INSTITUTO GEOFÍSICO DEL PERÚ

Resolución de Gerencia General

N° 043-IGP/2020

Lima, 13 de Diciembre del 2020

VISTOS:

El Informe N° 0234-2020-IGP/GG-OPP y el Informe Legal N° 131-2020-IGP/GG-OAJ; y

CONSIDERANDO:

Que, mediante el Decreto Legislativo N° 136, se crea el Instituto Geofísico del Perú (IGP) como un Organismo Descentralizado del Sector Educación, cuya finalidad es la investigación científica, la enseñanza, la capacitación, la prestación de servicios y, la realización de estudios y proyectos, en las diversas áreas de la Geofísica;

Que, la Primera Disposición Complementaria Final del Decreto Legislativo N° 1013, Ley de Creación, Organización y Funciones del Ministerio del Ambiente, dispone la adscripción del IGP como un organismo público ejecutor del Ministerio del Ambiente;

Que, mediante el Decreto Supremo N° 001-2015-MINAM, se aprobó el reglamento de Organizaciones y Funciones (ROF) del Instituto Geofísico del Perú (IGP);

Que, el numeral 1 de la Décima Séptima Disposición Complementaria Final del Decreto de urgencia N° 021-2020 establece que Instituto Geofísico del Perú es el Ente Rector de las investigaciones teóricas y aplicadas en la Ciencia Geofísica orientada a la ejecución de la Política Nacional de Gestión del Riego de Desastres;

Que, mediante Resolución de Gerencia General N° 029-IGP/2020, se aprueba la Directiva DI 001-2020-IGP, Directiva que estable los lineamientos para la aprobación, modificación y derogación de documentos normativos;

Que, el numeral 8.1.3 de la citada Directiva indica que la aprobación del documento normativo en el caso de los procedimientos, se dan a través de una Resolución de Gerencia General;

Que, mediante la Resolución de Gerencia General 032-IGP/2020 se aprobó el procedimiento PR 005-2020-IGP Seguimiento, Medición, Gestión del Cambio y Revisión por la Dirección;

Que, mediante la Resolución de Gerencia General 036-IGP/2020 se aprobó el procedimiento PR 014-2020-IGP Desarrollo de Soluciones Informáticas;

Que, mediante Informe N° 0234-2020-IGP/GG-OPO, de fecha 13 de diciembre del 2020, el Jefe de la Oficina de Planeamiento y Presupuesto, emitió opinión técnica favorable sobre la propuesta de modificación de los procedimientos PR 005-2020-IGP Seguimiento, Medición, Gestión del Cambio y Revisión por la Dirección y PR 014-2020-IGP Desarrollo de Soluciones Informáticas;

Que, a través del Informe Legal N° 0131-2020-IGP/GG-OAJ, la Oficina de Asesoría Jurídica emitió opinión legal favorable para la aprobación de la modificación de los procedimientos PR 005-2020-IGP Seguimiento, Medición, Gestión del Cambio y Revisión por la Dirección y PR 014-2020-IGP Desarrollo de Soluciones Informáticas;

Con el visado de la Oficina de Planeamiento y Presupuesto y la Oficina de Asesoría Jurídica;

De conformidad con lo dispuesto en el Decreto Legislativo N° 136, Ley del Instituto Geofísico del Perú, el Reglamento de Organizaciones y Funciones del Instituto Geofísico del Perú, aprobado por Decreto Supremo N° 01-2015-MINAM, Decreto Legislativo N° 1013, Ley de Creación, Organización y Funciones del Ministerio del Ambiente, que dispone la adscripción del Instituto Geofísico del Perú (IGP) como Organismo Público Ejecutor del ministerio del Ambiente, La Norma Técnica N° 001-2018-PCM/SGP, la Directiva DI 001-2020-IGP, "Aprobación, modificación o derogación de documentos normativos", aprobada ,mediante Resolución de Gerencia General N° 029-IGP/2020; y, la Resolución de Presidencia N° 005-IGP/2020, de fecha 09 de enero del 2020;

SE RESUELVE:

Artículo 1.- Aprobar las modificaciones de los procedimientos PR 005-2020-IGP Seguimiento, Medición, Gestión del Cambio y Revisión por la Dirección y PR 014-2020-IGP Desarrollo de Soluciones Informáticas, conforme a los anexos que forman parte integrante de la presente Resolución de Gerencia General.

Artículo 2.- Disponer que la Oficina de Planeamiento y Presupuesto, implemente y difunda los procedimientos y sus respectivas modificaciones aprobados en el artículo 1 de la presente Resolución de Gerencia General.

Artículo 3.- Disponer se publique la presente Resolución en el portal Institucional del Instituto Geofísico del Perú (www.gob.pe/igp).

Regístrese, publíquese y comuníquese.

