Defensoría del Pueblo

RESOLUCIÓN ADMINISTRATIVA Nº 021 -2016/DP

Lima, 06 MAYO 2016

VISTO:

El proveído Nº 052 de la Primera Adjuntía que adjunta los memorandos Nº 042-2016-DP/SG y Nº 015-2016-DP/OTIT, mediante el cual se solicita la emisión de la resolución que apruebe los documentos denominados: "Alcance del Sistema de Gestión de Seguridad de la Información", "Funciones y Responsabilidades de la Seguridad de la Información" y "Metodología de Evaluación y Tratamiento de Riesgos" de la Defensoría del Pueblo; y,

CONSIDERANDO:

Que, de conformidad con los artículos 161º y 162º de la Constitución Política del Perú se aprobó la Ley Nº 26520, Ley Orgánica de la Defensoría del Pueblo y sus modificatorias, y mediante Resolución Defensorial Nº 0012-2011/DP se aprobó su vigente Reglamento de Organización y Funciones;

Que, a través de Resolución Nº 129-2014/CNB-INDECOPI, se aprobó la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2º Edición", la cual tiene por objetivo establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información, en concordancia a la normativa vigente y los requerimientos de cada entidad, y asimismo, deja sin efecto la Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 1º Edición";

Que, asimismo, mediante Resolución Ministerial Nº 004-2016-PCM, se aprobó el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2º Edición", en todas las entidades integrantes del Sistema Nacional de Informática;

Que, conforme a lo establecido en el literal b) del artículo 60º del Reglamento de Organización y Funciones de la Defensoría del Pueblo, corresponde a la Oficina de Tecnología de la Información y Telecomunicaciones, diseñar, proponer y coordinar la implementación de normas, estándares, lineamientos y procedimientos relacionados con los elementos de hardware, software, redes y comunicaciones IP de la plataforma técnica y tecnologías relacionadas con la gestión informática de la entidad;

Que, mediante Resolución Administrativa Nº 020-2016/DP se aprobó el documento denominado: "Políticas y Objetivos de la Seguridad de la Información" de la Defensoría del Pueblo, que establece los lineamientos de Seguridad de la Información y tiene entre sus objetivos, el preservar la confidencialidad, integridad y

Defensoría del Pueblo

disponibilidad de la información que la Defensoría del Pueblo produce o utiliza en su quehacer cotidiano;

Que, los documentos denominados: "Alcance del Sistema de Gestión de Seguridad de la Información", "Funciones y Responsabilidades de la Seguridad de la Información" y "Metodología de Evaluación y Tratamiento de Riesgos" de la Defensoría del Pueblo, propuestos por la Oficina de Tecnología de la Información y Telecomunicaciones, fueron elaborados teniendo como base la actualización de la precitada Norma Técnica Peruana, y ante la necesidad de implementar mecanismos que permitan mejorar la seguridad de la información que se utiliza o produce en la Defensoría del Pueblo;

Que, en consecuencia, a fin de implementar la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2° Edición" y adecuar nuestros lineamientos internos al marco normativo vigente de forma progresiva, resulta procedente aprobar el mencionado documento;

Con los visados de la Primera Adjuntía, de la Secretaría General y de las oficinas de Tecnología de la Información y Telecomunicaciones y de Asesoría Jurídica; y,

En uso de las atribuciones y facultades conferidas por el numeral 8) del artículo 9° de la Ley Orgánica de la Defensoría del Pueblo y sus modificatorias; de conformidad con lo señalado por el artículo 6° y los literales d) y q) del artículo 7° del Reglamento de Organización y Funciones de la Defensoría del Pueblo, aprobado por Resolución Defensorial Nº 0012-2011/DP; en atención a lo dispuesto por la Resolución Ministerial Nº 004-2016-PCM; de acuerdo a lo previsto por la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2º Edición", aprobada por Resolución Nº 129-2014/CNB-INDECOPI; y estando al encargo efectuado mediante la Resolución Defensorial Nº 004-2011/DP;

SE RESUELVE:

Artículo Primero.- **APROBAR** los documentos relacionados a la implementación del Sistema de Seguridad de la Información en la Defensoría del Pueblo, en el marco de lo dispuesto por la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2º Edición", aprobada por Resolución Nº 129-2014/CNB-INDECOPI, siendo las siguientes:

- "Alcance del Sistema de Gestión de Seguridad de la Información" de la Defensoría del Pueblo, el mismo que consta de diez (10) páginas.
- "Funciones y Responsabilidades de la Seguridad de la Información" de la Defensoría del Pueblo, el mismo que consta de nueve (09) páginas.
- "Metodología de Evaluación y Tratamiento de Riesgos" de la Defensoría del Pueblo, el mismo que consta de veinticinco (25) páginas.

Defensoría del Pueblo

Artículo Segundo.- **ENCARGAR** a la Oficina de Tecnología de la Información y Telecomunicaciones la publicación de la presente resolución en el Portal de Transparencia de la Defensoría del Pueblo.

Regístrese, comuníquese y publíquese.

Eduardo Vega Luna
DEFENSOR DEL PUEBLO (e)

ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Código:	SGSI-DP-002
Versión:	1.2
Fecha de la versión:	25/01/2015
Creado por:	Ing. CIP Maurice Frayssinet Delgado
Aprobado por:	
Nombre del archivo:	SGSI-DP-002.docx
Nivel de confidencialidad:	Público

Historial de Revisiones

Fecha	Versión	Modificado/Creado por	Descripción de la modificación
19/05/2015	1.0	M. Frayssinet	Creación del primer documento
20/11/2015	1.1	F.Neira	Revisión ortográfica
25/01/2016	1.2	F.Neira	Adaptación a la RM 004-2016-PCM

Aprobación

Fecha	Nombre	Cargo	Sello y Firma

Mejora Continua

Fecha	Revisor/Auditor	Resumen Observaciones

DEFENSORIA DEL PUEBLO - Oficina de Asesoría Jurídica -

Contenido

DEFENSORÍA DEL PUEBLO · Oficina de Asesoría Jurídica ·

1. Presentación

La planificación para la implementación de un SGSI es una etapa ineludible, por tanto, definir el alcance para la implementación del sistema en una organización es uno de los primeros aspectos que se debe considerar. Teniendo en cuenta que existen organizaciones que difieren en tamaño por el número de empleados, volumen de información manejada, número de clientes, volúmenes de activos físicos y lógicos, número de sedes u oficinas, entre otros elementos, se hace necesario determinar en qué áreas o dependencias de la organización se desea implantar el SGSI como primera medida y en cuáles, posteriormente. Las primeras áreas que se deben considerar son aquellas que, por sus funciones y responsabilidades ayudan, en primera instancia, a dar cumplimiento a la misión institucional.

