO] Sistema Operativo. 5. [EMAIL] Correo Electrónico Institucional. 6. [WWW] Portal Web Institucional 7. [ANT_VIR] Anti virus
<b>SERVICIOS</b>	8. [SV_WEB] Servidor Sitios Web. 9. [SV_SIGGEDO] Tramite documentario 10. [SV_PROXY] Servidor Proxy (Internet). 11. [SV_CS] Controlador de Dominio (DNS) 12. [SV_email] Correo Electrónico Institucional 13. [SV_VoIP] Telefonía IP 14. [SV_CAM] Servidor Cámaras IP
<b>REDES COMUNICACIONES</b>	15. [RC_ADSL] Internet Speedy Telefónica 16. [RC_INFOINTERNET] Línea dedicada Telefónica 17. [RC_TELEFONIA FIJA] Líneas telefónicas fijas 18. [RC_TELEFONIA MOVIL ] líneas telefónicas móviles
<b>EQUIPAMIENTO INFORMÁTICO</b>	19. [HW_SRVF] Servidores físicos 20. [HW_SRVV] Servidores virtuales 21. [HW_UTM] Firewall / Equipo Unificado contra Amenazas. 22. [HW_NAS] Sistema de almacenamiento en Red 23. [HW_PC] Equipos de computo 24. [HW_SWC] Switchs Core 25. [HW_ROUTER] Router de voz 26. [HW_SW] Switchs distribución 27. [HW_AP] Access Point
<b>EQUIPAMIENTO</b>	28. [CAB_RED] Cableado de Red



	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAREVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

<b>AUXILIAR</b>	29. [UPS] Sistema de Alimentación Ininterrumpida. 30. [HW_BK] Robot de cintas
<b>INSTALACIONES</b>	31. [DC] Data Center
<b>PERSONAL</b>	32. [ADM_SYS] administradores de sistemas 33. [ADM_COM] administradores de comunicaciones 34. [DBA] administradores de BBDD 35. [ST] encargado de soporte técnicos informático.

### Valoración de los Activos

Para realizar el proceso de valoración de activos de acuerdo a la metodología MAGERIT Versión 3; se usa las siguientes dimensiones.

- [D] disponibilidad
- [I] integridad de los datos
- [C] confidencialidad de la Información.
- [A] Autenticidad
- [T] trazabilidad

Las dimensiones se utilizan para valorar las consecuencias de la materialización de la amenaza. La valoración que recibe un activo en una cierta dimensión es la medida del perjuicio para la organización si el activo se ve dañado en dicha dimensión.

Tabla 02: Escala de valoración activos

Valor			Criterio
10	Extremo	E	Daño extremadamente grave.
9	Muy Alto	MA	Daño Muy grave.
6-8	Alto	A	Daño grave.
3-5	Medio	M	Daño importante.
1-2	Bajo	B	Daño Menor.
0	Despreciable	D	Irrelevante a efectos prácticos.

Fuente: Magerit V.3 - Libro II - Catálogo de Elementos


### Valoración de Activos Tipo: Aplicaciones Informáticas

Tabla 03: Valoración activos tipo: aplicaciones

Activo	Dimensiones de Seguridad				
	[D]	[I]	[C]	[A]	[T]
[SIAF] Sistema Integrado de Administración Financiera (1)	[MA]	[E]	[B]	[B]	[B]
[SIGA] Sistema Integrado de Gestión Logística (2)	[MA]	[MA]	[B]	[B]	[ ]
[SISGEDO] Sistema de Gestión Documentaria (3)	[MA]	[MA]	[B]	[B]	[B]
[BIOMETRICO] Sistema de Registro y Control Biométrico (4)	[M]	[A]	[B]	[B]	[B]
[SO] Sistema Operativo (5)	[MA]	[A]			
[ANT_VIR] Antivirus (6)	[A]				

(1) y (2) [6.pi1] Probablemente afecte gravemente a un grupo de individuos.

[5.lro] Probablemente cause un incumplimiento grave de una ley o regulación.

	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

- [7.da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones.
- [7.cei.c] Causa de graves pérdidas económicas.
- [7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística.
- [7.adm] Probablemente impediría la operación efectiva de la Organización.
- [1.lg] Pudiera causar una pérdida menor de la confianza dentro de la organización

- (3) [6.pi1] Probablemente afecte gravemente a un grupo de individuos.
- [5.lro] Probablemente cause un incumplimiento grave de una ley o regulación.
- [7.da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones.
- [7.adm] Probablemente impediría la operación efectiva de la Organización.
- [1.lg] Pudiera causar una pérdida menor de la confianza dentro de la organización.
- (4) [4.pi1] Probablemente afecte a un grupo de individuos.
- [1.lro] Pudiera causar el incumplimiento leve o técnico de una ley o regulación.
- (5) [4.pi1] Probablemente afecte a un grupo de individuos.
- [3.da] Probablemente cause la interrupción de actividades propias de la Organización
- [7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística.
- (6) [7.si] Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves.
- [7.da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones

**Valoración de Activos Tipo: Servicios**


Tabla 04 Valoración activos tipo: servicios

Activo	Dimensiones de Seguridad				
	[D]	[I]	[C]	[A]	[T]
[WWW] Portal Web Institucional.(7)	[A]	[MA]			
[EMAIL] Correo Electrónico Institucional.(8)	[MA]	[MA]	[MA]	[A]	
[SIGGEDO] SIGGEDO.(9)	[MA]	[MA]	[D]	[A]	[A]
[PROXY] Servidor Proxy (Internet).(10)	[A]				
[DOMINIO] Controlador de Dominio (DNS)(11)	[MA]	[MA]		[MA]	[A]
[VoIP] Telefonía IP. (12)	[A]				

- (7) [4. pi2] Probablemente afecte a un grupo de individuos.
- [7.lro] Probablemente cause un incumplimiento grave de una ley o regulación.
- [1.da] Pudiera causar la interrupción de actividades propias de la Organización.
- (8) [4.pi2] Probablemente afecte a un grupo de individuos.
- [1.da] Pudiera causar la interrupción de actividades propias de la Organización.





	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0


- (9) [6.pi1] Probablemente afecte gravemente a un grupo de individuos.  
 [7.da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones.  
 [7.adm] Probablemente impediría la operación efectiva de la Organización.
- (10) [4.pi1] Probablemente afecte a un grupo de individuos  
 [9.da] Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones.  
 [3.adm] Probablemente impediría la operación efectiva de una parte de la Organización.
- (11) [6.pi1] Probablemente afecte gravemente a un grupo de individuos.  
 [7.da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones.  
 [7.adm] Probablemente impediría la operación efectiva de la Organización.
- (12) [4.pi1] Probablemente afecte a un grupo de individuos.  
 [3.da] Probablemente cause la interrupción de actividades propias de la Organización.  
 [3.adm] probablemente impediría la operación efectiva de una parte de la Organización.

#### Valoración de Activos Tipo: Redes de Comunicaciones

Tabla 05: Valoración activos tipo: redes de comunicaciones

Activo	Dimensiones de Seguridad				
	[D]	[I]	[C]	[A]	[T]
[RC_ADSL] Internet Speedy (13)	[MA]				
[RC_INFOINTERNET] Línea dedicada (IP Publicas)(14)	[MA]				
[RC_TELEFONIA FIJA] Líneas telefónicas fijas (15)	[MA]				
[RC_TELEFONIA MOVIL] Líneas telefónicas móviles (16)	[MA]				

- (13) [4.pi1] Probablemente afecte a un grupo de individuos.  
 [9.da] Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones.  
 [3.adm] probablemente impediría la operación efectiva de una parte de la Organización.
- (14) [6.pi1] Probablemente afecte gravemente a un grupo de individuos.  
 [9.da] Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones.  
 [7.adm] Probablemente impediría la operación efectiva de la Organización.

	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAMELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

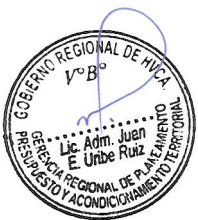
- (15) [4.pi1] Probablemente afecte a un grupo de individuos.
- [5.da] Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones.
- [1.adm] Pudiera impedir la operación efectiva de una parte de la Organización.

**Valoración de Activos Tipo: Equipamiento Informático**

Tabla 06: Valoración activos tipo: equipamiento informático

Activo	Dimensiones de Seguridad				
	[D]	[I]	[C]	[A]	[T]
[HW_SRVF] Servidores físicos (19)	[MA]	[MA]	[M]	[MA]	[A]
[HW_SRVV] Servidores virtuales (20)	[MA]	[M]	[M]	[M]	[M]
[HW_UTM] Firewall / Equipo Unificado contra Amenazas. (21)	[MA]	[M]	[MA]	[M]	[A]
[HW_NAS] Sistema de almacenamiento en Red. (22)	[MA]	[M]	[A]		
[HW_PC] Equipos de cómputo. (23)	[B]	[B]	[B]		[B]
[HW_SWC] Switchs Core. (24)	[MA]	[B]	[B]	[M]	[M]
[HW_ROUTER] Router de voz (25)	[M]	[M]	[M]		
[HW_SW] Switchs distribución. (26)	[B]	[B]	[B]		
[HW_AP] Access Point. (27)	[A]	[A]	[A]		[A]

- (19) [4.pi1] Probablemente afecte a un grupo de individuos.
- [4.pi2] Probablemente quebrante leyes o regulaciones.
- [9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios.
- [3.da] Probablemente cause la interrupción de actividades propias de la Organización.
- [7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística.
- [5.adm] Probablemente impediría la operación efectiva de más de una parte de la Organización.
- [7.lg.b] Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general.




- (20) [4.pi1] Probablemente afecte a un grupo de individuos.
- [3.lro] Probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
- [3.da] Probablemente cause la interrupción de actividades propias de la Organización.



- (21) [4.pi1] Probablemente afecte a un grupo de individuos.
- [5.lro] Probablemente sea causa de incumplimiento de una ley o regulación.
- [3.da] Probablemente cause la interrupción de actividades propias de la Organización.



	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAMELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización.

- (22) [4.pi1] Probablemente afecte a un grupo de individuos.  
 [7.si] Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves.  
 [3.da] Probablemente cause la interrupción de actividades propias de la Organización.  
 [1.adm] Pudiera impedir la operación efectiva de una parte de la Organización.

(23) y (24) [3.pi1] Probablemente afecte a un individuo.

- (25) [4.pi1] probablemente afecte a un grupo de individuos.  
 [7.si] Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación.

[3.da] Probablemente cause la interrupción de actividades propias de la Organización.

[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística.

[7.adm] Probablemente impediría la operación efectiva de la Organización.

(26) y (27) [4.pi1] Probablemente afecte a un grupo de individuos.

[7.si] Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves.

[3.da] Probablemente cause la interrupción de actividades propias de la Organización.

[1.adm] P udiera impedir la operación efectiva de una parte de la Organización.

### Valoración de Activos Tipo: Equipamiento Auxiliar

Tabla 07: Valoración activos tipo: Equipamiento informático

Activo	Dimensiones de Seguridad				
	[D]	[I]	[C]	[A]	[T]
[CAB_RED] Cableado de Red (28)	[A]	[M]			[M]
[FA_UPS] Sistema de Alimentación Ininterrumpida. (29)	[M]				
[HW_BK] Robot de cintas. (30)	[M]				

26(28) [4.pi1] Probablemente afecte a un grupo de individuos.