Raúl Javier Bueno Cano
Gerente General

IGP

Firmado digitalmente por:
BUENO CANO Raul Javier
FAU 20131367008 soft
Motivo: Soy el Autor del
Documento
Fecha: 13/12/2020 23:23:49-0500

PROCEDIMIENTO PR 005-2020-IGP

SEGUIMIENTO, MEDICIÓN, GESTIÓN DEL CAMBIO Y REVISIÓN POR LA DIRECCIÓN

Versión 03

PROCEDIMIENTO PR 005-2020-IGP

SEGUIMIENTO, MEDICIÓN, GESTIÓN DEL CAMBIO Y REVISIÓN POR LA DIRECCIÓN

VERSIÓN	FECHA	DESCRIPCIÓN
1	09/09/2019	Creación del documento
2	02/11/2020	1. Cambio de Codificación de procedimiento. 2. Cambio en el alcance. 3. Cambio de Base Normativa. 4. Se agrego definición de SGSI.
3	09/12/2020	1. Se actualiza el punto 9 del procedimiento.
FORMULADO **OFICINA DE PLANEAMIENTO Y PRESUPUESTO**	**REVISADO Y VISADO** **OFICINA DE PLANEAMIENTO Y PRESUPUESTO**	**REVISADO Y VISADO** **OFICINA DE ASESORÍA JURÍDICA**
APROBADO **GERENCIA GENERAL**	**REVISADO Y VISADO** **(DENOMINACIÓN DE ORGANO/UNIDAD ORGANICA)**	**REVISADO Y VISADO** **(DENOMINACIÓN DE ORGANO/UNIDAD ORGANICA)**

SEGUIMIENTO, MEDICIÓN, GESTIÓN DEL CAMBIO Y REVISIÓN POR LA DIRECCIÓN

IGP Instituto Geofísico del Perú	INSTITUTO GEOFÍSICO DEL PERÚ		
	FICHA TÉCNICA DEL PROCEDIMIENTO		
DATOS DEL PROCEDIMIENTO			
Nombre del procedimiento	SEGUIMIENTO, MEDICIÓN, GESTIÓN DEL CAMBIO Y REVISIÓN POR LA DIRECCIÓN	Objetivo del procedimiento	Establecer las directrices para realizar el seguimiento y medición al Sistema de Gestión de Calidad y al Sistema de Gestión de la Seguridad de la Información a través de la información reportada por los procesos mediante los objetivos y metas establecidos, incluyendo la planeación para gestionar los cambios en el SGC o en el SGSI y la revisión por la dirección con el fin de asegurar su continua conveniencia, adecuación y eficacia, y así establecer mecanismos de mejora continua.
Código del Proceso relacionado	E01, E04	Alcance del procedimiento	Este procedimiento aplica para todas las Unidades de Organización del IGP, cuyos procesos se encuentran vinculados al alcance del Sistema de Gestión de Calidad y del Sistema de Gestión de la Seguridad de la Información.
Versión	2		
Base Normativa (Son disposiciones legales que soportan el procedimiento)			

Norma ISO 9001:2015	Requisito 8.5.6. Control de los cambios Requisito 9.1. Seguimiento, medición, análisis y evaluación. Requisito 9.3. Revisión por la Dirección
Norma ISO 27001:2013	Requisito 8.1 Planificación y control operacional Requisito 9.1. Monitoreo, medición, análisis y evaluación. Requisito 9.3. Revisión por la Dirección

Siglas y Definiciones (Abreviaturas y acrónimos)
SGC: Sistema de Gestión de Calidad
SGSI: Sistema de Gestión de la Seguridad de la Información
OPP: Oficina de Planeamiento y Presupuesto
ALT: Persona o grupo de personas que dirige y controla una organización al más alto nivel. El Comité de Alta Dirección del Sistema de Gestión de Calidad ISO 9001:2015, es responsable de dirigir la implementación del SGC.
CGD: Comité de Gobierno Digital.
ET: Equipo Técnico del Sistema de Gestión de Calidad. Está conformado por los dueños de procesos involucrados en el alcance del SGC, responsable del cumplimiento de la política y objetivos de calidad establecidos por el Comité de Alta Dirección del Sistema de Gestión de Calidad ISO 9001:2015, así como del control y mejora continua de los procesos asignados, según su competencia.
Cambio: Modificación significativa de un proceso, instalación, metodología de hacer o equipo ya existente.
Cambio Interno: Introducción de nuevos procesos, cambios de métodos de trabajo, cambio en instalaciones.

Cambio Externo: Cambio en la Legislación
Gestión del Cambio: Aplicación sistemática de procesos y procedimientos para generar una nueva salida del proceso o resultado previsto.
Desempeño: Resultados medibles de la gestión que realiza la entidad en cuanto a gestión de la calidad.
Mejora: Actividad para mejorar el desempeño.
Mejora continua: Actividad recurrente para mejorar el desempeño.
Monitoreo: Mediciones repetidas destinadas a seguir la evolución de un indicador durante un período de tiempo. En el sentido más específico, este término se aplica a la medición de la eficacia de un sistema.
Revisión por la Dirección: Actividad realizada para determinar la relevancia, adecuación y eficacia de lo que está siendo examinado, para alcanzar los objetivos establecidos para el Sistema de Gestión de la Calidad (SGC) y para el Sistema de Gestión de la Seguridad de la Información (SGSI).
Responsable del SGC: Servidor que cumple el rol del aseguramiento del SGC, a través del asesoramiento al Comité de Alta Dirección, el seguimiento y el control de la documentación.
Seguimiento: Determinación del estado de un sistema, un proceso, un producto, un servicio o una actividad.
Oficial de Seguridad de la Información: Miembro del Comité de Gobierno Digital que tiene funciones específicas en relación con la implementación y mejoramiento del SGSI en la institución.
Sistema de gestión: Conjunto de elementos de una organización interrelacionados o que interactúan para establecer políticas, objetivos y procesos para lograr estos objetivos.
Elemento de Entrada (Requisitos para iniciar el procedimiento)