Recordando las familias de la serie ISO 27001, la norma ISO 27003: 2010 (Guía para la Implementación de un Sistema de Gestión de Seguridad de la Información), orienta el diseño de la norma ISO/IEC 27001 para la iniciación de un proyecto de implantación de un SGSI. En él se describe el proceso de especificación del SGSI y el diseño, desde el inicio hasta la generación de la ejecución de los proyectos que abarquen las actividades de planificación, de preparación, antes de la implementación real.

2. Referencias Normativas

- Ley N° 27444, Ley del Procedimiento Administrativo General y sus modificatorias.
- Ley N° 29733, Ley de Protección de Datos Personales.
- Ley N° 28612, Ley que norma el Uso, Adquisición y Adecuación del Software en la Administración Pública, sus modificatorias, sus ampliatorias y su Reglamento.
- Ley N° 28493, Ley que regula el uso del Correo Electrónico comercial no solicitado (SPAM).
- Ley N° 27269, Ley de Firmas y Certificados Digitales, sus modificatorias, sus ampliatorias, su Reglamento y complementarios.
- Ley N° 28612, Ley que norma el Uso, Adquisición y Adecuación del Software en la Administración Pública.
- Ley N° 27806, Ley que aprueba la Ley de Transparencia y Acceso a la Información Pública y su Reglamento.
- Ley N° 27309, Ley que incorpora los Delitos Informáticos al Código Penal.
- Decreto Supremo N° 070-2011-PCM, que modifica el Reglamento de la Ley N° 27269, Ley de Firmas y Certificados Digitales, y establece normas aplicables al procedimiento registral en virtud del Decreto Legislativo N° 681 y ampliatorias.

DEFENSORIA DEL PUEBLO - Oficina de Asesoría Jurídica -

- Decreto Supremo N° 066-2011-PCM que aprueba el "Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana 2.0".
- Resolución de Contraloría N° 320-2006-CG.
- Resolución Ministerial N°004-2016-PCM que aprueba el uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 27001:2014.
- Resolución Ministerial N° 246-2007-PCM que aprueban uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 17799:2007.

3. Alcance del SGSI

3.1. Mapa de Procesos

La Defensoría del Pueblo tiene distribuidos sus procesos según el siguiente mapa de procesos:

Procesos Estratégicos:

- Comunicaciones e Imagen Institucional.
- Cooperación Internacional e Inversiones.
- Gestión Estratégica.
- Gestión de Seguridad de la Información.

Procesos Operativos:

- Gestiona de Atención al Ciudadano
- Gestión de Adjuntías.

Procesos de Apoyo:

- Administración y Finanzas.
- Tecnologías de la Información y Telecomunicaciones.
- Asesoría Jurídica.
- Recursos Humanos
- Planificación y Presupuesto

3.2. Selección del proceso para el alcance

El proceso seleccionado para el alcance del SGSI es:

"Gestión de Atención al Ciudadano"

3.3. Límites

- Solo se contemplara dentro del proceso de "Gestión de Atención al Ciudadano" la recepción o apertura de los casos.
- Contempla el registro en los sistemas de información
- Solo aplica a la oficina principal de Lima, ubicada en Jr Ucayali N° 394 -398 - Cercado (Lima)

3.4. Exclusiones

- No incluye el traslado o ambiente físico de los expedientes
- Los demás procesos no nombrados en el presente documento son excluidos para la implementación y ejecución del SGSI.
- No se contemplan las oficinas a nivel nacional

METODOLOGÍA DE EVALUACIÓN Y TRATAMIENTO DE RIESGOS

Código:	SGSI-DP-004
Versión:	1.2
Fecha de la versión:	25/01/2016
Creado por:	Ing. CIP Maurice Victor Frayssinet Delgado
Aprobado por:	
Nombre del archivo:	SGSI-DP-001.docx
Nivel de confidencialidad:	Público

Historial de Revisiones

Fecha	Versión	Modificado/Creado por	Descripción de la modificación
05/06/2015	1.0	M. Frayssinet	Creación del primer documento
20/11/2015	1.1	F.Neira	Revisión ortográfica
25/01/2016	1.2	F.Neira	Adaptación a la RM 004-2016-PCM

Aprobación

Fecha	Nombre	Cargo	Sello y Firma

Mejora Continua

Fecha	Revisor/Auditor	Resumen Observaciones

DEFENSORIA DEL PUEBLO · Oficina de Tecnología de la Información y Telecomunicaciones · REPÚBLICA DEL PERÚ

DEFENSORIA DEL PUEBLO · Oficina de Asesoría Jurídica · REPÚBLICA DEL PERÚ

Contenido

1. Objetivo

El presente documento define los lineamientos y procedimiento para realizar, dentro de la Defensoría del Pueblo, la identificación, análisis, evaluación y tratamiento de los riegos derivados de la seguridad de la información.

Esta metodología pretende implementar una adecuada gestión de los riesgos para tener un adecuado nivel de confidencialidad, integridad y disponibilidad de la información.

2. Alcance

Este procedimiento está definido para la adecuada gestión de riesgos dentro del marco del SGSI en la Defensoría del Pueblo. El alcance está enmarcado en el ciclo de gestión de riesgos enmarcado en la norma NTP-ISO/IEC 27001:2014.

3. Definiciones

3.1. **Activo:** Todo aquello que tenga valor para la Institución.

Tipos:

- Información; tal como una base de datos, un reporte, file de documentos.
- Software; tal como un programa de computadora.
- Físicos; tal como una computadora.
- Servicios; tal como courier, mantenimiento de computadoras.
- Personas; sus calificaciones, habilidades y experiencia.

3.2. **Confidencialidad:** Propiedad que determina que la información no esté disponible, ni sea divulgada a personas, entidades o procesos no autorizados.