[3.si] Probablemente sea causa de una disminución en la seguridad o dificulte la investigación de un incidente.

[7.cei.d] Proporciona ganancias o ventajas desmedidas a individuos u organizaciones.

[7.da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones.

[6.po] Probablemente cause manifestaciones, o presiones significativas.



	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística.

[7.adm] Probablemente impediría la operación efectiva de la Organización.

- (29) [4.pi1] probablemente afecte a un grupo de individuos  
 [3.si] probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente  
 [3.adm] probablemente impediría la operación efectiva de una parte de la Organización  
 [6.po] Probablemente cause manifestaciones, o presiones significativas.
- (30) [4.pi1] Probablemente afecte a un grupo de individuos.  
 [3.si] Probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente.

#### Valoración de Activos Tipo: Instalaciones

Tabla 08: Valoración activos tipo: instalaciones

Activo	Dimensiones de Seguridad				
	[D]	[I]	[C]	[A]	[T]
[DC] Data Center (31)	[MA]	[MA]			[M]


- (31) [7.lro] Probablemente cause un incumplimiento grave de una ley o regulación.  
 [9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios.  
 [9.cei.b] De muy elevado valor comercial.  
 [9.da2] Probablemente tenga un serio impacto en otras organizaciones  
 [7.adm] probablemente impediría la operación efectiva de la Organización.  
 [79.lg.b] Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con el público en general.

#### Valoración de Activos Tipo: Personal

Tabla 09: Valoración activos tipo: personal

Activo	Dimensiones de Seguridad				
	[D]	[I]	[C]	[A]	[T]
[ADM_SYS] administradores de sistemas (32)	[E]		[MA]		
[ADM_COM] administradores de comunicaciones (33)	[E]	[MA]	[MA]	[MA]	[A]
[DBA] administradores de BBDD (34)	[E]	[A]	[A]	[A]	[A]
[ST] encargado de soporte técnicos informático. (35)	[MA]	[A]	[A]	[A]	[A]

- (32) [6.pi1] Probablemente afecte gravemente a un grupo de individuos.  
 [7.si] Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves.  
 [3.cei.d] Facilita ventajas desproporcionadas a individuos u organizaciones.

	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

[7.da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones.

[5.da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones.

[6.po] Probablemente cause manifestaciones, o presiones significativas.

[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística.

[5.adm] Probablemente impediría la operación efectiva de más de una parte de la Organización.

[7.lg.b] Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general.

(33) [6.pi1] Probablemente afecte gravemente a un grupo de individuos.

[9.lro] Probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación.

[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios.

[9.cei.b] De muy elevado valor comercial.

[9.da] Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones.

[3.po] Causa de protestas puntuales.

[10.olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística

[7.adm] Probablemente impediría la operación efectiva de la Organización.

[9.lg.b] Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con el público en general.

[4.crm] Dificulte la investigación o facilite la comisión de delitos.



(34) [4.pi1] Probablemente afecte a un grupo de individuos.

[7.si] Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves.

[9.da] Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones.

[6.po] Probablemente cause manifestaciones, o presiones significativas.

[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística.


[7.adm] Probablemente impediría la operación efectiva de la Organización.



(35) [4.pi1] Probablemente afecte a un grupo de individuos.

[7.si] Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves.



	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

- [9.da] Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones.
- [5.olm] Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local.
- [3.adm] Probablemente impediría la operación efectiva de una parte de la Organización.
- [2.lg] Probablemente cause una pérdida menor de la confianza dentro de la Organización.

### 3.1.2. Caracterización y Valoración de los Activos

El objetivo de esta actividad es determinar la degradación del activo; proceso que consiste en evaluar el valor que pierde el activo (en porcentaje) en caso que se materialice una amenaza.

Estas Amenazas se han tomado del catálogo de elementos que presenta la metodología MAGERIT en su libro II Versión 3.0.

Para el desarrollo de esta actividad es necesario tener presente los rangos dados en los siguientes cuadros tanto de frecuencia como de degradación.

#### Frecuencia de Amenazas

Tabla 10: Valor frecuencia de amenazas

	Valor		Criterio
4	Muy frecuente	MF	A diario
3	Frecuente	F	Mensualmente
2	Normal	FN	Una vez al año
1	Poco frecuente	PF	Cada varios años

Fuente: Magerit V.3 - Libro II - Catálogo de Elementos

#### Degradación de las Amenazas

Tabla 11: Valor degradación de amenazas


Valor	Criterio	
100%	MA	Degradación MUY ALTA del activo
80%	A	Degradación ALTA considerable del activo
50%	M	Degradación MEDIANA del activo
10%	B	Degradación BAJA del activo
1%	MB	Degradación MUY BAJA del activo

Fuente: Magerit V.3 - Libro II - Catálogo de Elementos

#### Identificación y Valoración de Amenazas Tipo: Aplicaciones Informáticas

Tabla 12: Valoración de Amenazas Tipo: Aplicaciones Informáticas

Activo / Amenaza	Frecuencia	Dimensiones de seguridad				
		D	I	C	A	T
[E.1] Errores de los usuarios	F	B	B			

	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAMELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

[E.2] Errores del administrador	FN	M				
[E.4] Errores de configuración	FN	A				
[E.14] Escapes de información	PF			A		
[E.18] Destrucción de información	PF	MA		A		
[A.5] Suplantación de la identidad del usuario	MF		A	A	A	
[A.11] Acceso no autorizado	PF	M	A	A	A	
[A.15] Modificación de la información	PF		MA			

### Justificación de Amenazas – Aplicaciones Informáticas

**[E.1] Errores de los usuarios:** Se considera que este tipo de amenaza llegue a presentarse frecuentemente debido a que los usuarios o personal nuevo no es capacitado adecuadamente en el uso de los activos “aplicaciones informáticas” y su degradación es considerada de muy alto impacto en la dimensión de Disponibilidad por que dichos activos están directamente relacionados con los servicios y el modelo de negocio de la institución.

**[E.2] errores del administrador:** Se da un valor ALTO, ya que si llegase a presentar un “error del administrador” la disponibilidad de las aplicaciones y servicios que ellos soportan se verá seriamente afectada y debido a que el personal encargado de la administración de estas aplicaciones es altamente calificado; la probabilidad de ocurrencia en POCO FRECUENTE.

**[E.4] Errores de configuración:** Se valora como de ALTA degradación porque debido a una mala configuración en los activos pertenecientes a las aplicaciones informáticas llevaría a ataques como intrusión, denegación de servicios, robo de información, etc. Afectando directamente el corazón informático de la Institución llevándola a una suspensión de los servicios ofrecidos.

**[E.14] Escapes de información:** Se considera que la afectación sería Alta para la dimensión de Confidencialidad, ya que si hay escape de información esta puede ser modificada o usada para beneficios propios llevando a pérdida de confianza Institucional.


**[E.18] Destrucción de información:** Dado el caso de llegarse a presentar esta amenaza las dimensiones más afectadas son la Disponibilidad y la Confidencialidad, porque los activos de las aplicaciones informáticas guardan toda la información que se maneja a diario dentro de los procesos de la Institución.

**[A.5] Suplantación de la identidad del usuario:** Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente, afecta la confidencialidad, autenticidad e integridad.

**[A.11] Acceso no autorizado.** La dimensión que afecta directamente es la Disponibilidad y se considera muy alta porque al presentarse una intrusión desencadenaría la materialización de las amenazas [E.14], [E.18] y [A.15] entre otras.

**[A.15] Modificación de la información:** Afectará directamente la dimensión de integridad en un nivel muy alto, porque de presentarse ataques de modificación de información se van a ver alterados los datos almacenados en los activos pertenecientes a este grupo, causando un caos informático y arrojando datos erróneos a la hora de las



	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

consultas y transacciones en cada uno de los procesos normalizados dentro de las labores institucionales.

### Identificación y Valoración de Amenazas Tipo: Servicios

Tabla 13: Valoración de Amenazas Tipo: servicios

Activo / Amenaza	Frecuencia	Dimensiones de seguridad				
		D	I	C	A	T
[E.20] Vulnerabilidades de los programas	PF	MA				
[A.5] Suplantación de la identidad del usuario	FN			A	A	
[A.8] Difusión de Software dañino	F	A		M	M	
[A.24] Denegación de Servicios	PF	MA				

### Justificación de Amenazas – Servicios

**[E.20] Vulnerabilidades de los programas:** La probabilidad de ocurrencia se consideró como PF y que afectará directamente la disponibilidad por qué; los programas usados para dar soporte a los servicios implementados en la Institución primero son evaluados en ambientes de prueba antes de ponerlos en funcionamiento. Pero en caso de sufrir un ataque por esta amenaza se experimentaría una suspensión de los servicios en un nivel muy alto, cerca al 100%.

**[A.5] Suplantación de la identidad del usuario:** Este es quizá una de las mayores amenazas visibles dentro de los servicios que ofrece la Institución debido a que no se han implementado normativas para el uso de contraseñas fuertes para el acceso a los servicios, por lo que se puede presentar con mucha frecuencia.

**[A.8] Difusión de Software dañino:** Esta amenaza es considerada de alto grado de degradación y que pudiese presentar en un nivel de frecuencia normal; con afectación directa a la disponibilidad; debido a la gran cantidad de equipos de cómputo que están destinados al personal de la institución y por la falta de concientización sobre el uso de internet y cuidados en el uso de medios extraíbles que pueden traer malware y virus informáticos.

**[A.24] Denegación de Servicio,** Se ha valorado de muy alta degradación en la dimensión de disponibilidad, porque debido a falta de recursos a nivel de hardware y redes de comunicaciones provocan que los servicios no estén disponibles para todos los usuarios de los sistemas, pero con poca frecuencia de ocurrencia.


### Identificación y Valoración de Amenazas Tipo: Redes de Comunicaciones.

Tabla 14: Valoración de Amenazas Tipo: Redes de Comunicaciones

Activo / Amenaza	Frecuencia	Dimensiones de seguridad				
		D	I	C	A	T
[N.1] Fuego	PF	MA				
[N.*] Desastres Naturales	PF	MA				
[I.8] Fallo de Servicio de comunicaciones	F	A				





	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

### Justificación de Amenazas – Redes de Comunicaciones

**[N.1] Fuego:** los incendios sean provocados o accidentales pueden cortar las líneas físicas de Internet o telefonía fija, es muy poco frecuentes pero causaría una deflagración muy alta del activo.

**[N.\*] Desastres Naturales:** Incidentes que se producen sin intervención humana: lluvias, inundaciones, rayos, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, ... Se puede llegar a cortar los servicios de comunicaciones afectando la disponibilidad de los activos de redes de comunicaciones tendría un detrimento muy alto porque, causarían que se caigan todos los servicios llevando a una paralización total de las actividades en los procesos.

**[I.8] Fallo de Servicio de comunicaciones:** El activo de redes de comunicaciones se ha calificado con grado de afectación en la disponibilidad de nivel Alto y frecuente, debido a que actualmente se cuenta con un solo proveedor de Servicios de internet, telefonía fija y celular y se presentan fallas continuas que duran horas.