Descripción del Requisito	Fuente
Información Documentada del IGP	DI Nº 001-2020-IGP Aprobación, Modificación o Derogación de Documentos Normativos del Instituto Geofísico del Perú - IGP
Indicadores	Objetivos del Sistema de Gestión de la Calidad, Objetivos del Sistema de Gestión de la Seguridad de la Información
Procesos vinculados al alcance del Sistema de Gestión de Calidad y al Sistema de Gestión de la Seguridad de la Información.	MP Nº 001-2020-IGP Manual de Procesos

ACTIVIDADES (Actividad, Unidad de Organización y Responsable)			
Nº	**Descripción de la Actividad**	**Unidad de Organización (*)**	**Responsable**
1	Establecer los objetivos, metas e indicadores de procesos: Definir anualmente los objetivos y metas del SGC y del SGSI, tomando como base: • El contexto de la organización. • La Política del Sistema de Gestión de la Calidad. • La Política de Seguridad de la Información • Resultados de la evaluación de riesgos y oportunidades. • Requisitos legales y suscritos. • Las opciones tecnológicas, operacionales, financieras y comerciales relevantes. • Otros resultados de la última revisión por la dirección.	OPP / CGD	Responsable del SGC / Oficial de Seguridad de la Información

2	Para cada uno de los objetivos se definirán sus respectivas metas, los plazos para la consecución de las mismas, se definirán los medios y la asignación de responsabilidades para conseguirlos, quedando como evidencia la PR Nº 007-F01 Matriz de Indicadores.	OPP / CGD	Responsable del SGC / Oficial de Seguridad de la Información
3	Para los procesos del SGC, cada propietario de proceso debe definir al menos un indicador para realizar la medición del proceso en la Caracterización de Procesos.	Unidades de Organización	Responsable de los Procesos
4	Para el SGSI, determinar indicadores necesarios para monitorear y medir los controles y procesos vinculados.	CGD	Oficial de Seguridad de la Información
5	Seguimiento del Programa SGC: Realizar seguimiento del programa SGC y del programa del SGSI y tomar las medidas necesarias para asegurar su cumplimiento.	OPP / CGD	Responsable del SGC / Oficial de Seguridad de la Información
6	Seguimiento de los Indicadores SGC: Cada Responsable de proceso debe enviar al responsable del SGC el resultado del cálculo de sus indicadores de proceso de acuerdo con la frecuencia especificada. El responsable del SGC consolidará los resultados en PR Nº 005-F01 Matriz de Indicadores con la cual también realizará seguimiento de los mismos. Los resultados quedan disponibles para las entradas de la revisión por la Dirección.	OPP/Unidades de Organización	Responsable del SGC / Responsable de los Procesos
7	Seguimiento de los Indicadores SGSI: El Oficial de Seguridad de la Información realiza el cálculo de los indicadores del SGSI de acuerdo con la frecuencia especificada consolidará los resultados en PR Nº 005-F01 Matriz de Indicadores con la cual también realizará seguimiento de los mismos. Los resultados quedan disponibles para las entradas de la revisión por la Dirección.	CGD	Oficial de Seguridad de la Información