3.3. **Disponibilidad:** Propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada.

3.4. **Estimación del Riesgo:** Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

3.5. **Identificación de Riesgos:** Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

3.6. **Impacto:** Es la consecuencia de la explotación de una vulnerabilidad por una amenaza debido a la falta o falla de controles, generando pérdida en confidencialidad, integridad y disponibilidad de la información u otros activos.

3.7. **Integridad:** Propiedad de salvaguardar la exactitud e integridad de los activos.

3.8. **Inventario de Activos:** Es un registro conformado por los activos de información que tienen valor para la Defensoría del Pueblo y que están dentro del alcance del SGSI.

3.9. **Probabilidad:** Es la posibilidad de que un evento cualquiera ocurra o no. A mayor probabilidad del evento existe más posibilidad de que ocurra, es decir, existen buenas razones para creer que sucederá.

3.10. Propietario: Identifica a la persona o la entidad que tiene la responsabilidad gerencial aprobada de controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos.

3.11. **Riesgo:** Es la probabilidad de que una amenaza en particular explote una vulnerabilidad causando un impacto negativo sobre los activos.

4. Desarrollo de la metodología

4.1. Identificación de Activos

Se aplica el formato SGSI-DP-091.xls

ORGANIZACION

ORGANIZACIÓN			
Correlativo	Unidad Operativa/Función	Proceso/Subproceso	Dueño del Proceso/Subproceso
1	VENTAS	VENTAS AL CONTADO	Gerente de ventas
2	VENTAS	VENTAS AL CONTADO	Gerente de ventas
3	VENTAS	VENTAS AL CONTADO	Gerente de ventas

Correlativo: Número correlativo para identificar la cantidad total de activos de información que se van identificando.

Proceso/Subproceso: Identificación del proceso o subproceso donde se encuentra el activo de información.

Dueño del Proceso: Consignar el responsable o dueño del proceso en donde se encuentra el activo definido.

ACTIVO DE INFORMACIÓN						
Código	Nombre Activo	Descripción	Tipo	Clasificación	Propietario (No se requiere en la nueva NTP ISO/IEC 27001:2014)	Usuario
Eje-001	Windows 7 Profesional	Sistema Operativo usado en los	Software	Activo de Soporte	Gerencia TI	Vendedores
Eje-002	Base de dato de clientes	Base de datos electronica de clientes	Información	Activo Primario	Gerencia TI	Vendedores
Eje-003	MS Office 2010	Software ofimatico word excel, etc	Software	Activo de Soporte	Gerencia TI	Vendedores

ACTIVO DE INFORMACIÓN

Código: Se debe llevar una codificación interna que permita identificar claramente los activos. Esta debe ser definida por el Oficial de Seguridad de la Información.

Nombre Activo: Definir el nombre del activo como lo conoce el propietario del mismo, es decir, en los términos de su uso día a día. Evitar usar palabra técnicas que dificulten su identificación.

Descripción: Agregar una descripción que nos explique, un poco para que nos sirve este activo o cuál es su necesidad dentro del proceso.

Tipo: Define el tipo de Activo según la tabla adjunta en el archivo Excel.

Clasificación: La clasificación se determina de manera automática según el tipo de activo siendo las dos opciones: Activo Primario y Activo de Soporte.

Propietario: Define al propietario del activo (No es obligatorio en el nuevo enfoque de la norma ISO/IEC 27001:2013).

Usuario: Aquel que hace uso del activo como parte de su proceso cotidiano dentro de la organización.

LEY DE PROTECCION DE DATOS PERSONALES

LEY PROTECCIÓN DATOS PERSONALES		
¿Es un dato personal? (S/N)	¿Es un dato personal sensible? (S/N)	¿Es un dato sensible de los clientes? (S/N)
N	N	N
S	S	S
N	N	N

Se debe contestar S (SI) o N (No) para aplicar las tres preguntas referidas y en cumplimiento a la ley de datos personales

UBICACIÓN

UBICACIÓN	
Ubicación Física	Ubicación Electrónica
Local Lima	
Local Lima	192.168.10.231
Local Lima	

Se debe definir en la matriz la ubicación física y/o electrónica del activo de información.

VALORACION

Aspecto de Seguridad afectado por el riesgo			IMPACTO
C	I	D	
1	1	1	No Significativo
1	1	2	Menor
1	1		Significativo
1	2	1	Menor
1	2	2	Moderado
1	2		Significativo
1		1	Significativo
1		2	Significativo
1			
2	1	1	Menor
2	1	2	Moderado
2	1		Significativo
2	2	1	Moderado
2	2	2	Moderado
2	2		Significativo
2		1	Significativo
2		2	Significativo
2			
	1	1	Significativo
	1	2	Significativo
	1		
	2	1	Significativo
	2	2	Significativo
	2		
		1	
		2	

Tabla de Valorización de Confidencialidad

Valor	Clasificación	Definición	Consecuencia
10	Alta	Es la información o recurso que debe ser divulgada sólo a fuentes autorizadas, controladas y debidamente identificadas. Debe ser modificada y leída por un grupo reducido de personas autorizadas y claramente identificadas.	La divulgación no autorizada produce: - Pérdida de la ventaja competitiva. - Uso malicioso en contra de la Defensoría del Pueblo. - Pérdidas financieras que no pueden ser absorbidas por la Defensoría del Pueblo. - Demandas legales que dañan la imagen y confianza pública de la Defensoría del Pueblo.
5	Media	Es la información que debe ser divulgada sólo al personal de las áreas que la manejan y modificada sólo por personas autorizadas e individualizadas.	La divulgación no autorizada produce: - Uso malicioso en contra de la imagen o situaciones puntuales. - Pérdidas financieras que pueden ser absorbidas por la Defensoría del Pueblo. - No se producen demandas legales.
1	Baja	Es la información que puede ser divulgada al público en general, pero que sólo puede ser modificada por personas autorizadas.	La divulgación no autorizada no representa perjuicio para la Defensoría del Pueblo.