### Identificación y Valoración de Amenazas Tipo: Desastres Naturales

Tabla 15: Valoración de Amenazas Tipo: Desastres Naturales

Activo / Amenaza	Frecuencia	Dimensiones de seguridad				
		D	I	C	A	T
[N.1] Fuego	PF	MA				
[N.2] Daños por agua	PF	MA				
[N.*] Desastres Naturales	PF	MA				

### Justificación de Amenazas – Desastres Naturales

**[N.1] Fuego:** los incendios sean provocados o accidentales pueden acarrear la posibilidad de que el fuego acabe con recursos del sistema.

**[N.2] Daños por agua:** Posibilidad de que el agua acabe con recursos del sistema.

**[N.\*] Desastres Naturales:** Incidentes que se producen sin intervención humana: lluvias, inundaciones, rayos, tormenta eléctrica, terremoto, etc; acabe con los recursos del sistema

### Identificación y Valoración de Amenazas Tipo: Equipamiento Auxiliar

Tabla 16: Valoración de Amenazas Tipo: Equipamiento Auxiliar

Activo / Amenaza	Frecuencia	Dimensiones de seguridad				
		D	I	C	A	T
[N.1] Fuego	PF	MA				

### Justificación de Amenazas – Equipamiento Auxiliar

**[N.1] Fuego:** los incendios sean provocados o accidentales pueden acarrear la posibilidad de que el fuego acabe con recursos del sistema.

### Identificación y Valoración de Amenazas Tipo: Instalaciones




	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

Tabla 17: Valoración de Amenazas Tipo: Instalaciones

Activo / Amenaza	Frecuencia	Dimensiones de seguridad				
		D	I	C	A	T
[N.1] Fuego	PF	MA				
[N.2] Daños por agua	PF	MA				
[N.*] Desastres Naturales	PF	MA				

#### Justificación de Amenazas –Instalaciones

**[N.1] Fuego:** los incendios sean provocados o accidentales pueden acarrear la posibilidad de que el fuego acabe con recursos del sistema.

**[N.2] Daños por agua:** Posibilidad de que el agua acabe con recursos del sistema.

**[N.\*] Desastres Naturales:** Incidentes que se producen sin intervención humana: lluvias, inundaciones, rayos, tormenta eléctrica, terremoto, etc; acabe con los recursos del sistema

#### Identificación y Valoración de Amenazas Tipo: Personal

Tabla 18: Valoración de Amenazas Tipo: Personal

Activo / Amenaza	Frecuencia	Dimensiones de seguridad				
		D	I	C	A	T
[E.28] Indisponibilidad de personal	FN	MA				

#### Justificación de Amenazas –Personal

**[E.7] Deficiencias en la organización:** cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión.


Acciones descoordinadas, errores por omisión, etc.

### 3.1.3. Tablas de Amenazas vs Vulnerabilidades

#### Desastres Naturales [DesN]

[DesN.1] Fuego	
Tipo de Activos: [HW] Equipos Informáticos (hardware) [SI] Soportes de Información [EAUX] Equipamiento Auxiliar	Dimensiones: [Dis] Disponibilidad
<b>Descripción:</b>	
Incendios: Existe el riesgo de que un corto circuito provoque un incendio y el fuego dañe los equipos informáticos de la institución.	
<b>Vulnerabilidades:</b>	
<ul style="list-style-type: none"> <li>No existen sensores de humo o alarma contra incendios.</li> <li>No existen suficientes extintores de incendios, o no están distribuidos en los sitios claves de manejo de información.</li> <li>Los usuarios no cumplen con dejar apagado sus computadores de</li> </ul>	



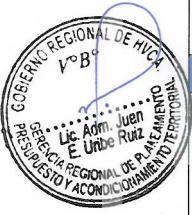
	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

escritorio y demás equipos informáticos.

- No hay procedimientos de emergencia ante un incendio. Existe la posibilidad de lluvias torrenciales que deterioren los equipos informáticos en meses críticos de cierre de ejecución presupuestal.

[DesN.2] Daños por agua	
Tipo de Activos: [HW] Equipos Informáticos (hardware) [SI] Soportes de Información	Dimensiones: [Dis] Disponibilidad
Descripción:	
Inundaciones: Posibilidad de que el agua dañe por completo los recursos del sistema	
Vulnerabilidades:	
<ul style="list-style-type: none"> <li>Las instalaciones sanitarias no reciben un adecuado mantenimiento preventivo en la institución.</li> <li>Existe la posibilidad de lluvias torrenciales que deterioren los equipos informáticos en meses críticos de cierre de ejecución presupuestal.</li> </ul>	


[DesN.3] Fallo de servicios de comunicaciones	
Tipo de Activos: [COM] redes de comunicaciones	Dimensiones: [Dis] Disponibilidad
Descripción:	
cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente.	
Origen: Entorno (accidental) Humano (accidental o deliberado)	
Vulnerabilidades:	
<ul style="list-style-type: none"> <li>Las instalaciones sanitarias no reciben un adecuado mantenimiento preventivo en la institución.</li> <li>Existe la posibilidad de lluvias torrenciales que deterioren los equipos informáticos en meses críticos de cierre de ejecución presupuestal.</li> </ul>	



**Errores y fallos no intencionados [E.N]**

[E.1] Indisponibilidad del personal	
Tipo de Activos: [ADM_SYS] Administrador de Sistemas. [ADM_COM] Administrador de redes de comunicación	Dimensiones: [Dis] Disponibilidad
Descripción:	
Servicios informáticos paralizados (parcial o total) por ausencia de personal especialista en el puesto de trabajo.	



	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAMELICA</b>	Fecha: Noviembre 2016
		Versión:1.0


<b>Vulnerabilidades:</b> <ul style="list-style-type: none"> <li>El administrador de la red de comunicaciones es la única persona que conoce al detalle la infraestructura tecnológica de la entidad.</li> <li>Los administradores de los sistemas críticos de la entidad (SIGA, SIAF y SIGEDO), son personales con contrato temporal.</li> </ul>
--

**Amenazas de origen industrial [Indus.]**

<b>[Indus.1] Corte del Suministro Eléctrico</b>	
[HW] Equipos Informáticos (hardware) [SI] Soportes de Información [EAUX] Equipamiento Auxiliar	Dimensiones: [Dis] Disponibilidad
<b>Descripción:</b> Corte total o parcial de energía eléctrica en el Gobierno Regional de Huancavelica.	
<b>Vulnerabilidades:</b> <ul style="list-style-type: none"> <li>No cuentan aún con un generador de energía eléctrica para este tipo de emergencias.</li> <li>No todos los equipos informáticos son alimentados mediante UPS.</li> <li>Cortes de energía prolongados (más de veinte minutos) requerirán que los equipos de misión crítica de la institución sean apagados. No existirá disponibilidad de los servicios de información en la institución durante el lapso que dure el corte de energía.</li> <li>Los sistemas eléctricos podrían ser susceptibles a cortos circuitos que podrían provocar la interrupción del suministro total o parcial.</li> <li>El corte de energía podría dejar sin trabajar al personal de la empresa.</li> </ul>	

<b>[Indus.2] Degradación de los soportes de almacenamiento de la información</b>	
[SI] Soportes de Información	Dimensiones: [Dis] Disponibilidad
<b>Descripción:</b> Como consecuencia del paso del tiempo, los medios en el cual se tienen almacenados los backups de los sistemas informáticos podrían ser afectados en su forma física. (humedad, polvo entre otros aspectos)	
<b>Vulnerabilidades:</b> <ul style="list-style-type: none"> <li>No hay una ubicación adecuada para almacenar y resguardar soportes de información (medios magnéticos, medios ópticos, documentos en papel).</li> <li>Los backups se hacen en medios ópticos (DVD's, CD's y Blueray)</li> <li>Documentos en papel no se convierten a otro medio (no se digitalizan). Estos documentos son susceptibles a los daños que pueda sufrir el papel como consecuencia de un proceso de archivado inadecuado o daños provocados por el paso del tiempo.</li> </ul>	




	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

## Amenazas a Causa de Ataques Intencionados [A\_Int.]

[A_Int.1] Manipulación de la Configuración	
[D] Datos / información [SW] Aplicaciones (software) [HW] Equipos informáticos (hardware)	<b>Dimensiones:</b> 1. [I] Integridad 2. [C] Confidencialidad 3. [A_S] Autenticidad del servicio 4. [A_D] Autenticidad de los datos 7. [D] Disponibilidad
<b>Descripción:</b>	
Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.	
<b>Vulnerabilidades:</b>	
<ul style="list-style-type: none"> <li>No existe un sistema para detección de intrusos dentro de la red de información.</li> <li>No mantienen un sistema de monitoreo constante en el cual detecten notificaciones automáticas a quienes administran la red.</li> <li>Nunca han implementado un nivel de políticas de seguridad como el uso de contraseñas, y el cambio constante de estas.</li> <li>No mantienen un sistema de Active Directory u otros servicios.</li> </ul>	

[A_Int.2] Suplantación de la Identidad del Usuario	
[SW] Aplicaciones (software)	<b>Dimensiones:</b> 1. [C] Confidencialidad 2. [A_S] Autenticidad del servicio 3. [A_D] Autenticidad de los datos 4. [I] Integridad
<b>Descripción:</b>	
Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la institución o por personal contratado temporalmente.	
<b>Vulnerabilidades:</b>	
<ul style="list-style-type: none"> <li>No hay restricciones sobre la cantidad de sesiones que un usuario puede iniciar.</li> <li>Tampoco existen restricciones sobre las estaciones de trabajo sobre las cuales los usuarios pueden iniciar sesión, aun a pesar de que de manera física, cada usuario tiene asignado un puesto de trabajo y una estación de trabajo. No se han implementado a nivel de las políticas de seguridad el uso de contraseñas fuertes y el cambio obligatorio de estas en forma periódica.</li> <li>No existe dentro de la administración de usuarios, directivas o políticas que deshabilite a los usuarios que por diversas razones se ausenten de sus puestos de trabajo en periodos temporales relativamente largos, como por ejemplo cuando algún usuario está de vacaciones.</li> <li>El proceso para dar de alta y de baja a los usuarios, cuando entran a formar parte de la organización o cuando dejan de trabajar en la</li> </ul>	



	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

misma, no es automático. Hasta que se reciben las notificaciones de recursos humanos, el administrador del dominio toma las acciones correspondientes para actualizar el directorio, lo cual podría generar ciertos espacios de riesgo sobre uso no autorizado de los recursos de información.

**[A\_Int.3] Abuso de Privilegios de Acceso**

[SW] Aplicaciones (software)	Dimensiones:
[HW] Equipos Informáticos (hardware)	1. [C] Confidencialidad
	2. [I] Integridad

**Descripción:**  
Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.

**Vulnerabilidades:**

- No existen procedimientos de revisión periódica de los derechos y permisos efectivos de los usuarios, para comprobar si debido a un cambio de configuración, o a una acción errónea o indebida se le han concedido a un usuario o grupo de usuarios más derechos y permisos de los que le corresponden.
- No existen sistemas de monitorización en línea que detecten y generen alarmas y notificaciones automáticas a los administradores de red si se ejecutan cambios o alteraciones en la configuración que pudieran afectar el funcionamiento normal de los sistemas.
- No existen mecanismos de control que detecten y prevengan posibles abusos de privilegios en las aplicaciones.