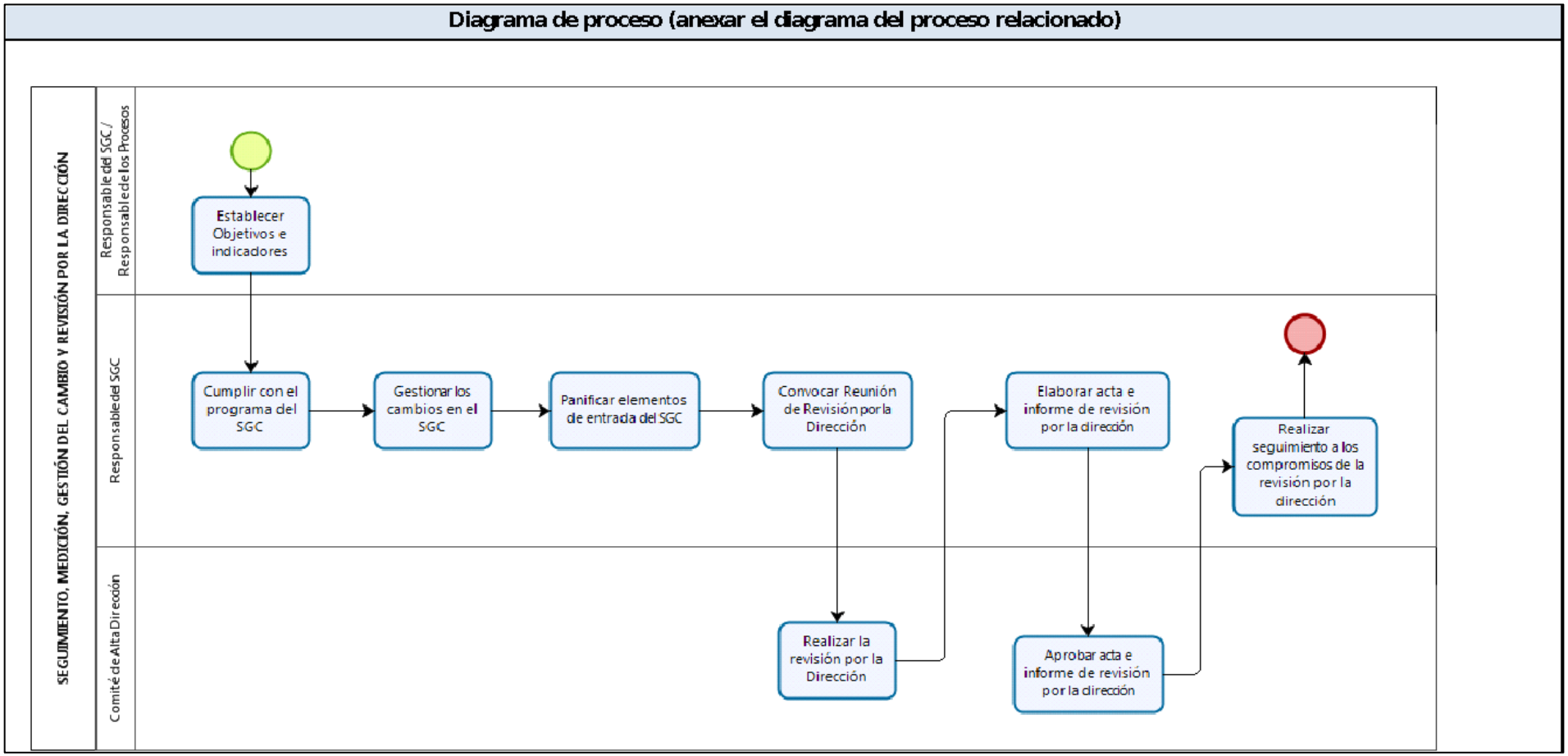
8	**Gestionar los cambios en el SGC y en el SGSI**: Identificar la necesidad de implementación de un cambio significativo que impacte al Sistema de Gestión de Calidad o al Sistema de Gestión de la Seguridad de la Información.	OPP / Unidades de Organización / CGD	Responsable del SGC / Responsable de los Procesos / Oficial de Seguridad de la Información
9	*Entre los cambios significativos para el SGC y SGSI se presenta:* *- Inclusión o eliminación de procesos al SGC o SGSI* *- Cambio en el alcance del SGC o SGSI* *- Cambio en la norma ISO 9001 o ISO 27001* *- Inclusión de software que elimine documentación aplicable a un proceso.* *- Inclusión de otra sede de operación* *- Cambios en la normatividad que requieran modificación de más de dos (2) procesos y más de tres (3) procedimientos.* *- Los cambios en la Política y Objetivos (de Calidad o de Gestión de la Seguridad de la Información) se dejan documentados en la Revisión por la Dirección.* *- Los cambios de la información documentada se procede según la ficha de procedimiento PR Nº 003-2020-IGP Gestión de Control de la Información Documentada.* ***-La gestión del cambio se realizará a través de planeamiento estratégico del IGP y se deberá tener en consideración los siguientes puntos: Cambio, propósito del cambio, consecuencias del cambio, proceso , actividades a realizar, responsable , recursos entre otros**.*	OPP / Unidades de Organización / CGD	Responsable del SGC / Responsable de los Procesos / Oficial de Seguridad de la Información
10	Diligenciar el formato PR Nº 004-F02 Solicitud de Acciones de Mejora / Cambio en el cual se establece las actividades, responsables y fechas para efectuar el cambio.	OPP / Unidades de Organización / CGD	Responsable del SGC / Responsable de los Procesos / Oficial de Seguridad de la Información

11	Planificar los elementos de entrada para la revisión por la dirección: Planificar anualmente los requisitos de entrada necesarios para la Revisión a los responsables de los procesos. Los elementos de entrada se consignan en PR Nº 005-F02 Informe revisión por la Dirección.	OPP / CGD	Responsable del SGC / Oficial de Seguridad de la Información
12	**Reunión de Revisión por la Dirección y salida**: Sustentar los indicadores, parámetros de control e informes y análisis de los componentes de la Revisión para la toma de decisiones. Revisar el Informe de Revisión por la Dirección tomando en cuenta las recomendaciones de los responsables de los procesos, del responsable SGC y del Oficial de Seguridad de la Información.	ALT / CGD	Comité de la Alta Dirección / Comité de Gobierno Digital
13	Las conclusiones, decisiones y acciones solicitadas por el Comité de la Alta Dirección como salidas o resultados de la revisión por la dirección se consignan en la sección "Acuerdos y Compromisos" del PR Nº 005-F02 Informe revisión por la Dirección y deben estar relacionadas con: • Conclusiones sobre la conveniencia, adecuación y eficacia continúas del SGC y del SGSI. • Las oportunidades de mejora. • Cualquier necesidad de cambio en el SGC o en el SGSI. • Necesidades de recursos. • Acciones ante objetivos no logrados y cualquier otra implicación para la dirección estratégica Las salidas de la revisión por la dirección son plasmadas en un Acta de reunión.	ALT / CGD	Comité de la Alta Dirección / Comité de Gobierno Digital
14	Aprobar el Documento: Se redacta el documento Revisión por la Dirección y lo firman representa la aprobación de la revisión por la dirección a través de la firma ológrafica o	ALT / CGD	Comité de la Alta Dirección / Comité de Gobierno Digital