Tabla de Valorización de Integridad

Valor	Clasificación	Criterio	Consecuencia
3	Alta	Es la información o recurso que al ser modificado, intencional o casualmente, por personas o procesos autorizados o no autorizados provoca daños de gran magnitud.	La falta de integridad produce daños de gran magnitud los que se pueden expresar como: - Pérdidas económicas (pérdida, incumplimiento de metas). - Falla de los procesos informáticos (incapacidad de ejecutarlos por un periodo de tiempo más allá de lo estimado como manejable). - Daño de la imagen de la Defensoría del Pueblo (daño a nivel nacional e internacional que no se puede reparar en el corto plazo). - Pérdida de la confianza de los usuarios.

Valor	Clasificación	Criterio	Consecuencia
2	Media	Es la información o recurso que al ser modificado, intencional o casualmente, por personas o procesos autorizados o no autorizados provoca daños de mediana magnitud.	La falta de integridad produce daños de mediana magnitud los que se pueden expresar como: - Pérdidas económicas (menor ganancia, incumplimiento de metas en menor escala). - Falla de los procesos informáticos (incapacidad de ejecutarlos por un periodo de tiempo que está en el límite superior de lo estimado como manejable). - Daño de la imagen de la Defensoría del Pueblo (daño a nivel nacional, se puede reparar en el corto plazo). - No se pierde la confianza de los usuarios.
1	Baja	Es la información o recurso que al ser modificado, intencional o casualmente, por personas o procesos autorizados o no autorizados provoca daños de pequeña magnitud.	La falta de integridad produce daños de pequeña magnitud los que se pueden expresar como: - Pérdidas económicas (no impacta las ganancias, se cumplen las metas). - Falla de los procesos informáticos (incapacidad de ejecutarlos por un período de tiempo pero este es manejable). - Daño de la imagen de la Defensoría del Pueblo (daño a nivel nacional que puede no ser percibido y se puede reparar prontamente). - No se pierde la confianza de los usuarios.

Tabla de Valorización de Disponibilidad

Valor	Clasificación	Definición	Consecuencia
3	Alta	Es información o activo indispensable para la continuidad de la Defensoría del Pueblo. El recurso principal y el alternativo no pueden faltar por un período prolongado de tiempo en horarios críticos.	La falta de disponibilidad por períodos prolongados produce: - Incumplimiento a los acuerdos de nivel de servicio. La transición entre el recurso principal y el alternativo no debe impactar el acuerdo de servicio. - Perjuicios legales que afectan la imagen de la Defensoría del Pueblo. - Perjuicios económicos que no pueden ser absorbidos por la Defensoría del Pueblo. - Problemas sindicales.

Valor	Clasificación	Definición	Consecuencia
2	**Media**	La disponibilidad de la información es necesaria para la continuidad de la Defensoría del Pueblo, pero existen canales alternativos para contrarrestar una pérdida de disponibilidad en un tiempo razonable. El recurso principal y el alternativo pueden quedar fuera de servicio por un periodo mínimo de tiempo en horarios críticos.	La falta de disponibilidad produce: - Que los niveles de servicio acordados se puedan ver afectados en la transición entre el medio principal y el alternativo. - Perjuicios legales que no comprometen la imagen de la Defensoría del Pueblo. - Perjuicios económicos que pueden ser absorbidos por la Defensoría del Pueblo. - No hay problemas sindicales.
1	**Baja**	Es información o activos de apoyo o secundarios para el negocio. La información se encuentra duplicada en varias fuentes. Si no está disponible no compromete procesos operativos importantes	La falta de disponibilidad produce: - Que los niveles de servicio acordados para los procesos operativos importantes, no se ven afectados. - Problemas administrativos y operativos no significativos. - Perjuicios económicos que no son significativos. - No hay perjuicios legales. - No hay problemas sindicales.

4.2. Identificación de amenazas

Amenaza: Es un evento que potencialmente puede causar daño. Para la identificación de las amenazas se utilizará la tabla de amenazas y vulnerabilidades (ver Anexo 01 - Tabla de Amenazas).

ACTIVO	AMENAZA

4.3. Identificación de Vulnerabilidades

Vulnerabilidad: Es una debilidad que puede ser explotada por una amenaza. Para la identificación de las vulnerabilidades se utilizará la tabla de amenazas y vulnerabilidades (ver Anexo 02 - Tabla de Vulnerabilidades).

ACTIVO	AMENAZA	VULNERABILIDAD

4.4. Determinación del Impacto en la Institución

Finalmente se determina el impacto de acuerdo a la siguiente tabla:

a. Tabla de Valorización del Impacto del Riesgo

Nivel	Descripción	Impacto en la Institución
5	**Catastrófico**	Impacta en forma severa en la Defensoría del Pueblo al punto de comprometer la confidencialidad o integridad de información crítica de la Institución o la continuidad de las operaciones por paralización de los servicios críticos más allá de los tiempos tolerables por el negocio. El impacto es a toda la Institución y su efecto se siente en todo el personal involucrado.
4	**Significativo**	Impacta en forma grave a un área o servicio específico de la Defensoría del Pueblo, se puede llegar a comprometer documentos internos clasificados como confidenciales, paralizar o retrasar procesos claves de la Defensoría del Pueblo por un tiempo considerable. Su efecto está limitado dentro de la Defensoría del Pueblo.
3	**Moderado**	El impacto sobre la confidencialidad, integridad y disponibilidad de la información es limitado en tiempo y alcance. Su efecto es para un proceso de soporte o actividad específica que puede subsanarse en corto plazo.
2	**Menor**	El impacto es leve y se puede prescindir del mismo en un tiempo limitado.

1	No Significativo	No representa un impacto importante para la Defensoría del Pueblo.

4.5. Determinación de la Probabilidad de Ocurrencia

Finalmente se determina la probabilidad de ocurrencia.

ACTIVO	AMENAZA	VULNERABILIDAD	¿Qué afecta en los activos de información?				RIESGO EFECTIVO	
			C	I	D	VALOR CID	IMPACTO	PROBABILIDAD

Para este caso utilizaremos los siguientes valores

Valor	Clasificación	Definición
1	Muy Baja	El evento no ocurre nunca o casi nunca. Ha ocurrido al menos 1 vez al año.
2	Baja	Si bien el evento puede ocurrir el periodo entre uno y otro evento puede ser muy grande. Al menos 2 veces al año.
3	Moderada	Es posible que ocurra el evento con una frecuencia baja. 3 o 4 veces al año.
4	Alta	Existen antecedentes de que el evento ocurrirá, dentro de un plazo de tiempo que implique una acción para enfrentarlo pero la frecuencia no es alta. 1 vez al mes.
5	Muy Alta	El evento se sabe que ocurre con cierto grado de certeza y que la frecuencia es alta. 1 vez a la semana o más.