**[A\_Int.4] Uso no Previsto**

[SW] Aplicaciones (software)	Dimensiones:
[HW] Equipos Informáticos (hardware)	[Dis] Disponibilidad
[SI] Soportes de Información	

**Descripción:**  
Utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.

**Vulnerabilidades:**


- No existen herramientas de control de contenido o monitorización de tráfico para el uso de Internet u otros servicios de la infraestructura de red y los sistemas de información.
- Tampoco se implementan inventarios automatizados de software y hardware para comprobar que no se hayan instalado componentes adicionales y no autorizados a los equipos de los usuarios.

**[A\_Int.5] Destrucción de la información**

[D] Datos / Información	Dimensiones:
	[Dis] Disponibilidad

**Descripción:**  
Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.



	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

Vulnerabilidades:
<ul style="list-style-type: none"> <li>• Hacen frecuentemente la realización de backup por medio de DVD's y CD's de los datos.</li> <li>• No se cuenta con un cuidado exclusivo del almacenamiento de datos por medio ópticos.</li> <li>• No se cuenta con una oficina, en la cual se pueda guardar la información de los backup's y las aplicaciones fundamentales de la empresa.</li> </ul>

### 3.1.4. Estimación Del Estado De Riesgo

Actividad realizada con el propósito de analizar los datos recopilados en las actividades anteriores y evaluar el estado de riesgo, donde se incluye la estimación de impacto y riesgo. Se toma la siguiente escala para calificar el valor de los activos, la magnitud del impacto y la magnitud del riesgo:

- MA:** muy alto
- A:** alto
- M:** medio
- B:** bajo
- MB:** muy bajo

### Estimación Del Impacto

El objetivo de esta actividad es determinar el alcance del daño producido sobre los activos de información en caso de llegarse a materializar una amenaza.


Se evalúa el grado de repercusión que pueda presentar cada activo, dentro de las dimensiones de valoración analizadas anteriormente como son: Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad, haciendo uso de la siguiente tabla de doble entrada (ver tabla) propuestas por Magerit v.3.

Los activos con calificación Media deberán ser re-evaluados para mejorar, cambiar o adaptar nuevos controles, los de calificación Alta y muy alta deberán ser objeto atención Urgente.

Tabla 19: Valores estimación de impacto

IMPACTO	DEGRADACION				
	1%	10%	50%	80%	100%
MA	M	A	A	MA	MA
A	B	M	M	A	A
M	MB	B	B	M	M
B	MB	MB	MB	B	B
MB	MB	MB	MB	MB	MB

Fuente: Magerit V.3 – Libro II - Catálogo de Elementos

	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

Impacto acumulado: es el impacto potencial al que está expuesto el sistema tomando como base los valores obtenidos de los activos y valoración de las amenazas, sin tener en cuenta las salvaguardas actuales. Estos requieren atención inmediata.


Impacto residual: es el resultado de combinar el valor de los activos, la valoración de las amenazas y la efectividad de las salvaguardas aplicadas; los activos con resultado muy bajo o bajo (o casillas en blanco), son riesgos con los que se puede convivir pero que se tuvieron en cuenta dentro de los controles, políticas de seguridad y recomendaciones.

Tabla 20: Valoración impacto en activos de información

ACTIVO	AMENAZA	IMPACTO				
		D	I	C	A	T
SOFTWARE - APLICACIONES INFORMATICAS	[E.1] Errores de los usuarios	B	B	A		
	[E.2] Errores del administrador	B				
	[E.4] Errores de configuración	M				
	[E.14] Escapes de información			A		
	[E.18] Destrucción de información	MA	MA	A		
	[A.5] Suplantación de la identidad del usuario		A	A	A	
	[A.11] Acceso no autorizado	M	A	A	A	
	[A.15] Modificación de la información		A	M	A	M
SERVICIOS	[E.20] Vulnerabilidades de los programas	A	A	A	A	
	[A.5] Suplantación de la identidad del usuario			MA	A	
	[A.8] Difusión de Software dañino	A	A	M		
	[A.24] Denegación de Servicios	MA				
REDES DE CUMUNICACION ES	[N.1] Fuego	MA				
	[N.*] Desastres Naturales	MA				
	[I.8] Fallo de Servicio de comunicaciones	MA				
EQUIPAMIEN TO INFORMATICO	[N.1] Fuego.	MA	MA			
	[I.2] Daños por Agua.	MA	MA			
	[I.5] Avería de origen físico o lógico	A				
	[E.23] Errores de mantenimiento/ actualización de equipos (hardware).	A				
	[A.11] Acceso no Autorizado.			A		
	[A.23] Manipulación de los equipos.			A		
EQUIPAMIENTO AUXILIAR	[I.5] Avería de origen físico o lógico	A				
INSTALACIONES	[A.26] Ataque destructiva	MA	MA			
PERSONAL	[E.7] Deficiencia en la organización.	A	A			
	Indisponibilidad de Personal		MA	MA		
			A	A		





	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

### Actividad A: Estimación Del Riesgo

Para realizar la estimación del riesgo se hace uso de la siguiente escala cualitativa, tomando como entradas impacto acumulado y frecuencia.

Tabla 21: valores de frecuencia.

Valor		Criterio	
100	Muy frecuente	MF	A diario
10	Frecuente	F	Mensualmente
1	Normal	FN	Una vez al año
1/10	Poco frecuente	PF	Cada varios años

Fuente: Esta Investigación

Tabla 22: Criterios de valoración para estimación de riesgo


RIESGO	FRECUENCIA				
	PF	FN	F	MF	
IMPACTO	MA	M	A	MA	MA
	A	B	A	MA	MA
	M	B	M	A	A
	B	MB	B	M	A
	MB	MB	MB	B	B

Para la estimación del riesgo se toman los valores de la frecuencia de ocurrencia de cada amenaza frente a los activos e impacto acumulado ya que estos son los activos que necesitan una acción urgente.

### Valoración de riesgo en activos de información

Tabla 23: Valoración de riesgo en activos de información

ACTIVO	AMENAZA	IMPACTO					F	RIESGO
		D	I	C	A	T		
COMUNICACIONES INFORMATICAS	[E.1] Errores de los usuarios	B	B	M			F	B
	[E.2] Errores del administrador	MA					FN	B
	[E.4] Errores de configuración	A					FN	B
	[E.14] Escapes de información			A			PF	B
	[E.18] Destrucción de información	MA	MA	A			PF	MA
	[A.5] Suplantación de la identidad del usuario		M	B	B		F	B
SERVICIOS	[A.11] Acceso no autorizado	M	A	A	A		PF	B
	[A.15] Modificación de la información		A	M	A	M	PF	B
	[E.20] Vulnerabilidades de los programas	A	A	A	A		PF	B
REDES DE COMUNICACIONES	[A.5] Suplantación de la identidad del usuario			M			FN	B
	[A.8] Difusión de Software dañino	M	M	M			F	B
	[A.24] Denegación de Servicios	MA					PF	B
REDES DE COMUNICACIONES	[N.1] Fuego	MA					PF	B
	[N.*] Desastres Naturales	MA					FN	A
	[I.8] Fallo de Servicio de comunicaciones	MA					F	A


	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

EQUIPAMIENTO INFORMATICO	[N.1] Fuego.	MA				PF	MA
	[I.2] Daños por Agua.	MA				PF	B
	[I.5] Avería de origen físico o lógico			A		PF	A
	[E.23] Errores de mantenimiento/ Actualización de equipos (hardware).			B		FN	B
	[A.11] Acceso no Autorizado.	A				FN	B
	[A.23] Manipulación de los equipos.	M	M			PF	B
EQUIPAMIENTO AUXILIAR	[I.5] Avería de origen físico o lógico	A				PF	B
INSTALACIONES	[A.26] Ataque destructiva	MA	MA			PF	MA
PERSONAL	[E.28] Indisponibilidad de personal	A	A			FN	A

Luego de realizar el análisis de riesgo en el Gobierno Regional de Huancavelica, se continúa con seleccionar de aquellas amenazas que tienen riesgos que califican con riesgo ALTO y MUY ALTO, para la toma de acciones en caso se presente una contingencia que pudiera afectar el normal desarrollo de las actividades que se realizan en la institución; para este caso en particular se toman las siguientes amenazas:

- [E.18] Destrucción de información.
- [N.\*] Desastres Naturales.
- [I.8] Fallo de Servicio de comunicaciones
- [N.1] Fuego. (Para el activo Equipamiento Informático).
- [I.5] Avería de origen físico o lógico.
- [A.26] Ataque destructiva.
- [E.28] Indisponibilidad de personal.

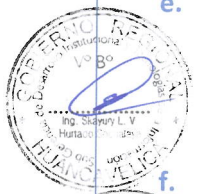



	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAMELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

#### 4. DESARROLLO DE FASES, ACTIVIDADES, ESTRATEGIA, PROGRAMAS Y POLÍTICAS

##### CONTINGENCIAS RELACIONADAS A: APLICACIONES INFORMATICAS

GOBIERNO REGIONAL DE HUANCAMELICA	Evento: DESTRUCCIÓN DE INFORMACIÓN	FPC-001
<b>1. PLAN DE PREVENCIÓN</b>		
<p><b>a. Descripción del evento</b></p> <p>La destrucción de Información es la eliminación intencional o no intencional de información por personas ligadas o no a la institución con ánimo de obtener un beneficio o causar un perjuicio, también puede producirse por fallas de equipos y/o componentes, asimismo debido al ataque de malwares o virus informáticos. Pueden afectar los siguientes activos informáticos.</p> <p><b>APLICACIONES INFORMATICAS</b></p> <ul style="list-style-type: none"> <li>• [SIAF] Sistema Integrado de Administración Financiera</li> <li>• [SIGA] Sistema Integrado de Gestión Logística</li> <li>• [SIGEDO] Sistema de Gestión Documentaria</li> <li>• [SO] Sistema Operativo.</li> <li>• [EMAIL] Correo Electrónico Institucional.</li> <li>• [WWW] Portal Web Institucional</li> <li>• [ANT_VIR] Anti virus</li> </ul> <p><b>SERVICIOS</b></p> <ul style="list-style-type: none"> <li>• [SV_WEB] Servidor Sitios Web.</li> <li>• [SV_SIGEDO] Tramite documentario</li> <li>• [SV_PROXY] Servidor Proxy (Internet).</li> <li>• [SV_CS] Controlador de Dominio (DNS)</li> <li>• [SV_email] Correo Electrónico Institucional</li> <li>• [SV_VoIP] Telefonía IP</li> </ul> <p><b>b. Objetivo</b></p> <p>Establecer las acciones que se ejecutaran ante la destrucción de la información producida de cualquier forma a fin de minimizar el tiempo de interrupción de las operaciones del Gobierno Regional de Huancavelica.</p> <p><b>c. Criticidad</b></p> <p>El Estudio determina que el presente evento tiene un MUY ALTO impacto y RIESGO medio.</p> <p><b>Entorno</b></p> <p>Este evento se puede dar en los medios de almacenamiento de datos de fácil acceso por el personal del Gobierno Regional de Huancavelica.</p> <p><b>e. Personal Encargado</b></p> <p>El Administrador de sistemas y/o Bases de datos de la Sub Gerencia de Desarrollo Institucional y Tecnologías de la Información (SGDIyTI), es quien debe dar cumplimiento a lo descrito en las Condiciones de Prevención de Riesgo del presente Plan.</p> <p><b>f. Condiciones de Prevención de Riesgo</b></p> <ul style="list-style-type: none"> <li>• Revisión periódica de los privilegios de los usuarios en los diferentes recursos de la red informática.</li> <li>• Contar con los backups periódicos de los datos de las aplicaciones en desarrollo/producción en la Institución. Se realizan copias de la información o de los registros con la finalidad de asegurar la información mantenida en la base de</li> </ul>		



	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

datos.