	digital de todos los miembros del comité correspondiente, que asistieron a la reunión.		
15	Seguimiento al Plan de Acción: Realizar revisión a la ejecución de los planes de acción derivados de los acuerdos y compromisos de la revisión por la dirección.	OPP / CGD	Responsable del SGC / Oficial de Seguridad de la Información
Fin del procedimiento			
DOCUMENTOS QUE SE GENERAN (Documento de salida del procedimiento)			
PR Nº 005-F01 Matriz de Indicadores			
PR Nº 005-F02 Informe revisión por la Dirección			
PR Nº 005-F03 Programa Anual del Sistema de Gestión de Calidad			
“Toda copia impresa es un Documento No Controlado a excepción del original”			

ANEXO I – DIAGRAMA DE PROCESO

Diagrama de proceso (anexar el diagrama del proceso relacionado)



PROCEDIMIENTO PR 014-2020-IGP

DESARROLLO DE SOLUCIONES INFORMÁTICAS

Versión 03

PROCEDIMIENTO PR 014-2020-IGP

DESARROLLO DE SOLUCIONES INFORMÁTICAS

VERSIÓN	FECHA	DESCRIPCIÓN
01 02 03	12/10/2019 20/12/2019 22/11/2020	1. Documento Inicial 1. Actualización de actividades 1. Se modifica la estructura y codificación y se actualiza la secuencia de actividades.
FORMULADO **OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN Y DATOS GEOFÍSICOS**	**REVISADO Y VISADO** **OFICINA DE PLANEAMIENTO Y PRESUPUESTO**	**REVISADO Y VISADO** **OFICINA DE ASESORÍA JURÍDICA**
APROBADO **GERENCIA GENERAL**	**REVISADO Y VISADO** **(DENOMINACIÓN DE ÓRGANO/UNIDAD ORGÁNICA)**	**REVISADO Y VISADO** **(DENOMINACIÓN DE ÓRGANO/UNIDAD ORGÁNICA)**

DESARROLLO DE SOLUCIONES INFORMÁTICAS

IGP Instituto Geofísico del Perú	INSTITUTO GEOFÍSICO DEL PERÚ		
	FICHA TÉCNICA DEL PROCEDIMIENTO		
DATOS DEL PROCEDIMIENTO			
Nombre del procedimiento	DESARROLLO DE SOLUCIONES INFORMATICAS	Objetivo del procedimiento	Establecer la metodología de desarrollo de soluciones informáticas que cumplan los requisitos funcionales y de seguridad, en el marco del Sistema de Gestión de Seguridad de la Información (SGSI) del IGP, incluyendo las mejores prácticas de desarrollo posibles en cumplimiento a la Norma ISO/IEC 27001:2013 "Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos"
Código del Proceso relacionado	S03	Alcance del procedimiento	El presente procedimiento es aplicable para la Oficina de Tecnología de Información y Datos Geofísicos – OTIDG y abarca las actividades de ingeniería de software y desarrollo de aplicaciones que esta oficina realice.
Versión	3		

Base Normativa (Son disposiciones legales que soportan el procedimiento)	
Resolución Ministerial N° 004-2016-PCM y modificatorias.	Aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2013 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
Decreto Supremo No 001-2015-MINAM	Reglamento Organización de Funciones (ROF) del Instituto Geofísico del Perú
Directiva DI 001-2020- IGP/OPP	Aprobación, Modificación o Derogación de Documentos Normativos del Instituto Geofísico del Perú – IGP
Resolución de Presidencia N° 140-IGP/2019 (31 de Diciembre del 2019)	Plan Operativo Institucional del IGP 2020
Norma NTP ISO/IEC 27001:2014 (basada en ISO/IEC 27001:2013)	8.1 Planificación y control operacional Anexo A. A.14.2 Seguridad en procesos de desarrollo y soporte

Siglas y Definiciones (Abreviaturas y acrónimos)
IGP: Instituto Geofísico del Perú
SGSI: Sistema de Gestión de la Seguridad de la Información
OTIDG: Oficina de Tecnología de Información y Datos Geofísicos
UIS: Unidad de Ingeniería de Software
UO: Unidad Orgánica