4.6. Determinación del Riesgo Efectivo

El riesgo efectivo es la medida del daño probable causado por una amenaza que se materializa en un activo.

ACTIVO	AMENAZA	VULNERABILIDAD	¿Qué afecta en los activos de información?				RIESGO EFECTIVO				
			C	I	D	VALOR CID	IMPACTO	PROBABILIDAD	NIVEL DE RIESGO	NOMBRE DEL RIESGO	CÓDIGO DE RIESGO

Con el valor obtenido del producto del Impacto por la Probabilidad obtenemos el Riesgo, para esta actividad utilizaremos la Tabla de Valorización del Riesgo.

4.7. Determinación del Riesgo Residual

Es la determinación de riesgo cuando ya se ha aplicado las medidas de control previstas. Los valores a utilizar, se hacen sobre la premisa de controles implementados.

De forma similar que el riesgo efectivo, para el riesgo residual utilizaremos la Tabla de Valorización del Riesgo.

CONTROL EXISTENTE	¿Qué afecta en los activos de información?				RIESGO RESIDUAL		
	C	I	D	VALOR CID	IMPACTO	PROBABILIDAD	NIVEL DE RIESGO

a. Tabla de Valorización del Riesgo

Tabla de Valorización de Riesgos

Impacto		Probabilidad		Riesgo	
Catastrófico	5	Muy Alta	5	Extremo	25
Significativo	4	Muy Alta	5	Extremo	20
Moderado	3	Muy Alta	5	Extremo	15
Menor	2	Muy Alta	5	Alto	10
No Significativo	1	Muy Alta	5	Mediano	5
Catastrófico	5	Alta	4	Extremo	20
Significativo	4	Alta	4	Extremo	16
Moderado	3	Alta	4	Alto	12
Menor	2	Alta	4	Mediano	8
No Significativo	1	Alta	4	Bajo	4
Catastrófico	5	Moderada	3	Extremo	15
Significativo	4	Moderada	3	Alto	12
Moderado	3	Moderada	3	Alto	9
Menor	2	Moderada	3	Mediano	6
No Significativo	1	Moderada	3	Bajo	3
Catastrófico	5	Baja	2	Alto	10
Significativo	4	Baja	2	Mediano	8
Moderado	3	Baja	2	Mediano	6
Menor	2	Baja	2	Bajo	4
No Significativo	1	Baja	2	No Significativo	2
Catastrófico	5	Muy Baja	1	Mediano	5
Significativo	4	Muy Baja	1	Bajo	4
Moderado	3	Muy Baja	1	Bajo	3
Menor	2	Muy Baja	1	No significativo	2
No Significativo	1	Muy Baja	1	No significativo	1

Nivel de Riesgo:

Del 1 a 2 → No Significativo
Del 3 a 4 → Bajo
Del 5 a 8 → Mediano
Del 9 a 12 → Alto
Del 15 a 25 → Extremo

Los riesgos serán clasificados de acuerdo a niveles, según su grado de exposición, lo cual se muestra en la siguiente tabla:

Nivel de Riesgo	Descripción de las Consecuencias
Extremo	Puede afectar seriamente a la Defensoría del Pueblo, en términos de paralización de las operaciones a la imagen de la Defensoría del Pueblo. Requiere acción correctiva inmediata más allá del tiempo tolerable, pérdidas considerables o demandas legales y daño considerable.
Alto	Puede afectar los niveles de operación y servicio de la Defensoría del Pueblo, incumplimiento de metas, y divulgación no autorizada de información fuera de la Defensoría del Pueblo. Requiere una acción correctiva sujeta a la discreción de la Alta Dirección en términos de plazos y compromisos.
Mediano	Afecta a los activos de información de soporte a los activos principales, puede afectar la disponibilidad en áreas específicas dela Defensoría del Pueblo. La divulgación no autorizada no representa perjuicio importante para la Defensoría del Pueblo.
Bajo	No causa un efecto considerable en la Defensoría del Pueblo. Usualmente son aceptados sin revisión.
No Significativo	El efecto para la Defensoría del Pueblo es insignificante. Usualmente no se les considera para la gestión de riesgos.

b. Mapa de Riesgos

Finalmente se utiliza el siguiente mapa de calor, para presentar los riesgos.

IMPACTO	Catastrófico	5	MEDIANO	ALTO	EXTREMO	EXTREMO	EXTREMO
	Significativo	4	BAJO	MEDIANO	ALTO	EXTREMO	EXTREMO
	Moderado	3	BAJO	MEDIANO	ALTO	ALTO	EXTREMO
	Menor	2	NO SIGNIFICATIVO	BAJO	MEDIANO	MEDIANO	ALTO
	NO Significativo	1	NO SIGNIFICATIVO	NO SIGNIFICATIVO	BAJO	BAJO	MEDIANO
			1	2	3	4	5
			Muy Baja	Baja	Moderada	Alta	Muy Alta
					PROBABILIDAD		

4.8. Tratamiento del riesgo

La Defensoría del Pueblo reconoce los siguientes niveles de riesgos:
"Extremo", "Alto", "Mediano", "Bajo y "No Significativo".
Para la etapa de tratamiento del riesgo, se han considerado como aceptables los riesgos definidos como:
"Mediano", "Bajo" y "No Significativo".
Para los riesgos de nivel "Extremo" y "Alto" se procederán a evaluar las siguientes opciones de tratamiento de riesgo:

La decisión sobre el tratamiento de un riesgo se realiza en cada ciclo de evaluación, la cual se realizará una vez al año o cuando ocurran cambios en los procesos del SGSI. Los planes de tratamiento de riesgo, son revisados con periodicidad no mayor a un año por parte de la Alta Dirección, los nuevos riesgos efectivos son medidos y comparados con los riesgos residuales estimados.

