FIRMA DIGITAL
GRC GOBIERNO REGIONAL CAJAMARCA
Firmado digitalmente por ALIAGA INFANTE Reinaldo Javier FAU 20453744168 soft
Motivo: Soy el autor del documento
Fecha: 05.05.2020 14:00:36 -05:00

PLAN DEL PROYECTO PARA LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Código:	**SGSI-PL-001**
Versión:	1.0
Fecha de la versión:	05/05/2020
Creado por:	Ing. Reinaldo Javier Aliaga Infante Oficial de Seguridad de la Información
Aprobado por:	Ronald Heenry Velásquez Díaz Jefe del Centro de Información y Sistemas
Nivel de confidencialidad:	Baja

FIRMA DIGITAL
V°B° GRC GOBIERNO REGIONAL CAJAMARCA
Firmado digitalmente por VELASQUEZ DIAZ Ronald Heenry FAU 20453744168 soft
Motivo: Doy V° B°
Fecha: 05.05.2020 16:20:48 -05:00

Historial de Revisiones y modificaciones

Fecha	Versión	Modificado/Creado por	Descripción de la modificación
05/05/2020	1.0	Oficial de Seguridad de la Información	Creación del primer documento

Contenido

I. OBJETIVO, ALCANCE Y USUARIOS 3
II. DOCUMENTOS DE REFERENCIA 3
III. PROYECTO DE IMPLEMENTACIÓN DEL SGSI 3
3.1. OBJETIVO DEL PROYECTO 3
3.2. ENTREGABLES DEL PROYECTO 3
3.3. ENTREGABLES Y PLAZOS 4
3.4. ORGANIZACIÓN DEL PROYECTO 6
3.4.1. Patrocinador del Proyecto 6
3.4.2. Gerente del Proyecto 6
3.4.3. Equipo del Proyecto 6
3.5. RIESGOS DEL PLAN 6
3.6. REQUISITOS 8
3.7. HERRAMIENTAS UTILIZADAS EN EL PROYECTO 9
IV. GESTIÓN DE REGISTROS 9
V. ANEXO N° 01 10

I. OBJETIVO, ALCANCE Y USUARIOS

1.1. OBJETIVO

Definir el proyecto de implementación del Sistema de Gestión de Seguridad de la Información (en adelante SGSI), los documentos que se elaborarán, los plazos, las funciones y responsabilidades del proyecto en la sede del Gobierno Regional de Cajamarca (en adelante GORECAJ).

1.2. ALCANCE

Aplica a todas las actividades que serán realizadas dentro del proyecto de implementación del SGSI.

1.3. USUARIOS

- Miembros de la Alta Dirección del GORECAJ.
- Miembros del equipo del proyecto de implementación del SGSI del GORECAJ.
- Oficial de Seguridad de la Información del GORECAJ.

II. DOCUMENTOS DE REFERENCIA

- Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado.
- Ley N° 29733, Ley de Protección de Datos Personales.
- Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistema de Gestión de Seguridad de la Información. Requisito. 2da Edición"
- Resolución ministerial N° 166-2017-PCM, que modifican el artículo 5 de la R.M. N° 004-2016-PCM referente al Comité de Gestión de Seguridad de la Información.
- DECRETO LEGISLATIVO N° 1412, que aprueba la Ley de Gobierno Digital.

III. PROYECTO DE IMPLEMENTACIÓN DEL SGSI

3.1. OBJETIVO DEL PROYECTO

Implementar un SGSI basado en la Norma Técnica Peruana NTP ISO/IEC 27001:2014 en la sede del GORECAJ.