Amenaza: Causa potencial de un incidente no deseado, que puede resultar en daño a un sistema u organización.
Confidencialidad: Propiedad de que la información no esté disponible o sea revelada a personas no autorizadas, las entidades o procesos.
Control: Medida que modifica un riesgo. Los controles incluyen cualquier proceso, la política, dispositivo, práctica, u otras acciones que modifiquen un riesgo. Los controles no siempre pueden proporcionar el efecto de modificación previsto o asumido.
Desarrollo de aplicaciones: El desarrollo de aplicaciones, también conocido como proceso de software, ciclo de vida del software y desarrollo de software, es el desarrollo de un producto de software en un proceso planificado y estructurado.
Disponibilidad: Propiedad de la información de ser accesible y utilizable por petición de una entidad autorizada.
Integridad: Propiedad de exactitud y lo completitud de la información.
Probabilidad: Posibilidad de que algún hecho se produzca.
Proceso: Conjunto de actividades interrelacionadas o interactivas que utilizan entradas para entregar un resultado previsto. El "resultado previsto" de un proceso se denomina salida, producto o servicio dependiendo del contexto de la referencia. Las entradas a un proceso son generalmente las salidas de otros procesos y las salidas de un proceso son generalmente las entradas a otros procesos.
Seguridad de la información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información. Además, otras propiedades, como la autenticidad, la responsabilidad, el no repudio, y confiabilidad también pueden estar involucrados.
Sistema de Gestión de Seguridad de la Información (SGSI): Consiste en un conjunto de políticas, procedimientos, guías y sus recursos y actividades asociados, que son gestionado de manera colectiva por una organización. Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la seguridad de la información de una organización para alcanzar los objetivos del negocio. Este enfoque está basado en una apreciación del riesgo y en los niveles de aceptación del riesgo de la organización diseñados para tratar y gestionar con eficacia los riesgos. El análisis de los requisitos para la protección de los activos de información, según sea necesario, contribuye a la exitosa implementación de un SGSI.
Vulnerabilidad: Debilidad de un activo o de control que puede ser explotado por una o más amenazas.

Elemento de Entrada (Requisitos para iniciar el procedimiento)	
Descripción del Requisito	**Fuente**
Expresión de necesidades de automatización o funcionalidades que pueden ser satisfechas a través del desarrollo de software	Correo y/o Memorándum

ACTIVIDADES (Actividad, Unidad de Organización y Responsable)			
Nº	**Descripción de la Actividad**	**Unidad de Organización (*)**	**Responsable**
1	**Realizar el requerimiento del software, aplicación o sistema.**	Unidad Orgánica	Jefe/Director de la Unidad Orgánica
2	**Recibir y evaluar requerimiento.**	OTIDG	Jefa de la OTIDG
3	**Informar no viabilidad de requerimiento**, si el requerimiento no cumple con los objetivos de la Institución	OTIDG	Jefa de la OTIDG
4	**Actualizar el Plan de Proyectos TI** y el Cronograma de Proyectos TI	OTIDG	Coordinador de Ingeniería de Software
5	**Asignar los roles de desarrollo** Asignar y documentar los roles en Ficha de Desarrollo Soluciones Informáticas, de acuerdo con el Anexo I Roles de Desarrollo	OTIDG	Coordinador de Ingeniería de Software
6	**Recabar elementos de entrada.** Realizar entrevistas, recibir documentos de referencia e identificar potenciales productos con los cuales hacer benchmarking para	OTIDG	Coordinador de Ingeniería de Software

	tener los requisitos del objeto a desarrollar. Incorporar a estos requisitos los niveles mínimos aceptables de seguridad y privacidad. Utilizar como guía el Anexo II: Formulación de Preguntas de Seguridad		
7	**Resumir los requisitos funcionales**, los requisitos de seguridad (resultantes de responder al Anexo II) y los criterios de aceptación acordados con el Representante del Usuario Final en la Ficha de Desarrollo de Soluciones Informáticas	OTIDG	Coordinador de Ingeniería de Software
8	**Elaborar la base de datos Entidad - Relación**	OTIDG	Coordinador de Ingeniería de Software
9	**Revisar el Anexo III:** Top 10 Riesgos de Seguridad en Aplicaciones Web, identificando si el desarrollo a realizarse puede ser susceptible a alguno de estos riesgos con fines preventivos.	OTIDG	Coordinador de Ingeniería de Software
10	Establecer capas de seguridad, tomando en cuenta los conceptos y controles en el Anexo IV Estándares de Desarrollo Seguro	OTIDG	Coordinador de Ingeniería de Software
11	**Entorno de Desarrollo** Realizar el desarrollo software, tomando en cuenta los roles previamente establecidos, las respuestas a las preguntas de seguridad, las capas de seguridad establecidas y las medidas de separación de entornos de desarrollo, prueba y producción establecidas	OTIDG	Coordinador de Ingeniería de Software

	en el Anexo IV Estándares de Desarrollo Seguro		
12	**Entorno de Pruebas** Copiar el código al servidor de pruebas (en segmento VLAN de pruebas segregado) a través de SFTP, bajo autenticación.	OTIDG	Coordinador de Ingeniería de Software
13	**Entorno de Pruebas** Realizar las pruebas funcionales y de seguridad al software y registrar los resultados en el formato Pruebas de Sistema de Información, Redes y Aplicativos	OTIDG	Coordinador de Ingeniería de Software
14	**Entorno de Operaciones** El código fuente es copiado a través de SFTP al servidor de producción, bajo autenticación.	OTIDG	Coordinador de Ingeniería de Software
15	**Entorno de Operaciones** Realizar despliegue de software	OTIDG	Coordinador de Ingeniería de Software
16	Capacitar a usuarios y/o difundir desarrollo	OTIDG	Coordinador de Ingeniería de Software
Fin del procedimiento			
DOCUMENTOS QUE SE GENERAN (Documento de salida del procedimiento)			
Correo o memorándum de solicitud de una solución informática			
Correo o memorándum de no viabilidad del requerimiento (Si aplica)			

Plan de Proyectos TI
Cronograma de Proyectos TI
Ficha de Desarrollo de Soluciones Informáticas
Pruebas de Sistema de Información, Redes y Aplicativos
Acta de capacitación

ANEXO I – Roles de Desarrollo

Rol de Desarrollo	Asignado a
Representante de usuario final	Jefe de la Unidad Orgánica solicitante y/o un subordinado
Seguimiento	Realizado por Coordinador de Ingeniería de Software y/o Jefe de OTIDG.
Equipo específico de desarrollo	Otros puestos de OTIDG asignados al proyecto según necesidad y competencias.