ANEXOS

Anexo 1 Tabla de Amenazas

Codigo	Amenaza	Tipo
AM1	Incendio	Daño físico
AM2	Daño por agua	
AM3	Contaminación	
AM4	Accidente mayor	
AM5	Destrucción del equipo o los medios	
AM6	Polvo, corrosión, congelación	
AM7	Fenómeno climático	Eventos naturales
AM8	Fenómeno sísmico	
AM9	Fenómeno volcánico	
AM10	Fenómeno meteorológico	
AM11	Inundación	
AM12	Fallas del sistema de aire acondicionado o del suministro de agua	Pérdida de servicios esenciales
AM13	Pérdida del suministro de electricidad	
AM14	Falla del equipo de telecomunicaciones	
AM15	Radiación electromagnética	Perturbación debido a radiación
AM16	Radiación térmica	
AM17	Pulsos electromagnéticos	
AM18	Intercepción de señales de interferencia comprometedoras	
AM19	Espionaje remoto	
AM20	Interceptación de comunicaciones	
AM21	Robo de medios o documentos	
AM22	Robo de equipos	
AM23	Hallazgo de medios reciclados o descartados	

Código	Amenaza	Tipo
AM24	Divulgación	Compromiso de la información
AM25	Datos de fuentes no confiables	
AM26	Adulteración del Hardware	
AM27	Adulteración del software	
AM28	Detección de posición	
AM29	Falla de equipo	Fallas técnicas
AM30	Mal funcionamiento del equipo	
AM31	Saturación del sistema de información	
AM32	Mal funcionamiento del software	
AM33	Uso no autorizado del equipo	Acciones no autorizadas
AM34	Copia fraudulenta del software	
AM35	Uso de software falsificado o copiado	
AM36	Corrupción de datos	
AM37	Procesamiento ilegal de datos	
AM38	Error en el uso	Compromiso de funciones
AM39	Abuso de derechos	
AM40	Falsificación de derechos	
AM41	Negación de acciones	
AM42	Ruptura en la disponibilidad del personal	
AM43	Hacking	Hacker, cracker
AM44	Ingeniería social	
AM45	Intrusión en el sistema, incursiones	
AM46	Acceso no autorizado al sistema	
AM47	Crimen informático (acoso cibernético)	
AM48	Acto fraudulento (reproducción de archivos, suplantación, intercepción)	

Código	Amenaza	Tipo
AM49	Soborno informático	Criminal informático
AM50	Falsificación o usurpación de la dirección	
AM51	Intrusión en el sistema	
AM52	Bomba/Terrorismo	Terrorismo
AM53	Equipo de guerra informática	
AM54	Ataque al sistema (ej. DDOS)	
AM55	Penetración en el sistema	
AM56	Adulteración del sistema	
AM57	Ventaja de defensa	Espionaje
AM58	Ventaja política	
AM59	Explotación económica	
AM60	Robo de información	
AM61	Intrusión en la privacidad personal	
AM62	Asalto a un empleado	Gente de adentro de la institución (empleados mal capacitados, resentidos, maliciosos, negligentes, deshonestos o despedidos)
AM63	Chantaje	
AM64	Búsqueda de información propietaria	
AM65	Abuso informático	
AM66	Fraude y robo	
AM67	Soborno por información	
AM68	Ingreso de datos falsificados o corruptos	
AM69	Intercepción	
AM70	Códigos maliciosos (ej. Virus, bomba lógica, troyano)	
AM71	Venta de información personal	
AM72	Disfunciones del sistema (bugs)	
AM73	Intrusión en el sistema	

Codigo	Amenaza	Tipo
AM74	Sabotaje al sistema	

Anexo 2Tabla de Vulnerabilidades

Codigo	Vulnerabilidad	Categoria
VU1	Mantenimiento insuficiente / instalación fallida de medios de almacenamiento	Hardware
VU2	Falta de esquemas de reemplazo periódicos	
VU3	Susceptibilidad a la humedad, al polvo y a la suciedad	
VU4	Sensibilidad a la radiación electromagnética	
VU5	Falta de control eficiente del cambio de configuración	
VU6	Susceptibilidad a variación de voltaje	
VU7	Susceptibilidad a variaciones de temperatura	
VU8	Almacenamiento no protegido	
VU9	Falta de cuidado al descartarlo	
VU10	Copia no controlada	
VU11	Pruebas al software inexistentes o insuficientes	Software
VU12	Errores conocidos en el software	
VU13	No hacer "logout" cuando se sale de la estación de trabajo	
VU14	Disposición o reutilización de medios de almacenamiento sin borrar apropiadamente	
VU15	Falta de evidencia de auditoria	
VU16	Asignación equivocada de derechos de acceso	
VU17	Software ampliamente distribuido	
VU18	Aplicar programas de aplicación a datos incorrectos en términos del tiempo	
VU19	Interfaz de usuario complicada	
U20	Falta de documentación	
VU21	Seteo incorrecto de parámetros	
VU22	Fechas incorrectas	
VU23	Falta de mecanismos de identificación y autentificación como la autentificación de usuarios	

Código	Vulnerabilidad	Categoria
VU24	Tablas de claves no protegidas	
VU25	Mala administración de claves	
VU26	Habilitación de servicios innecesarios	
VU27	Software inmaduro o nuevo	
VU28	Especificaciones no claras o incompletas para los desarrolladores	
VU29	Falta de control de cambios eficaz	
VU30	Descarga y uso incontrolado de software	
VU31	Falta de copias de respaldo	
VU32	Falta de protección física del edificio, puertas y ventanas	
VU33	No producir informes de gestión	
VU34	Falta de pruebas de envió o recepción de mensaje	
VU35	Líneas de comunicación no protegidas	
VU36	Tráfico delicado no protegido	
VU37	Juntas malas en el cableado	
VU38	Punto de falla única	Red
VU39	Falta de identificación y autentificación de emisor y destinatario	
VU40	Arquitectura de red insegura	
VU41	Transferencia de claves en claro	
VU42	Gestión inadecuada de la red (capacidad de recuperación del ruteo)	
VU43	Conexiones no protegidas de la red publica	
VU44	Ausencia del personal	
VU45	Procedimientos inadecuados del reclutamiento	
VU46	Capacitación de seguridad insuficiente	Personal
VU47	Uso incorrecto del software y hardware	
VU48	Falta de conciencia de seguridad	