3.2. ENTREGABLES DEL PROYECTO

Durante el proyecto de implementación del SGSI en la Sede del Gobierno Regional de Cajamarca, los entregables del proyecto estarán clasificados en:

- **Procedimiento para control de documentos:** Documento que establece reglas de redacción, aprobación, distribución y actualización de documentos.
- **Procedimiento para identificación de requisitos:** Detallar el procedimiento donde se debe consignar las obligaciones legales, normativas, contractuales, entre otras.
- **Alcance del Sistema de Gestión de Seguridad de la Información**: Documento que define el alcance del SGSI; considerando los procesos, ubicaciones físicas, partes interesadas y la determinación de los aspectos internos y externos a la organización.
- **Política de seguridad de la información:** Documento que define la forma en que la dirección controla la gestión de la seguridad de la información.
- **Metodología de Gestión de Riesgos:** documento que describe los métodos y procedimientos que se deben emplear para la evaluación y tratamiento de los riesgos de la información.
- **Matriz de evaluación de riesgos:** Cuadro resultante de la evaluación de riesgos aplicando la metodología elegida por el GORECAJ.
- **Declaración de aplicabilidad (SOA):** Es un documento que determina los objetivos y la aplicabilidad de cada control establecido en el Anexo A de la NTP-ISO/IEC 27001:2014.
- **Plan de tratamiento de riesgos:** Documento donde se detallan los controles de seguridad adecuados para cada riesgo inaceptable de tal forma que se evidencia su tratamiento.
- **Procedimiento para Auditoría interna:** Documento que define la forma de realizar los programas de auditoría, la forma de realizar las auditorías, informe de resultados, entre otros.
- **Procedimiento para acciones correctivas:** Descripción detallada de las actividades realizadas como parte de las correctivas.

3.3. ENTREGABLES Y PLAZOS

Entregables

FASES	ACTIVIDADES	ENTREGABLES
4. Contexto de la Organización y	4.1. Comprender la organización y su	Acta de compromiso de la alta dirección

5. Liderazgo	contexto 4.2. Comprender las necesidades y expectativas de las partes interesadas 4.3. Determinar el alcance del SGSI Obtener apoyo institucional 4.4. SGSI 5.1. Liderazgo y compromiso 5.2. Política 5.3. Roles, responsabilidades y autoridades organizacionales	Acta de conformación del Comité de SGSI
		Procedimiento de control documental del SGSI
		Procedimiento para la identificación de requisitos
		Acta de Procesos del GORECAJ implicados en el SGSI
		Acta del alcance del SGSI
		Acta de asignación de responsabilidades
		Documento de política del SGSI
6. Planificación	6.1. Acciones para tratar los riesgos y oportunidades 6.1.2. Valoración del riesgo de seguridad de la información 6.1.3. Tiramiento de riesgos de seguridad de la información 6.2. Objetivos de seguridad de la información y planificación para conseguirlos	Metodología de evaluación de riesgos
		Inventario de Activos de Información
		Amenazas y Vulnerabilidades
		Matriz de evaluación de riesgos
		Declaración de aplicabilidad SOA
		Plan de Tratamiento de riesgos
7. Soporte	7.1. Recursos 7.2. Competencia 7.3. Concientización 7.4. Comunicación 7.5. Información documentada	Plan de sensibilización del SGSI
		Despliegue del plan de sensibilización en SI
		Mejora de documentación del SGSI
8. Operación	8.1. Planificación y control operacional 8.2. Evaluación de riesgos de seguridad de la información 8.3. Tratamiento de riesgos de seguridad de la información	Documento de evaluación y tratamiento de riesgos periódicos
		Procedimientos continuos de tratamiento de riesgos
		Tratamiento de riesgos de seguridad de la información
9. Evaluación de Desempeño y	Monitoreo, medición, análisis y evaluación	Plan Auditoría interna

10. Mejoras	Auditoría Interna Revisión por la gerencia	Informe de auditoría interna
		Plan de acciones correctivas y preventivas
		Informe de seguimiento a las no conformidades

Plazos

- Definido en el ANEXO N° 01

3.4. ORGANIZACIÓN DEL PROYECTO

3.4.1. Patrocinador del Proyecto

Proveerán los recursos necesarios para la ejecución del proyecto. Para el GORECAJ, el patrocinador será el Gerente de Planeamiento, Presupuesto y Acondicionamiento Territorial