- Ejecución de tareas periódicas de respaldo de la información crítica: archivos, bases de datos, etc. En diferentes medios.
- Mantener actualizado los sistemas operativos, motores de bases de datos, con todos los parches del producto según el fabricante.
- Contar con servicios de soporte vigentes para los sistemas operativos y motores de bases de datos. En caso sea necesario, este soporte debe incluir actividades de prevención, revisión del sistema y mantenimiento general a la base de datos.

## 2. PLAN DE EJECUCION

### a. Eventos que activan la Contingencia

- Fallas en la conexión, Indisponibilidad del aplicativo informático.

### b. Procesos Relacionados antes del evento.

- Identificar la disponibilidad de las últimas copias de respaldo del sistema informático afectado.

### c. Personal que autoriza la contingencia.

El Administrador de sistemas, Bases de datos o Sub Gerente de la SGDIyTI pueden activar la contingencia.

### d. Descripción de las actividades después de activar la contingencia.

- Identificación de falla en la pantalla de las estaciones de trabajo y/o servidores del aplicativo informático afectado.

### e. Duración

La duración de la contingencia dependerá del tipo de daño y del sistema afectado, hasta su puesta en funcionamiento.

## 3. PLAN DE RECUPERACIÓN

### a. Personal Encargado

El Administrador de sistemas y/o Bases de datos de la SGDIyTI son los encargados de la recuperación.

### b. Descripción

- Sistemas con soporte por proveedores.- De producirse una falla al momento de la operación de estos sistemas, deberá ser comunicado y coordinado inmediatamente con el proveedor, para su corrección.
- Sistemas provistos por el Gobierno Nacional u otra entidad.- Al producirse una falla, primero el personal de soporte evaluara los daños, se efectuaran los protocolos de mantenimientos, restauración de datos, etc, particular para cada sistema (SIAF, SIGA, SOSGEDO, etc), de persistir el mal funcionamiento, se comunicara al residente del sistema y/o se comunicara con el soporte técnico especializado según sea el caso hasta lograr su puesta en funcionamiento.

### c. Mecanismos de Comprobación

Comprobación del buen funcionamiento del sistema desde el servidor donde está alojado, luego desde un equipo cliente.

### d. Desactivación del Plan de Contingencia

El Administrador de sistemas y/o Bases de datos de la SGDIyTI pone en producción el sistema afectado y se da por desactivado el plan de contingencia


### e. Proceso de Actualización

Se comunica a los Usuarios la puesta en producción del sistema afectado.

Se comprueba las tareas de respaldo de datos del sistema afectado.


Se determina las causas de la perdida de información y se realizan acciones para prevenir que se repitan hechos similares.



	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016 Versión:1.0


## CONTINGENCIAS RELACIONADAS A: REDES DE COMUNICACIONES

GOBIERNO REGIONAL DE HUANCAVELICA	Evento: FALLO DE SERVICIOS DE COMUNICACIONES	FPC-002
<b>1. PLAN DE PREVENCIÓN</b>		
<p><b>a. Descripción del evento</b></p> <p>Corte imprevisto de los servicios de comunicaciones contratados para las transmisión de datos (internet) y voz (telefonía fija). Pueden afectar los siguientes activos:</p> <p><b>APLICACIONES INFORMATICAS</b></p> <ul style="list-style-type: none"> <li>[SIAF] Sistema Integrado de Administración Financiera</li> <li>[SIGA] Sistema Integrado de Gestión Logística</li> <li>[SIGEDO] Sistema de Gestión Documentaria</li> <li>[EMAIL] Correo Electrónico Institucional.</li> <li>[WWW] Portal Web Institucional</li> <li>[ANT_VIR] Anti virus</li> </ul> <p><b>SERVICIOS</b></p> <ul style="list-style-type: none"> <li>[SV_WEB] Servidor Sitios Web.</li> <li>[SV_SISGEDO] Tramite documentario</li> <li>[SV_PROXY] Servidor Proxy (Internet).</li> <li>[SV_CS] Controlador de Dominio (DNS)</li> <li>[SV_email] Correo Electrónico Institucional</li> </ul> <p><b>b. Objetivo</b></p> <p>Establecer las acciones que se ejecutaran ante el fallo de los servicios de comunicaciones a fin de minimizar el tiempo de interrupción de las operaciones del Gobierno Regional de Huancavelica.</p> <p><b>c. Criticidad</b></p> <p>El Estudio determina que el presente evento tiene un MUY ALTO impacto y RIESGO medio.</p> <p><b>d. Entorno</b></p> <p>Este evento se puede dar en los servicios contratados a terceros por el Gobierno Regional de Huancavelica.</p> <p><b>Personal Encargado</b></p> <p>El Administrador de sistemas y/o Bases de datos de la Sub Gerencia de Desarrollo Institucional y Tecnologías de la Información (SGDlyTI), es quien debe dar cumplimiento a lo descrito en las Condiciones de Prevención de Riesgo del presente Plan.</p> <p><b>f. Condiciones de Prevención de Riesgo</b></p> <ul style="list-style-type: none"> <li>Pago de servicios en su debido momento.</li> <li>Contar con servicios de transmisión de datos (internet) alternos contratados a otro proveedor, solo para transmisión de datos críticos.</li> </ul>		
<b>2. PLAN DE EJECUCION</b>		
<p><b>a. Eventos que activan la Contingencia</b></p> <ul style="list-style-type: none"> <li>Cortes inesperados de los servicios de transmisión de datos (internet).</li> </ul> <p><b>b. Procesos Relacionados antes del evento.</b></p> <p>Comprobación del acceso a internet desde los navegadores de la LAN. Comprobación de respuesta de las pruebas de conectividad (PING) desde la LAN, hasta los servidores DNS del proveedor del servicio.</p>		

	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

<ul style="list-style-type: none"> <li>Comprobación del buen funcionamiento del router provisto por el proveedor del servicio.</li> <li>Comprobación del buen funcionamiento de los firewall, switchs y demás equipamiento de la institución.</li> </ul> <p><b>c. Personal que autoriza la contingencia.</b> El Administrador de sistemas y/o Bases de datos de la SGDlyTI pueden activar la contingencia.</p> <p><b>d. Descripción de las actividades después de activar la contingencia.</b></p> <ul style="list-style-type: none"> <li>Comunicarse con el área de reporte de averías del proveedor del servicio para determinar la causa del corte y determinar su duración.</li> </ul> <p><b>e. Duración</b> La duración de la contingencia dependerá del tiempo de respuesta y resolución de averías técnicas del proveedor del servicio afectado.</p>
<p><b>3. PLAN DE RECUPERACIÓN</b></p> <p><b>a. Personal Encargado</b> El Administrador de sistemas y/o Bases de datos de la SGDlyTI son los encargados de la recuperación.</p> <p><b>b. Descripción</b></p> <ul style="list-style-type: none"> <li>Se configurara el servicio alternativo de internet para la transmisión de datos críticos.</li> </ul> <p><b>c. Mecanismos de Comprobación</b> Comprobación del buen funcionamiento del servicio alternativo desde el lado del cliente o servidor crítico.</p> <p><b>d. Desactivación del Plan de Contingencia</b> El Administrador de sistemas y/o Bases de datos de la SGDlyTI, desactiva la contingencia cuando el servicio principal de internet se reestablezca.</p> <p><b>e. Proceso de Actualización</b></p> <ul style="list-style-type: none"> <li>Se comprueba el normal funcionamiento de los servicios de transmisión de datos (internet)</li> <li>Se desactiva el servicio alternativo de internet</li> </ul>




	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

## CONTINGENCIAS RELACIONADAS A: EQUIPAMIENTO INFORMATICO

GOBIERNO REGIONAL DE HUANCAVELICA	Evento: (FUEGO) INCENDIO	FPC-003
<b>1. PLAN DE PREVENCIÓN</b>		
<p><b>a. Descripción del evento</b></p> <p>Es un proceso de combustión caracterizado por la emisión de calor acompañado de humo, llamas o ambas que se propaga de manera incontrolable en el tiempo y en el espacio. Se producen en materiales sólidos, líquidos combustibles inflamables, equipos e instalaciones bajo carga eléctrica entre otros que se produzcan dentro del Data Center del Gobierno Regional de Huancavelica.</p> <p>Este evento puede afectar los siguientes activos:</p> <p><b>APLICACIONES INFORMATICAS</b></p> <ul style="list-style-type: none"> <li>Todas las aplicaciones informáticas implementadas en el Gobierno regional de Huancavelica.</li> </ul> <p><b>SERVICIOS</b></p> <ul style="list-style-type: none"> <li>Todos los servicios informáticos que presta el Gobierno regional de Huancavelica.</li> </ul> <p><b>INSTALACIONES</b></p> <ul style="list-style-type: none"> <li>“Centro de Datos” (Data Center) de la Sede central del Gobierno regional de Huancavelica.</li> </ul> <p><b>EQUIPAMIENTO INFORMATICO</b></p> <ul style="list-style-type: none"> <li>Todo el equipamiento informático ubicado en a data center y local de la sede central.</li> </ul> <p><b>EQUIPAMIENTO AUXILIAR</b></p> <ul style="list-style-type: none"> <li>Todo el equipamiento auxiliar ubicado en el data center y local de la sede central.</li> </ul> <p><b>PERSONAL</b></p> <ul style="list-style-type: none"> <li>Personal de la Sub Gerencia de Desarrollo Institucional y Tecnologías de la Información considerado o no como activo informático.</li> </ul> <p><b>b. Objetivo</b></p> <p>Establecer las acciones que se ejecutaran ante un incendio a fin de minimizar el tiempo de interrupción de las operaciones del Gobierno Regional de Huancavelica sin exponer la seguridad de las personas.</p> <p><b>Criticidad</b></p> <p>El Estudio determina que el presente evento tiene un MUY ALTO impacto y RIESGO medio.</p> <p><b>Entorno</b></p> <p>Este evento se puede dar en todas instalaciones del Gobierno Regional de Huancavelica.</p> <p><b>e. Personal Encargado</b></p> <p>El Director y/o Jefe de área, es quien debe dar cumplimiento a lo descrito en las Condiciones de Prevención de Riesgo del presente Plan.</p> <p><b>Condiciones de Prevención de Riesgo</b></p> <ul style="list-style-type: none"> <li>Realizar inspecciones de seguridad periódicamente.</li> <li>Mantener las conexiones eléctricas seguras en el rango de su vida útil.</li> <li>Charlas sobre el uso y manejo de extintores.</li> </ul> <p>Acatar las indicaciones del INDECI, en torno al evento</p> <p>Contar con una relación de teléfonos de emergencia que incluya a los bomberos, ambulancias, y personal del GRH responsable de las acciones de prevención y</p>		



	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAMELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

ejecución de la contingencia.  
Igualmente se contará con los siguientes elementos para la detección y extinción de un posible incendio, los cuales cubrirán los ambientes del “Centro de Datos” y áreas afines a las tecnologías de la información del GRH:

- Implementar detectores de humo en el “Centro de Datos”
- Considerar la Implementación de la Central de detección de incendios
- Mantener actualizado los extintores.