ANEXO II - Formulación de Preguntas de Seguridad

- ¿Mi aplicación contiene información confidencial?
- ¿Mi aplicación recopila o almacena datos que exigen que se cumplan estándares normativos nacionales?
- ¿Mi aplicación recopila o contiene datos confidenciales personales o de clientes que pueden utilizarse, solos o con otra información, para identificar, ponerse en contacto o buscar a una persona?
- ¿Mi aplicación recopila o contiene datos que se pueden usar para acceder a información médica, educativa, financiera o de empleo de una persona?
- ¿Dónde y cómo están los datos almacenados? Tenga en cuenta cómo va a supervisar los servicios de almacenamiento que usa la aplicación para detectar cualquier cambio inesperado de comportamiento (por ejemplo, tiempos de respuesta más lentos). ¿Podrá influir en el registro para recopilar datos más detallados y analizar un problema en profundidad?
- ¿Mi aplicación estará disponible para el público (en Internet) o solo internamente? Si la aplicación está disponible al público, ¿cómo protege los datos que puedan recopilarse para que no se utilicen de forma incorrecta? Si la aplicación solo está disponible internamente, tenga en cuenta qué usuarios de la organización han de tener acceso a la aplicación y durante cuánto tiempo.
- ¿Comprende el modelo de identidad antes de empezar a diseñar la aplicación? ¿Cómo va a determinar que los usuarios son quienes dicen ser y lo que un usuario está autorizado a hacer?
- ¿Mi aplicación lleva a cabo las tareas importantes o confidenciales? Tenga en cuenta cómo va a validar que el usuario que realiza una tarea confidencial está autorizado a realizarla y cómo se va a autenticar que la persona es quien dice ser.
- ¿Mi aplicación realiza actividades de riesgo de software, como permitir que los usuarios carguen o descarguen archivos u otros datos? Si la aplicación lleva a cabo actividades de riesgo, tenga en cuenta cómo va a proteger a los usuarios de la manipulación de datos o archivos malintencionados.

ANEXO III – Top 10 Riesgos de Seguridad en Aplicaciones Web

1. Inyección. Las fallas de inyección, como la inyección de SQL, NoSQL, OS y LDAP, ocurren cuando se envían datos que no son de confianza a un intérprete como parte de un comando o consulta. Los datos hostiles del atacante pueden engañar al intérprete para que ejecute comandos no deseados o acceda a datos sin la debida autorización.
2. Autenticación rota. Las funciones de la aplicación relacionadas con la autenticación y la administración de sesiones a menudo se implementan de manera incorrecta, lo que permite a los atacantes comprometer contraseñas, claves o tokens de sesión, o explotar otras fallas de implementación para asumir las identidades de otros usuarios de forma temporal o permanente.
3. Exposición de datos sensibles. Muchas aplicaciones web y API no protegen adecuadamente los datos confidenciales, como los financieros, de salud y PII. Los atacantes pueden robar o modificar esos datos débilmente protegidos para cometer fraude con tarjetas de crédito, robo de identidad u otros delitos. Los datos confidenciales pueden verse comprometidos sin protección adicional, como el cifrado en reposo o en tránsito, y requieren precauciones especiales cuando se intercambian con el navegador.
4. Entidades externas XML (XXE). Muchos procesadores XML más antiguos o mal configurados evalúan las referencias de entidades externas dentro de los documentos XML. Las entidades externas se pueden utilizar para divulgar archivos internos mediante el controlador de URI de archivos, recursos compartidos de archivos internos, escaneo de puertos internos, ejecución remota de código y ataques de denegación de servicio.
5. Control de acceso roto. Las restricciones sobre lo que los usuarios autenticados pueden hacer a menudo no se aplican correctamente. Los atacantes pueden explotar estos defectos para acceder a funciones y / o datos no autorizados, como acceder a las cuentas de otros usuarios, ver archivos confidenciales, modificar los datos de otros usuarios, cambiar los derechos de acceso, etc.
6. Mala configuración de seguridad. La configuración incorrecta de seguridad es el problema más común. Esto suele ser el resultado de configuraciones predeterminadas inseguras, configuraciones incompletas o ad hoc, almacenamiento en la nube abierta, encabezados HTTP mal configurados y mensajes de error detallados que contienen información confidencial. No solo todos los sistemas operativos, marcos, bibliotecas y aplicaciones deben

configurarse de forma segura, sino que también deben actualizarse o actualizarse de manera oportuna.