Codigo	Vulnerabilidad	Categoría
VU49	Falta de mecanismos de monitoreo	
VU50	Trabajo no supervisado del personal externo o de limpieza	
VU51	Falta de políticas para el uso correcto de medios de telecomunicaciones y mensajería	
VU52	Uso inadecuado o negligente del control de acceso físico a edificios y ambientes	Sitio
VU53	Ubicaciones en una área susceptible a las inundaciones	
VU54	Red inestable de energía eléctrica	
VU55	Falta de protección física del edificio, puertas y ventanas	
VU56	Falta de un procedimiento formal para el registro y baja de usuarios	Institución
VU57	Falta de proceso formal para revisar el derecho de acceso (supervisión)	
VU58	Disposiciones inexistentes o insuficientes (respecto de la seguridad) en contratos con clientes y/o terceros	
VU59	Falta de procedimientos de monitoreo de instalaciones de procesamiento de la información	
VU60	Falta de auditorías regulares (supervisión)	
VU61	Falta de procedimientos de identificación y evaluación del riesgo	
VU62	Falta de informes de fallas registradas en los registros del administrador y del operador	
VU63	Respuesta inadecuada del mantenimiento del servicio	
VU64	Inexistencia o insuficiencia de acuerdo sobre el nivel de servicio	
VU65	Falta de procedimiento de control de cambios	
VU66	Falta de procedimiento formal para el control de la documentación de la Defensoría del Pueblo	
VU67	Falta de procedimiento formal para la supervisión del registro de la Defensoría del Pueblo	
VU68	Falta de proceso formal para autorización de información pública disponible	
VU69	Falta de asignación apropiada de responsabilidades de seguridad en la información	
VU70	Falta de planes de continuidad	
VU71	Falta de una política de uso de correos electrónicos	
VU72	Falta de procedimientos para introducir software en sistemas operativos	
VU73	Faltas de registro en los historiales del administrador y del operador	

Código	Vulnerabilidad	Categoría
VU74	Falta de procedimientos para manejo de la información clasificada	
VU75	Falta de responsabilidades sobre la seguridad de la información en las descripciones de puestos	
VU76	Ausencia o insuficiencia de disposiciones (concernientes a la seguridad de la información en contratos con empleados)	
VU77	Falta de proceso disciplinario definido en caso de incidentes en la seguridad de la información	
VU78	Falta de política formal sobre el uso de computadoras portátiles	
VU79	Falta de control de activos que se encuentran fuera del local	
VU80	Inexistencia o insuficiencia de la política de "escritorio despejado y pantalla despejada"	
VU81	Falta de autorización al acceso a las instalaciones de procesamiento de la información	
VU82	Falta de mecanismos de monitoreo establecidos para las rupturas de la seguridad	
VU83	Falta de revisiones regulares de la gestión	
VU84	Falta de procedimientos para reportar debilidades en la seguridad	
VU85	Falta de procedimientos sobre el cumplimiento de disposiciones respecto de derechos intelectuales	

FUNCIONES Y RESPONSABILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN

Código:	SGSI-DP-003
Versión:	1.2
Fecha de la versión:	25/01/2015
Creado por:	Ing. CIP Maurice Frayssinet Delgado
Aprobado por:	
Nombre del archivo:	SGSI-DP-003.docx
Nivel de confidencialidad:	Público

DEFENSORIA DEL PUEBLO - Oficina de Asesoría Jurídica

DEFENSORIA DEL PUEBLO - Oficina de Tecnologías de la Información y Telecomunicaciones

Historial de Revisiones

Fecha	Versión	Modificado/Creado por	Descripción de la modificación
19/05/2015	1.0	M. Frayssinet	Creación del primer documento
20/11/2015	1.1	F.Neira	Replanteo constitución CGSI y sus funciones, exclusión de funciones de auditores.
25/01/2016	1.2	F.Neira	Adaptación a la RM 004-2016-PCM

Aprobación

Fecha	Nombre	Cargo	Sello y Firma

Mejora Continua

Fecha	Revisor/Auditor	Resumen Observaciones

DEFENSORIA DEL PUEBLO - REPUBLICA DEL PERU - Oficina de Asesoría Jurídica

Contenido

1. Introducción

El presente documento contiene la estructura organizativa del Sistema de Gestión de Seguridad de la Información - SGSI de la Defensoría del Pueblo, alineado a lo establecido en la norma NTP-ISO/IEC 27001:2014. En este documento de delimitan y regulan las funciones de cada uno de los actores de la implementación del Sistema de Gestión de Seguridad de la Información.

2. Objetivos

- Establecer claramente las funciones y responsabilidades para la gestión y operación del Sistema de Gestión de Seguridad de la Información.
- Disponer de una adecuada separación de funciones que conlleve a organizar a la Defensoría del Pueblo en base a principios de Seguridad de la Información.

3. Alcance

La presente organización de la seguridad de la información es de alcance nacional, en todos los procesos y actividades desarrolladas en la institución.

4. Estructura organizativa

Las funciones para el mantenimiento y la mejora de la seguridad de la información se asignarán mediante los siguientes roles:

a) Defensor del Pueblo
b) Comité de Seguridad de la Información
c) Oficial de Seguridad de la Información
d) Propietarios de la Información
e) Custodio de la Información

DEFENSORIA DEL PUEBLO · Oficina de Asesoría Jurídica ·

5. Roles y responsabilidades del SGSI

5.1. Defensor del Pueblo

El Defensor del Pueblo es la máxima autoridad en seguridad de la información de la Institución.

Las responsabilidades del Defensor del Pueblo respecto a la seguridad de la información son:

a) Aprobar la política del Sistema de Gestión Seguridad de la Información (SGSI).

b) Aprobar el Plan Estratégico de Seguridad de la Información (PESI), proporcionar los recursos y la autoridad suficientes para llevarlos a cabo.

c) Aprobar la estructura organizativa interna de seguridad de la información.

d) Designar a los miembros del Comité de Seguridad de la Información, según lo establecido en el artículo 5 de la RM N°004-2016-PCM.

e) Designar al Oficial de Seguridad de la Información.

f) Promover y patrocinar la capacitación y concientización del personal de la Defensoría del Pueblo en materia de seguridad de la información.

5.2. Comité de Seguridad de la Información

El Comité de Seguridad de la Información es el máximo órgano en materia de Seguridad de la Información.