## 2. PLAN DE EJECUCION

### a. Eventos que activan la Contingencia

La Contingencia se activará al ocurrir un incendio en el Data Center del Gobierno Regional de Huancavelica.

### b. Procesos Relacionados antes del evento.

- Identificar la ubicación del incendio.

### c. Personal que autoriza la contingencia.

Cualquier personal de SGDlyTI puede dar la alarma para activar la contingencia.

### d. Descripción de las actividades después de activar la contingencia.

- Tratar de apagar el incendio con extintores.
- Comunicar al personal responsable del GRH.
- Evacuar el área.
- Dar aviso a los bomberos.

### e. Duración

La duración de la contingencia dependerá del tiempo que demande controlar el incendio.

## 3. PLAN DE RECUPERACIÓN

### a. Personal Encargado

El Sub Gerente de la SGDlyTI, son encargados de dirigir ñas labores de recuperación.

### b. Descripción

- Evaluación de los daños ocasionados al personal y activos informáticos.
- Realizar inventario de los activos físicos operativos y dañados para efectuar trámites para el reemplazo de los equipos dañados.
- Evaluación estado de los sistemas informáticos y los activos que dependen para su funcionamiento.
- Utilizar los equipos en buen estado para implementar los servicios informáticos dañados en otra ubicación para lograr su disponibilidad en el menor tiempo posible.

### c. Mecanismos de Comprobación

Todos los sistemas informáticos operativos.

### d. Desactivación del Plan de Contingencia


El Sub Gerente de la SGDlyTI desactivara la contingencia cuando todos los servicios informáticos estén operativos y se haya recuperado todos los activos informáticos afectados.

### e. Proceso de Actualización

- Se elaborará un informe de los daños y pérdidas sufridos.
- Se implementará con extintores operativos y listos para su uso.
- Se determinará las causas y se procederá a efectuar las medidas correctivas necesarias para evitar que se vuelvan a producir..






	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

## CONTINGENCIAS RELACIONADAS A: PERSONAL

GOBIERNO REGIONAL DE HUANCAVELICA	Evento: AVERÍA DE ORIGEN FÍSICO O LÓGICO	FPC-004
<b>1. PLAN DE PREVENCIÓN</b>		
<p><b>a. Descripción del evento</b></p> <p>Son fallas de origen físico o lógico que pueden producir de manera imprevista al equipamiento informático. Pueden afectar los siguientes activos:</p> <p><b>APLICACIONES INFORMATICAS</b></p> <ul style="list-style-type: none"> <li>[SIAF] Sistema Integrado de Administración Financiera</li> <li>[SIGA] Sistema Integrado de Gestión Logística</li> <li>[SIGGEDO] Sistema de Gestión Documentaria</li> <li>[EMAIL] Correo Electrónico Institucional.</li> <li>[WWW] Portal Web Institucional</li> <li>Otras aplicaciones.</li> </ul> <p><b>SERVICIOS</b></p> <ul style="list-style-type: none"> <li>[SV_ WEB] Servidor Sitios Web.</li> <li>[SV_SIGGEDO] Tramite documentario</li> <li>[SV_PROXY] Servidor Proxy (Internet).</li> <li>[SV_CS] Controlador de Dominio (DNS)</li> <li>[SV_email] Correo Electrónico Institucional</li> <li>Otros servicios.</li> </ul> <p><b>EQUIPAMIENTO INFORMÁTICO</b></p> <ul style="list-style-type: none"> <li>[HW_SRVF] Servidores físicos</li> <li>[HW_SRVV] Servidores virtuales</li> <li>[HW_UTM] Firewall / Equipo Unificado contra Amenazas.</li> <li>[HW_NAS] Sistema de almacenamiento en Red</li> <li>[HW_PC] Equipos de computo</li> <li>[HW_SWC] Switchs Core</li> <li>[HW_ROUTER] Router de voz</li> <li>[HW_SW] Switchs distribución</li> <li>[HW_AP] Access Point</li> </ul> <p><b>Objetivo</b></p> <p>Establecer las acciones que se ejecutaran ante los fallo de origen físico o lógicos de los activos de la entidad a fin de minimizar el tiempo de interrupción de las operaciones del Gobierno Regional de Huancavelica.</p> <p><b>c. Criticidad</b></p> <p>El Estudio determina que el presente evento tiene un MUY ALTO impacto y RIESGO medio.</p> <p><b>d. Entorno</b></p> <p>Este evento se puede dar en todos los activos identificados como afectables.</p> <p><b>e. Personal Encargado</b></p> <p>El Administrador de sistemas y/o Bases de datos de la Sub Gerencia de Desarrollo Institucional y Tecnologías de la Información (SGDIyTI), es quien debe dar cumplimiento a lo descrito en las Condiciones de Prevención de Riesgo del presente Plan.</p> <p><b>Condiciones de Prevención de Riesgo</b></p> <ul style="list-style-type: none"> <li>Contar con repuestos de componentes del tipo consumibles para contingencias.</li> </ul>		



	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

- Contar con equipos con tolerancia a fallos en diversas partes: discos duros, fuentes de poder, etc.
- Implementar arreglos de discos con tolerancia a fallos en cada servidor.
- Contar con copias de seguridad periódicos de la información crítica (bases de datos, aplicativos) de las aplicaciones informáticas en desarrollo/producción en la Institución.
- Ejecución de tareas periódicas de respaldo de la información crítica: archivos, bases de datos, etc. En diferentes medios.
- Contar con servicios de soporte vigentes para los sistemas operativos y motores de bases de datos. En caso sea necesario, este soporte debe incluir actividades de prevención, revisión del sistema y mantenimiento general a la base de datos.

## 2. PLAN DE EJECUCION

### a. Eventos que activan la Contingencia

- Fallas físicas de componentes de servidores y/o equipamiento.
- Fallas de aplicativos de origen lógico.

### b. Procesos Relacionados antes del evento.

- Identificar el componente y/o equipos que presenta la falla.
- Identificar el sistema que presenta las fallas de origen lógico

### c. Personal que autoriza la contingencia.

El Administrador de sistemas y/o Bases de datos de la SGDlyTI pueden activar la contingencia.

### d. Descripción de las actividades después de activar la contingencia.

- Identificar los componentes y equipos donde se produjo la falla y si es de origen físico o lógico.

### e. Duración

La duración de la contingencia dependerá del tiempo que demande su puesta en funcionamiento.

## 3. PLAN DE RECUPERACIÓN

### a. Personal Encargado

El Administrador de sistemas y/o Bases de datos de la SGDlyTI son los encargados de la recuperación.

### b. Descripción

- De existir un repuesto disponible del componente que presenta la falla se procede al reemplazo.
- De no existir un repuesto disponible y existir una garantía vigente se comunicará con el proveedor y/o fabricante para su remplazo, En caso de no existir un repuesto disponible y sin una garantía vigente, se informará para la adquisición de los componentes averiados.
- En caso de tratarse de una avería de origen lógico se procederá con la contingencia para casos de destrucción de información.

### Mecanismos de Comprobación

Comprobación del buen funcionamiento sistema informático y sus componentes físicos donde se produjo la falla.


### d. Desactivación del Plan de Contingencia

El Administrador de sistemas y/o Bases de datos de la SGDlyTI, desactiva la contingencia cuando el equipo funciona con normalidad.

### e. Proceso de Actualización


- Se comprueba el normal funcionamiento de las aplicaciones y sistemas



	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN GOBIERNO REGIONAL DE HUANCAVELICA	Fecha: Noviembre 2016 Versión:1.0

informáticos.		
GOBIERNO REGIONAL DE HUANCAVELICA	Evento: INDISPONIBILIDAD DE PERSONAL	FPC-005
<b>1. PLAN DE PREVENCIÓN</b>		
<p><b>a. Descripción del evento</b> Indisponibilidad de personal clave para la Administración y/o soporte de los sistemas informáticos existentes en la Institución, pueden afectar los siguientes activos: <b>APLICACIONES INFORMATICAS</b></p> <ul style="list-style-type: none"> <li>• Todas</li> </ul> <p><b>SERVICIOS</b></p> <ul style="list-style-type: none"> <li>• Todas</li> </ul> <p><b>EQUIPAMIENTO INFORMÁTICO</b></p> <ul style="list-style-type: none"> <li>• Todas</li> </ul> <p><b>EQUIPAMIENTO AXILIAR</b></p> <ul style="list-style-type: none"> <li>• Todas</li> </ul>		
<p><b>b. Objetivo</b> Establecer las acciones que se ejecutaran ante la ausencia de los activos identificados como PERSONAL del Gobierno Regional de Huancavelica.</p>		
<p><b>c. Criticidad</b> El Estudio determina que el presente evento tiene un MUY ALTO impacto y RIESGO medio.</p>		
<p><b>d. Entorno</b> Este evento se puede dar en los contratos del personal identificado como activos en sus diversas modalidades.</p>		
<p><b>e. Personal Encargado</b> La Sub Gerencia de Desarrollo Institucional y Tecnologías de la Información (SGDIyTI), es quien debe dar cumplimiento a lo descrito en las Condiciones de Prevención de Riesgo del presente Plan.</p>		
<p><b>f. Condiciones de Prevención de Riesgo</b></p> <ul style="list-style-type: none"> <li>• Presupuesto disponible para la contratación del personal identificado como activos.</li> <li>• Contar con el personal debidamente capacitado y experimentado para la administración y soporte de todos los demás activos identificados.</li> <li>• Contar con más de un encargado para la administración de cada activo informático.</li> </ul>		
<b>2. PLAN DE EJECUCION</b>		
<p><b>f. Eventos que activan la Contingencia</b></p> <ul style="list-style-type: none"> <li>• Ausencia prevista o imprevista de uno o más del personal activo.</li> </ul>		
<p><b>g. Procesos Relacionados antes del evento.</b></p> <ul style="list-style-type: none"> <li>• Comprobación de la disponibilidad de otro personal para sustitución inmediata del personal ausente.</li> <li>• Comprobación de la existencia de recursos para contratación de personal capacitado y con experiencia para la sustitución temporal del personal ausente.</li> </ul>		
<p><b>h. Personal que autoriza la contingencia.</b> El Administrador de sistemas, Bases de datos o Sub Gerente de la SGDIyTI pueden activar la contingencia.</p>		
<p><b>Descripción de las actividades después de activar la contingencia.</b></p> <ul style="list-style-type: none"> <li>• Convocar al personal de reemplazo para el desempeño de las labores del personal</li> </ul>		



	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

nuevo personal.

- Contratación de nuevo personal si el caso lo amerita para asumir las funciones sin un responsable.

**j. Duración**  
La duración de la contingencia dependerá del tiempo que demande su puesta en funcionamiento.

**3. PLAN DE RECUPERACIÓN**

**f. Personal Encargado**  
El personal sustituto temporal o el personal de remplazo definitivos son los encargados de la recuperación.

**g. Descripción**

- Se asume de manera temporal o definitiva de las funciones que dejó el personal saliente.


**h. Mecanismos de Comprobación**  
Personal catalogado como activo informático, debidamente contratado y completo, para la administración de soporte de todos los demás Activos informáticos.

**i. Desactivación del Plan de Contingencia**  
El Administrador de sistemas o Sub Gerente de la SGDlyTI, desactiva la contingencia cuando se cumpla el mecanismo de comprobación.