3.4.2. Gerente del Proyecto

Oficial de Seguridad de la Información

3.4.3. Equipo del Proyecto

- Comité del SGSI, según Resolución Ministerial N° 166-2017-PCM deberá estar conformado por:
  - Gobernador Regional / Gerente General.
  - Directora Regional de Administración.
  - Gerente Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial.
  - Jefe del Centro de Información y Sistemas.
  - Director de Asesoría Jurídica.
  - Oficial de Seguridad de la Información del GORECAJ.
- Comité operativo de Seguridad de la Información: Estará conformado por el responsable de cada área inmersa en el **alcance del SGSI**.

3.5. RIESGOS DEL PLAN

La implementación de un SGSI implica un cambio de cultura organizacional, es por ende el total compromiso de todo el personal implicado en el proyecto. Los riesgos a los cuales nos podemos enfrentar en el proceso de implementación son los siguientes:

- Falta de respaldo de la alta dirección.
- Ausencia procesos y sub procesos mapeados de las áreas comprometidas en el alcance.
- Falta de presupuesto para la implementación del plan de tratamiento de riesgos resultante del proceso de análisis de riesgos.
- Falta de compromiso del personal de las áreas implicadas en el alcance.
- Falta de capacitación del personal implementador en gestión de procesos, entrega de servicios, desarrollo seguro y seguridad de la información.
- Ampliación de plazos en los entregables.

A continuación se definirá una pequeña matriz de riesgos, y el nivel de riesgo se definirá de acuerdo al siguiente criterio:

NIVEL DE RIESGO	RANGO DE VALORES
ALTO	>=4 y <=5
MEDIO	> 2 y < 4
BAJO	>= 1 y <=2

Cuadro N° 01: Valores de niveles de riesgo

NRO	RIESGO	PROBABILIDAD	IMPACTO	NIVEL RIESGO
1	Falta de respaldo de la Alta Dirección	0.9	5.0	4.5
2	Ausencia de procesos y sub procesos mapeados de las áreas comprometidas en el alcance	0.8	5.0	4.0
3	Falta de asignación de presupuesto para la implementación del plan de tratamiento de riesgos resultante del proceso de análisis de riesgos	0.5	5.0	2.0
4	Falta de compromiso del personal de las áreas implicadas en el alcance	0.9	5.0	4.5
5	Falta de capacitación del personal implementador en gestión de procesos, entrega de servicios, desarrollo seguro y seguridad de la información	0.3	5.0	1.5

6	Ampliación de plazos en los entregables	0.5	3.0	1.5

Cuadro N° 02: Matriz de nivel de riesgos de implementación del proyecto

NRO	RIESGO	MEDIDAS DE CONTINGENCIA PARA MITIGAR EL RIESGO
1	Falta de respaldo de la Alta Dirección	• Reuniones de socialización con Alta Dirección, informando sobre los beneficios de la implementación del proyecto. • Hacer de conocimiento los reglamentos establecidos por la Secretaría de Gobierno Digital.
2	Ausencia de procesos y sub procesos mapeados de las áreas comprometidas en el alcance	• Reuniones de socialización con la Alta Dirección y áreas usuarias inmersas en el alcance del proyecto. • Realizar levantamiento de información de procesos y subprocesos de áreas inmersas en el alcance del proyecto. • Formalizar procesos y sub procesos de áreas inmersas en el alcance del proyecto.
4	Falta de compromiso del personal de las áreas implicadas en el alcance	• Reuniones de socialización con el personal de las áreas implicadas en el alcance del proyecto, haciendo hincapié en los beneficios de la implementación del proyecto, y en la obligatoriedad de la implementación por parte de la Secretaría de Gobierno Digital.