El Comité de Seguridad de la Información se reunirá, por lo menos, semestralmente para evaluar la situación institucional en materia de seguridad de la información y el plan de acción para mejorarla continuamente.

Las funciones del Comité de Seguridad de la Información son las siguientes:

a) Patrocinar y participar en la implementación, operación, monitoreo, revisión, mantenimiento y mejora continua del Sistema de Gestión Seguridad de la Información (SGSI).

b) Definir y evaluar el Plan Estratégico Institucional de Seguridad de la Información, garantizando que las metas de seguridad de la información sean identificadas y cumplidas, y que la

seguridad de la información sea parte del proceso de planificación institucional.

c) Definir, evaluar y garantizar que la continuidad del negocio se gestione.

d) Atender la respuesta a incidentes de seguridad de la información que hayan sido elevados a su competencia.

e) Garantizar el cumplimiento de las exigencias legales en materias de seguridad de la información y de protección de datos personales.

f) Patrocinar auditorías internas del SGSI a intervalos planificados.

g) Iniciar planes y programas para mantener la conciencia en seguridad de la información entre el personal de la Defensoría del Pueblo.

h) Proveer direcciones claras y un visible apoyo en la gestión para iniciativas de seguridad de la información.

i) Analizar las buenas prácticas de controles de seguridad a fin de proponer su estandarización al Oficial de Seguridad.

j) Apoyar en el cumplimiento de las exigencias legales en materias de seguridad de la información y de protección de datos personales.

k) Apoyar en la definición de la estrategia de capacitación y concientización en materia de seguridad de la información.

l) Las demás funciones que se le encarguen, y otras necesarias para cumplir con las disposiciones normativas en materia de seguridad de la información.

DEFENSORIA DEL PUEBLO - Oficina de Asesoría Jurídica

5.3. Oficial de Seguridad de la Información

El Oficial de Seguridad de la Información tiene la responsabilidad completa de la gestión de la Seguridad de la Información asegurando el correcto manejo de los activos de información. Coordina, implementa y controla las medidas técnicas y organizativas necesarias para garantizar la seguridad de la información y evitar su alteración, pérdida, procesamiento o acceso no autorizado.

Las funciones del Oficial de Seguridad de la Información son las siguientes:

a) Informar al Comité de Seguridad de la Información la situación institucional en materia de seguridad de la información.

b) Coordinar con los propietarios de los activos de la información sus requerimientos de seguridad, la ejecución de los procesos de análisis y evaluación de riesgos.

c) Promover y colaborar en el mantenimiento, difusión y aplicación de la política de seguridad de la información, así como en la redacción de las normas, procedimientos y guías de buenas prácticas que la desarrollen.

d) Asesorarse con el Comité de Seguridad de la Información en materia de procesos que se realizan en la Defensoría del Pueblo, activos de información importantes y procesamientos de la información.

e) Realizar la implementación, operación, monitoreo, revisión, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).

f) Elaborar y proponer el Plan Estratégico Institucional de Seguridad de la Información, identificando objetivos estratégicos y asegurando que la seguridad de la información sea parte del proceso de planificación institucional.

g) Dirigir las actividades proyectadas en los planes estratégicos, controlando su grado de ejecución y eficacia.

h) Proponer la estructura organizativa de Seguridad de la Información.

i) Proponer estrategias para la continuidad del negocio.

j) Elaborar el análisis y evaluación de la situación institucional en materia de seguridad de la información y proponer el plan de actuación para mejorarlo continuamente.

k) Identificar y proponer los cambios en seguridad de la información en respuesta a los cambios del ambiente organizacional, circunstancias del entorno, condiciones legales o cambios en el ambiente técnico.

l) Comunicar al Comité de Seguridad de la Información las amenazas, incidentes y debilidades emergentes.

m) Establecer de las condiciones mínimas contractuales, técnicas y legales, para la seguridad de la información y la protección de

datos personales por parte de terceros, así como el control de su cumplimiento y eficacia.

n) Homologar el procesamiento, en especial las aplicaciones informáticas y servicios de información, respecto a los requisitos de seguridad exigibles.

o) Las demás funciones que se le encarguen, y otras necesarias para cumplir con las disposiciones normativas en materia de seguridad de la información.

5.4. Propietarios de la Información

El Propietario de la Información es una persona designada por cada proceso de la organización. Es llamada también "responsable de la información" o "propietario de los activos de información" para todos los asuntos o temas de seguridad de la información relacionados con el procesamiento de datos dentro de este proceso de la organización en particular.

Las funciones del Propietario de la Información son las siguientes:

a) Identificar y clasificar los activos de su propiedad. Revisar periódicamente la clasificación de la información con la finalidad de verificar el cumplimiento de los requerimientos de seguridad de la Institución.

b) Autorizar el procesamiento de la información que está bajo su responsabilidad.

c) Valorar los riesgos de la información que está bajo su responsabilidad, o que se sometan a su consideración, y ordenar las actuaciones pertinentes. En caso de asumir riesgos, compartir riesgos o evitar riesgos, las acciones necesarias deben ser adoptadas desde el enfoque de seguridad de la organización.

d) Verificar que los controles o medidas de seguridad aplicados sean consistentes con la clasificación realizada.

e) Autorizar los accesos a la información que está bajo su responsabilidad.

f) Controlar la calidad y la eficiencia del procesamiento dentro de un ciclo de mejora continua.

g) Informará diligentemente de las alertas, incidencias o problemas de seguridad que detecte mediante los procedimientos de comunicación establecidos al efecto.

5.5. Custodios de la Información

El Custodio de los Activos de Información es el responsable del resguardo y de asegurar el buen uso de los activos de información; asimismo, del monitoreo del cumplimiento de los controles de seguridad en los activos que se encuentren bajo su administración.

Las funciones del Custodio de la Información son las siguientes:

a) Dar acceso a los usuarios de acuerdo con las especificaciones establecidas por los propietarios.

b) Administrar los accesos físicos o lógicos a los activos de información que permanecen bajo su custodia.

c) Cumplir con los controles implementados para la protección de los activos asignados para su custodia.

d) Administrar los procedimientos de respaldo, recuperación y restauración de información.

e) Reportar incidentes y debilidades de seguridad de la información.

f) En caso de identificar oportunidades de mejora, comunicarlas a los responsables de Seguridad de la Información inmediatos.