**j. Proceso de Actualización**

- Se comprueba que existan recursos financieros para asumir la contingencia en cualquier momento.




	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

## RECOMENDACIONES

- Se debe contar con la misma cantidad de componentes de reemplazo (servidores, equipos de red, respaldo de energía, Discos SAS, aire acondicionado, etc) para la correcta aplicación del presente Plan de Contingencias de los Sistemas de Información.
- Para casos de corte eléctrico prolongado, contar con un generador eléctrico.
- Implementar extintores de polvo químico seco o HALOTRON para el Data Center y áreas aledañas.
- Implementar cámaras de seguridad, sensor de temperatura y detector de humo en el Data Center.
- Implementar el control de acceso restringido al Data Center.
- Implementar un Sistema de Gestión de Seguridad de la Información.
- Socializar a todos los servidores de la entidad la importancia de la Seguridad de la Información.




	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

## CONCLUSIONES

- Es necesario se asigne anualmente a la Sub Gerencia de Desarrollo Institucional y Tecnologías de la Información los recursos financiero necesarios para la correcta aplicación del presente Plan de Contingencias de los Sistemas de Información para cada año, ya sea para la adquisición de equipos o repuestos necesarios y contratación de personal calificado y experimentado para la administración y soporte de los sistemas informáticos identificados como activos informáticos.
- Esta es la primera versión 1.0 del Plan de Contingencias de los Sistemas de Información del Gobierno Regional de Huancavelica, que servirá como una guía rápida para solucionar los imprevistos y situaciones que afecten el correcto funcionamiento de los Activos informáticos identificados a nivel del Data Center de la institución, Quedando abierto para una mejora continua conforme se presenten los avances de la tecnología.



	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

## GLOSARIO DE TERMINOS

**Sistema de Información:** Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo.

**Seguridad de la Información:** Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.

**Seguridad Informática:** es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático. De todas formas, no existe ninguna técnica que permita asegurar la inviolabilidad de un sistema.

**Confidencialidad:** aseguramiento de que la información es accesible solo para aquellos autorizados a tener acceso.

**Disponibilidad:** aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

**Integridad:** garantía de la exactitud y completitud de la información de la información y los métodos de su procesamiento.

**Análisis de Riesgos:** El análisis de riesgo es el uso sistemático de la información disponible para determinar la frecuencia con la que determinados eventos se pueden producir y la magnitud de sus consecuencias.

**Riesgo:** Posibilidad de que se produzca un contratiempo o una desgracia, de que alguien o algo sufra perjuicio o daño.

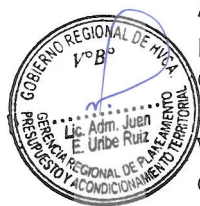
**Amenaza:** Una amenaza a un sistema informático es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque en el equipo.


**Vulnerabilidad:** Es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.

**Impacto:** Se habla de un Impacto, cuando un ataque exitoso perjudicó la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones.

**Servidores:** Un servidor es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia. Los servidores se pueden ejecutar en cualquier tipo de computadora, incluso en computadoras dedicadas a las cuales se les conoce individualmente como "el servidor".

**Aplicaciones Informáticas:** Es un programa informático hecho para permitir a un usuario realizar uno o varios tipos de trabajo.



	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

**SIGA:** El Sistema Integrado de Gestión Administrativa, es una aplicación en la cual se ve plasmada toda la normatividad relacionada a las contrataciones y adquisiciones del Estado y en cada una de las interfaces y opciones que tiene este sistema se puede apreciar todo el proceso logístico que va desde la generación de los pedidos, el proceso de selección y posteriormente se generan ya sean los contratos, las órdenes de compra o de servicio.

**SIAF:** El Sistema Integrado de Administración Financiera, es un sistema informático que permite administrar, mejorar y supervisar las operaciones de ingresos y gastos de las Entidades del Estado, además de permitir la integración de los procesos presupuestarios, contables y de tesorería de cada entidad.

**SISGEDO:** El Sistema de Gestión Documentaria - SISGEDO 2.0.0 es una aplicación WEB desarrollada por el Gobierno Regional Lambayeque para efectuar el registro, control, seguimiento detallado y estricto de todos los documentos que se procesan en la Institución, tanto externos como internos.

**Redes de Comunicación:** es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

**Antivirus:** Es una software que se instala en tu ordenador y que permite prevenir que programas diseñados para producir daños, también llamados virus, dañen tu equipo. También tiene la misión de limpiar ordenadores ya infectados.

**Backup:** También llamado copia de seguridad, es la tarea de duplicar y guardar cualquier tipo de datos o información en otro lugar (disco, servidor...) para que pueda ser recuperado en caso de la pérdida de la información original.

**Browser:** Es un programa o aplicación que nos permite navegar por Internet y encontrar exactamente la información o temática que nos interesa. Las mas populares son Internet Explorer, Netscape y Firefox.

**Copyright:** Son los derechos de autor de un determinado producto.

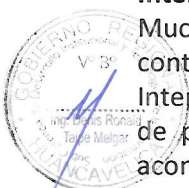
**Dominio:** Estrictamente hablando, es un nombre que representa una entidad lógica y que puede estar formado por otros dominios formando un árbol o estructura jerárquica.

**Firewall:** Es un dispositivo que asegura las comunicaciones entre usuarios de una red e Internet.


**Hardware:** Hace referencia a la parte física o sólida de un ordenador u otro elemento informático.

**Interface:** Es el punto de comunicación entre dos elementos electrónicos o informáticos. Muchas veces se refiere a el como puerto. También se podría definir como El punto de contacto entre el usuario, el ordenador y el programa, por ejemplo, el teclado o un menú.

**Internet - Red de telecomunicaciones** a la cual están conectadas centenares de millones de personas, organismos y empresas en todo el mundo. Su creación fue uno de los acontecimientos más importantes en la historia de la informática.






	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

## BIBLIOGRAFIA

- Guía práctica para planes de contingencia de sistemas de información – INEI 2001
- MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.
- R.J. N° 340-94-INEI, Normas Técnicas para el procesamiento y respaldo de la información que se procesa en entidades del Estado.
- R.J. N° 076-95-INEI, Recomendaciones Técnicas para la seguridad e integridad de la información que se procesa en la administración pública.
- R.J. N° 090-95-INEI, Recomendaciones Técnicas para la protección física de los equipos y medios de procesamiento de la información en la administración pública.






	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

A-02: FORMATO DE REGISTRO DE PLAN DE CONTINGENCIA

GOBIERNO REGIONAL DE HUANCAVELICA	DESCRIPCIÓN DEL EVENTO	CODIGO FORMATO PLAN DE CONTINGENCIA-FPC
<b>1. PLAN DE PREVENCIÓN</b>		
<p><b>a. Descripción del evento</b> Aquí se describirá el evento generado.</p> <p><b>b. Objetivo</b> Aquí se describirá el objetivo y funciones principales de un proceso, ejecutándose a condiciones /(normales/, es decir sin la presencia de un evento que genere contingencia.</p> <p><b>c. Criticidad</b> Señala cuan crítico es un proceso, así como el nivel de impacto del mismo dentro del servicio como se clasifica a continuación:  <b>Crítico:</b> El proceso o actividad es de alto impacto o altamente crítico, no debe sufrir ningún tipo de interrupción.  <b>Importante:</b> El proceso o actividad puede ser suspendido por un breve lapso de tiempo no mayor a las 2 horas.  <b>Menos Importante:</b> El proceso o actividad puede ser suspendido por un lapso de tiempo no mayor a 24 horas.</p> <p><b>d. Entorno</b> Aquí se describirá la ubicación y los ambientes, equipos informáticos y equipos de diversa índole que pueden ser automáticos o mecánicos, desde donde se ejecutan sus procesos en forma normal, así como las condiciones básicas para su operación.</p> <p><b>e. Personal Encargado</b> Aquí se detallarán los nombres y cargos del personal del servicio, responsable de ejecutar el proceso en condiciones normales y sus roles dentro del mismo.</p> <p><b>f. Condiciones de Prevención de Riesgo</b> Aquí se describen detalladamente las acciones que se ejecutarán durante el proceso normal y los puntos de control implementados, a efectos de prevenir que se presente el evento que genere la activación de un estado de contingencia.</p>		
<b>PLAN DE EJECUCION</b>		
<p><b>Eventos que activan la Contingencia</b> Aquí se describen los eventos que deciden la activación de la contingencia. Asimismo, se especifica el lapso de tiempo en el cual se empieza a ejecutar el proceso de contingencia.</p> <p><b>g. Procesos Relacionados antes del evento.</b> Aquí se describen de forma secuencial todos los procesos o actividades que se tengan que ejecutar con anterioridad al ingreso del proceso de contingencia.</p> <p><b>h. Personal que autoriza la contingencia.</b> Aquí se especificará los cargos del personal que autorizara e iniciara el proceso de contingencia, así como el nivel de coordinación con funcionarios de la entidad.</p> <p><b>i. Descripción de las actividades después de activar la contingencia.</b> Aquí se describirá en forma detallada y secuencial los pasos a realizar para poner en marcha el proceso de contingencia.</p> <p><b>Duración</b> Aquí se especificara el lapso de tiempo por el cual estará activada la contingencia, así</p>		



	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

como el evento que determine la culminación del mismo.

### 3. PLAN DE RECUPERACIÓN

#### f. Personal Encargado

Aquí se especificará los nombres y cargos del personal encargado del proceso de Recuperación cuando se presente un evento de contingencia.

#### g. Descripción

Aquí se describirá en forma detallada y secuencial los pasos a ejecutar para recuperar los procesos a su estado normal, debiendo indicar lo necesario para asegurar la recuperación efectiva del mismo.

#### h. Mecanismos de Comprobación

Aquí se describirán aquellas actividades que permitan asegurar que el proceso recuperado opere en condiciones normales y sin volver a presentar la falla que originó la ocurrencia del evento. Mientras esta etapa se realiza, aún sigue activado el Plan de Contingencia.


#### i. Desactivación del Plan de Contingencia

Aquí se especificará de forma secuencial cual es el procedimiento para desactivar el proceso de contingencia.

#### j. Proceso de Actualización

Aquí se especificará de forma detallada las actividades a ejecutar para actualizar el proceso normal recientemente recuperado.



	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

## CATÁLOGOS DE ACTIVOS: MAGERIT VERSIÓN 3.0

### 1. [D] Datos / Información

Los datos son el corazón que permite a una organización prestar sus servicios. La información es un activo abstracto que será almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos.


<b>[D] Datos / Información</b>
[files] ficheros [backup] copias de respaldo [conf] datos de configuración (1) [int] datos de gestión interna [password] credenciales (ej. contraseñas) [auth] datos de validación de credenciales [acl] datos de control de acceso [log] registro de actividad (2) [source] código fuente [exe] código ejecutable [test] datos de prueba
(1) Los datos de configuración son críticos para mantener la funcionalidad de las partes y del conjunto del sistema de información. (2) Los registros de actividad sustentan los requisitos de trazabilidad.

### 2. [S] Servicios

Función que satisface una necesidad de los usuarios (del servicio). Esta sección contempla servicios prestados por el sistema.