7. Cross-Site Scripting XSS . Los defectos de XSS ocurren cuando una aplicación incluye datos que no son de confianza en una nueva página web sin la validación o el escape adecuados, o actualiza una página web existente con datos proporcionados por el usuario mediante una API de navegador que puede crear HTML o JavaScript. XSS permite a los atacantes ejecutar scripts en el navegador de la víctima que pueden secuestrar sesiones de usuario, desfigurar sitios web o redirigir al usuario a sitios maliciosos.
8. Deserialización insegura. La deserialización insegura a menudo conduce a la ejecución remota de código. Incluso si las fallas de deserialización no dan como resultado la ejecución remota de código, pueden usarse para realizar ataques, incluidos ataques de reproducción, ataques de inyección y ataques de escalada de privilegios.
9. Uso de componentes con vulnerabilidades conocidas. Los componentes, como bibliotecas, marcos y otros módulos de software se ejecutan con los mismos privilegios que la aplicación. Si se explota un componente vulnerable, dicho ataque puede facilitar la pérdida de datos o la toma de control del servidor. Las aplicaciones y API que utilizan componentes con vulnerabilidades conocidas pueden socavar las defensas de las aplicaciones y permitir varios ataques e impactos.
10. Registro y monitoreo insuficientes. Un registro y una supervisión insuficientes, junto con una integración faltante o ineficaz con la respuesta a incidentes, permiten a los atacantes atacar aún más los sistemas, mantener la persistencia, cambiar a más sistemas y manipular, extraer o destruir datos. La mayoría de los estudios de infracciones muestran que el tiempo para detectar una infracción es de más de 200 días, generalmente detectados por partes externas en lugar de procesos internos o monitoreo.

Fuente: OWASP Foundation, Inc.
https://owasp.org/www-project-top-ten/

ANEXO IV – Estándares de Desarrollo Seguro

Lenguajes de Programación Aprobados por la OTIDG
Javascript
Java
PHP
Python
Swift
Kotlin

Consideraciones Para Establecer Capas de Seguridad
• Uso de una biblioteca de codificación segura y un marco de software. • Búsqueda de componentes vulnerables. • Listar las amenazas a las que es susceptible la solución informática • Reducción de la superficie expuesta a ataques. • Adopción de una directiva de identidad como perímetro de seguridad principal. • Exigencia de re-autenticación con transacciones importantes. • Uso de una solución de administración de claves para proteger las claves, las credenciales y otros secretos. • Protección de datos confidenciales. • Implementación de medidas para notificaciones de error. • Aprovechamiento del control de errores y excepciones. • Uso del registro y las alertas. • Comunicaciones entre servicios. • Generación de logs, gestión de eventos.

Estándares de seguridad para la codificación y pruebas
• No está permitido modificar programas sin que quede registrado el cambio. • En caso de requerirse la implementación de un cambio, este deberá seguir el procedimiento de control de cambios. • No está permitido escribir cambios no autorizados ni código malicioso. • Las pruebas de software deben cubrir instalación, stress, almacenamiento, configuración, funcionalidad, seguridad y recuperación ante errores. Las pruebas buscan asegurar que el software no muestre detalles de posibles errores o datos confidenciales que puedan ser usados por atacantes. No indexar directorios de recursos y presentar las interfaces de usuario fieles a los prototipos de software aceptados por el usuario final. • Se deberá realizar una gestión de las sesiones, que tenga en cuenta los siguientes aspectos: • Garantizar la existencia de opciones de desconexión o cierre de sesión de los aplicativos que permita terminar completamente con la conexión asociada. • No exponer los identificadores de sesión en URL, mensajes de error ni logs, y no transmitirlos como parámetros.

- Asegurar que los aplicativos proporcionen la mínima información de la sesión establecida, almacenada en cookies y complementos, entre otros.
- Asegurar que la sesión expire después de cierto tiempo.
- No permitir la apertura de sesiones simultaneas con el mismo usuario.
- Todas las funciones de criptografía de las aplicaciones desarrolladas deben ser implementadas en sistemas confiables (por ejemplo: el servidor).
- Se deben considerar los siguientes aspectos en el manejo de errores:
- Garantizar que no se divulgue información sensible en respuestas de error.
- Liberar espacio en memoria cuando ocurra una condición de error.
- Para el manejo de archivos se deberán acatar las siguientes consideraciones:
- Remover todas las funcionalidades y archivos que no sean parte del software.
- Prevenir la revelación de la estructura de directorios del software.
- Para el establecimiento de conexión a las bases de datos se deberán considerar los siguientes aspectos:
- No incluir las cadenas de conexión a las bases de datos en el código de los aplicativos.
- Cerrar la conexión a las bases de datos desde los aplicativos, tan pronto como estas no sean requeridas.

Separación de Entornos de Desarrollo, Pruebas y Producción

- Se separan los entornos principalmente al funcionar en VLAN distintas.
- El desarrollo se realiza utilizando un terminal en la VLAN de desarrollo.
- El software de desarrollo se realiza en un entorno de desarrollo y en la VLAN de desarrollo.
- El software de producción funciona en un servidor ajeno a los demás entornos.
- Existen reglas que solo permiten a las computadoras del sistema de publicación acceder al mismo.
- Se despliega un servidor para integración continua y entrega continua basado en Jenkins