Cuadro N° 03: Medidas para mitigación de riesgos de implementación del proyecto

3.6. REQUISITOS

3.6.1. Para el inicio de la implementación del proyecto

- Conformación del comité del SGSI.
- Plan Estratégico Institucional del GORECAJ
- Identificación de procesos: Los procesos de la entidad es la principal fuente de alimentación de datos para un SGSI.
- Fortalecimiento de capacidades: es importante que los participantes clave del proyecto conozcan los fundamentos básicos / intermedios de Seguridad de la Información basados en la Norma Técnica Peruana NTP-ISO/IEC-27001:2014.

3.6.2. Para la implementación del Proyecto

- Asesoramiento especializado, para el acompañamiento en el proceso de implementación.
- Análisis de vulnerabilidades de TI, para determinar el nivel de vulnerabilidades en aplicaciones, servicios y equipamiento de telecomunicaciones de la sede del GORECAJ.

3.7. HERRAMIENTAS UTILIZADAS EN EL PROYECTO

- El contenedor de los documentos del SGSI: mediante una carpeta compartida (creada en el servidor de archivos del GORECAJ) o mediante un sistema de gestión documental, se tendrá disponible los archivos generados en cada una de las etapas de implementación.
- Todos los miembros del equipo del proyecto tendrán acceso a esos documentos. Sólo el gerente del proyecto y miembros del equipo del proyecto estarán autorizados a realizar modificaciones y borrado archivos.
- Software ofimático, para elaboración de documentos del SGSI.
- Software para la gestión de riesgos de seguridad de la información, según corresponda.
- Entrevistas en sitio, según corresponda.
- Cuestionarios según corresponda.

IV. GESTIÓN DE REGISTROS

- La mejora continua de este documento.
- Los informes parciales de la implementación del proyecto
- Las incidencias producto de cambios o mejoras al proyecto

V. ANEXO N° 01

FASES	ACTIVIDADES	ENTREGABLES	TIEMPO DE IMPLEMENTACIÓN
4. Contexto de la Organización y 5. Liderazgo	4.1. Comprender la organización y su contexto 4.2. Comprender las necesidades y expectativas de las partes interesadas 4.3. Determinar el alcance del SGSI Obtener apoyo institucional 4.4. SGSI 5.1. Liderazgo y compromiso 5.2. Política 5.3. Roles, responsabilidades y autoridades organizacionales	Acta de compromiso de la alta dirección Acta de conformación del Comité de SGSI	03 meses
		Procedimiento de control documental del SGSI	
		Procedimiento para la identificación de requisitos	
		Acta de Procesos del GORECAJ implicados en el SGSI	
		Acta del alcance del SGSI	
		Acta de asignación de responsabilidades	
		Documento de política del SGSI	
6. Planificación	6.1. Acciones para tratar los riesgos y oportunidades 6.1.2. Valoración del riesgo de seguridad de la información 6.1.3. Tiramiento de riesgos de seguridad de la información 6.2. Objetivos de seguridad de la información y planificación para conseguirlos	Metodología de evaluación de riesgos	04 meses
		Inventario de Activos de Información	
		Amenazas y Vulnerabilidades	
		Matriz de evaluación de riesgos	
		Declaración de aplicabilidad SOA	
		Plan de Tratamiento de riesgos	
7. Soporte	7.1. Recursos 7.2. Competencia 7.3. Concientización 7.4. Comunicación 7.5. Información documentada	Plan de sensibilización del SGSI	02 meses
		Despliegue del plan de sensibilización en SI	
		Mejora de documentación del SGSI	
8. Operación	8.1. Planificación y control operacional	Documento de evaluación y tratamiento de riesgos periódicos	04 meses

	8.2. Evaluación de riesgos de seguridad de la información 8.3. Tratamiento de riesgos de seguridad de la información	Procedimientos continuos de tratamiento de riesgos	
		Tratamiento de riesgos de seguridad de la información	
9. Evaluación de Desempeño y 10. Mejoras	Monitoreo, medición, análisis y evaluación Auditoría Interna Revisión por la gerencia	Plan Auditoría interna	04 meses
		Ejecución e Informe de auditoría interna	
		Plan de acciones correctivas y preventivas	
		Informe de seguimiento a las no conformidades	