<b>[S] Servicios</b>
[anon] anónimo (sin requerir identificación del usuario) [pub] al público en general (sin relación contractual) [ext] a usuarios externos (bajo una relación contractual) [int] interno (a usuarios de la propia organización) [www] world wide web [telnet] acceso remoto a cuenta local [email] correo electrónico [file] almacenamiento de ficheros [ftp] transferencia de ficheros [edi] intercambio electrónico de datos [dir] servicio de directorio (1) [idm] gestión de identidades (2) [ipm] gestión de privilegios [pmi] PKI - infraestructura de clave pública (3)
(1) Localización de personas (páginas blancas), empresas o servicios (páginas amarillas); permitiendo la identificación y facilitando los atributos que caracterizan al elemento determinado. (2) Servicios que permiten altas y bajas de usuarios de los sistemas, incluyendo su caracterización y activando los servicios de aprovisionamiento asociados a sus cambios de estado respecto de la organización. (3) Servicios asociados a sistemas de criptografía de clave pública, incluyendo especialmente la gestión de certificados.



	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

### 3. [SW] Software - Aplicaciones informáticas

Con múltiples denominaciones (programas, aplicativos, desarrollos, etc.) este epígrafe se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.

No preocupa en este apartado el denominado “código fuente” o programas que serán datos de interés comercial, a valorar y proteger como tales. Dicho código aparecería como datos.

#### **[SW] Aplicaciones (software)**

[prp] desarrollo propio (in house)  
[sub] desarrollo a medida (subcontratado)  
[std] estándar (off the shelf)  
[browser] navegador web  
[www] servidor de presentación  
[app] servidor de aplicaciones  
[email\_client] cliente de correo electrónico  
[email\_server] servidor de correo electrónico  
[file] servidor de ficheros  
[dbms] sistema de gestión de bases de datos  
[tm] monitor transaccional  
[office] ofimática  
[av] anti virus  
[os] sistema operativo  
[hypervisor] gestor de máquinas virtuales  
[ts] servidor de terminales  
[backup] sistema de backup


### 4. [HW] Equipamiento informático (hardware)

Dícese de los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.

#### **HW] Equipos informáticos (hardware)**

[host] grandes equipos (1)  
[mid] equipos medios (2)  
[pc] informática personal (3)  
[mobile] informática móvil (4)  
[pda] agendas electrónicas  
[vhost] equipo virtual  
[backup] equipamiento de respaldo (5)  
[peripheral] periféricos  
[print] medios de impresión (6)  
[scan] escáneres  
[crypto] dispositivos criptográficos  
[bp] dispositivo de frontera (7)  
[network] soporte de la red (8)  
[modem] módems  
[hub] concentradores  
[switch] conmutadores  
[router] encaminadores  
[bridge] pasarelas  
[firewall] cortafuegos  
[wap] punto de acceso inalámbrico



	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

[pabx] centralita telefónica
[iphone] teléfono IP
<ol style="list-style-type: none"> <li>(1) Se caracterizan por haber pocos, frecuentemente uno sólo, ser económicamente gravosos y requerir un entorno específico para su operación. Son difícilmente reemplazables en caso de destrucción.</li> <li>(2) Se caracterizan por haber varios, tener un coste económico medio tanto de adquisición como de mantenimiento e imponer requerimientos estándar como entorno de operación. No es difícil reemplazarlos en caso de destrucción.</li> <li>(3) Se caracterizan por ser multitud, tener un coste económico relativamente pequeño e imponer solamente unos requerimientos mínimos como entorno de operación. Son fácilmente reemplazables en caso de destrucción.</li> <li>(4) Se caracterizan por ser equipos afectos a la clasificación como informática personal que, además, son fácilmente transportables de un sitio a otro, pudiendo estar tanto dentro del recinto propio de la organización como en cualquier otro lugar.</li> <li>(5) Son aquellos equipos preparados para hacerse cargo inmediato de los equipos en producción.</li> <li>(6) Dícese de impresoras y servidores de impresión.</li> <li>(7) Son los equipos que se instalan entre dos zonas de confianza.</li> <li>(8) Dícese de equipamiento necesario para transmitir datos: routers, módems, etc.</li> </ol>

#### 5. [COM] Redes de comunicaciones

Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.

<b>[COM] Redes de comunicaciones</b>
[PSTN] red telefónica [ISDN] rdsi (red digital) [X25] X25 (red de datos) [ADSL] ADSL [pp] punto a punto [radio] comunicaciones radio [wifi] red inalámbrica [mobile] telefonía móvil [sat] por satélite [LAN] red local [MAN] red metropolitana [Internet] Internet




#### 6. [AUX] Equipamiento auxiliar

En este epígrafe se consideran otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.

<b>[AUX] Equipamiento auxiliar</b>
[power] fuentes de alimentación [ups] sistemas de alimentación ininterrumpida [gen] generadores eléctricos [ac] equipos de climatización [cabling] cableado [wire] cable eléctrico [fiber] fibra óptica [robot] robots [tape] ... de cintas [disk] ... de discos



	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

[supply] suministros esenciales  
 [destroy] equipos de destrucción de soportes de información  
 [furniture] mobiliario: armarios, etc  
 [safe] cajas fuertes

### 7. [L] Instalaciones

En este epígrafe entran los lugares donde se hospedan los sistemas de información y comunicaciones.

#### [L] Instalaciones

[site] recinto  
 [building] edificio  
 [local] cuarto  
 [mobile] plataformas móviles  
 [car] vehículo terrestre: coche, camión, etc.  
 [plane] vehículo aéreo: avión, etc.  
 [ship] vehículo marítimo: buque, lancha, etc.  
 [shelter] contenedores  
 [channel] canalización  
 [backup] instalaciones de respaldo

### 8. [P] Personal


En este epígrafe aparecen las personas relacionadas con los sistemas de información.

#### [P] Personal

[ue] usuarios externos  
 [ui] usuarios internos  
 [op] operadores  
 [adm] administradores de sistemas  
 [com] administradores de comunicaciones  
 [dba] administradores de BBDD  
 [sec] administradores de seguridad  
 [des] desarrolladores / programadores  
 [sub] subcontratas  
 [prov] proveedores





	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAMELICA</b>	Fecha: Noviembre 2016
		Versión:1.0


## CRITERIOS DE VALORACIÓN

### ESCALA ESTÁNDAR

<b>[pi] Información de carácter personal</b>		
6	6.pi1	probablemente afecte gravemente a un grupo de individuos
	6.pi2	probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
5	5.pi1	probablemente afecte gravemente a un individuo
	5.pi2	probablemente quebrante seriamente leyes o regulaciones
4	4.pi1	probablemente afecte a un grupo de individuos
	4.pi2	probablemente quebrante leyes o regulaciones
3	3.pi1	probablemente afecte a un individuo
	3.pi2	probablemente suponga el incumplimiento de una ley o regulación
2	2.pi1	podría causar molestias a un individuo
	2.pi2	podría quebrantar de forma leve leyes o regulaciones
1	1.pi1	podría causar molestias a un individuo

<b>[lpo] Obligaciones legales</b>		
9	9.lro	probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
7	7.lro	probablemente cause un incumplimiento grave de una ley o regulación
5	5.lro	probablemente sea causa de incumplimiento de una ley o regulación
3	3.lro	probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
	1.lro	podría causar el incumplimiento leve o técnico de una ley o regulación

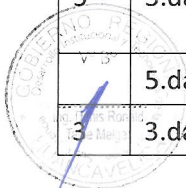
<b>[si] Seguridad</b>		
	10.si	probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios
9	9.si	probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
	7.si	probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
	3.si	probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
	1.si	podría causar una merma en la seguridad o dificultar la investigación de un incidente


	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016 Versión:1.0

<b>[cei] Intereses comerciales o económicos</b>		
9	9.cei.a	de enorme interés para la competencia
	9.cei.b	de muy elevado valor comercial
	9.cei.c	causa de pérdidas económicas excepcionalmente elevadas
	9.cei.d	causa de muy significativas ganancias o ventajas para individuos u
	9.cei.e	constituye un incumplimiento excepcionalmente grave de las obligaciones contrac- tuales relativas a la seguridad de la información proporcionada por
7	7.cei.a	de alto interés para la competencia
	7.cei.b	de elevado valor comercial
	7.cei.c	causa de graves pérdidas económicas
	7.cei.d	proporciona ganancias o ventajas desmedidas a individuos u organizaciones
	7.cei.e	constituye un serio incumplimiento de obligaciones contractuales relativas a la se- guridad de la información proporcionada por terceros
3	3.cei.a	de cierto interés para la competencia
	3.cei.b	de cierto valor comercial
	3.cei.c	causa de pérdidas financieras o merma de ingresos
	3.cei.d	facilita ventajas desproporcionadas a individuos u organizaciones
	3.cei.e	constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros
2	2.cei.a	de bajo interés para la competencia
	2.cei.b	de bajo valor comercial
1	1.cei.a	de pequeño interés para la competencia
	1.cei.b	de pequeño valor comercial
	0.3	supondría pérdidas económicas mínimas



<b>[da] Interrupción del servicio</b>		
9	9.da	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras
	9.da2	Probablemente tenga un serio impacto en otras organizaciones
	7.da	Probablemente cause una interrupción seria de las actividades propias de la Or- ganización con un impacto significativo en otras organizaciones
	7.da2	Probablemente tenga un gran impacto en otras organizaciones
5	5.da	Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
	5.da2	Probablemente cause un cierto impacto en otras organizaciones
3	3.da	Probablemente cause la interrupción de actividades propias de la



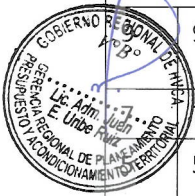
	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0


1	1.da	Pudiera causar la interrupción de actividades propias de la Organización
---	------	--

<b>[po] Orden público</b>		
9	9.po	alteración seria del orden público
6	6.po	probablemente cause manifestaciones, o presiones significativas
3	3.po	causa de protestas puntuales
1	1.po	pudiera causar protestas puntuales

<b>[olm] Operaciones</b>		
10	10.olm	Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
9	9.olm	Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
7	7.olm	Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
5	5.olm	Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local
3	3.olm	Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)
1	1.olm	Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)

<b>[adm] Administración y gestión</b>		
9.adm		probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre
7.adm		probablemente impediría la operación efectiva de la Organización
5.adm		probablemente impediría la operación efectiva de más de una parte de la Organización
3.adm		probablemente impediría la operación efectiva de una parte de la Organización
1.adm		pudiera impedir la operación efectiva de una parte de la Organización



	SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍAS DE LA INFORMACIÓN	Código:PCSI-001
	<b>PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN</b> <b>GOBIERNO REGIONAL DE HUANCAVELICA</b>	Fecha: Noviembre 2016
		Versión:1.0

<b>[lg] Pérdida de confianza (reputación)</b>		
9	9.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con otras organizaciones
	9.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con el público en general
7	7.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con otras organizaciones
	7.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general
5	5.lg.a	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con otras organizaciones
	5.lg.b	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con el público
3	3.lg	Probablemente afecte negativamente a las relaciones internas de la Organización
2	2.lg	Probablemente cause una pérdida menor de la confianza dentro de la Organización
1	1.lg	Pudiera causar una pérdida menor de la confianza dentro de la Organización
0	0.4	no supondría daño a la reputación o buena imagen de las personas u organizaciones

<b>[crm] Persecución de delitos</b>		
8	8.crm	Impida la investigación de delitos graves o facilite su comisión
	4.crm	Dificulte la investigación o facilite la comisión de delitos

