INSTITUTO GEOFÍSICO DEL PERÚ

# Resolución de Gerencia General

## N° 031-IGP/2020

Lima, 27 de Octubre del 2020

VISTOS:

El Informe Legal N° 093-2020-IGP/GG-OAJ y el Informe N° 0178-2020-IGP/GG-OPP; 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 presentación 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 Organización 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 el 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 Riesgo de Desastres;

Que, es necesario precisar que de acuerdo al Cuadro N° 2. Tipo de Documento de la Directiva DI 001-2020-IGP Aprobación, Modificación o Derogación de Documentos Normativos, aprobada mediante Resolución de Gerencia General N° 029-IGP/2020, de fecha 16 de octubre de 2020, los procedimientos de una entidad son aprobadas mediante Resolución de Gerencia General;

Que el artículo 4° de la Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado establece que:

*"El proceso de modernización de la gestión del Estado tiene como finalidad fundamental la obtención de mayores niveles de eficiencia del aparato estatal, de manera que se logre una mejor atención a la ciudadanía, priorizando y optimizando el uso de los recursos públicos (…)";*

Que, el artículo 1° de la Resolución Ministerial N° 119-2018-PCM, que disponen la creación de un Comité de Gobierno Digital en cada entidad de la Administración Pública, señala que:

*"1.1 Cada entidad de la Administración Pública debe constituir un Comité de Gobierno Digital (…)*

*1.2 El Titular de la entidad puede incorporar a otros miembros al Comité de Gobierno Digital atendiendo a las necesidades de la entidad para el cumplimiento de las políticas nacionales, sectoriales o el logro de sus objetivos estratégicos institucionales".*

Que, mediante Resolución de Secretaria de Gestión Publica N° 006-2018-PCM/SGP se aprobó la Norma Técnica N° 001-2018-PCM/SGP para la "Implementación de la gestión por procesos en las entidades de la administración pública";

Que, según el Informe N° 0178-2020-IGP/GG-OPP señala que la evaluación técnica, *"consiste en verificar lo siguiente: i) Se encuentre alineado al marco técnico-normativo y políticas nacionales. ii) Se encuentre alineada con lo establecido en la presente Directiva. iii) Se encuentre en el marco de las funciones y competencias de los órganos involucrados. iv) Se encuentre alineada a las políticas y objetivos institucionales"*,

Que, asimismo, señala que: *"(… informe tiene por objeto validar si el procedimiento Metodología de Gestión de Riesgos de Seguridad de la Información guarda coherencia y alineamiento con las normas internas y bajo el enfoque de gestión por procesos según la Norma Técnica N° 001-2018-PCM/SGP "IMPLEMENTACIÓN DE LA GESTIÓN POR PROCESOS EN LAS ENTIDADES DE LA ADMINISTRACIÓN PÚBLICA";*

Que, siendo así, de la revisión del citado Informe N° 0178-2020-IGP/GG-OPP se advierte que cumple con la normativa y resulta favorable la propuesta del procedimiento de Metodología de Gestión de Riesgos de Seguridad de la Información;

Que, mediante Informe Legal N° 093-2020-IGP/GG-OAJ, se emite opinión legal favorable para aprobar la propuesta del procedimiento de Metodología de Gestión de Riesgos de Seguridad de la Información;

Con el visado de la Oficina de Asesoría Jurídica, de la Oficina de Tecnología de Información y Datos Geofísicos y de la Oficina de Planeamiento y Presupuesto, y;

De conformidad con el Decreto Supremo N° 001-2015-MINAM, la Directiva DI 001-2020-IGP Aprobación, Modificación o Derogación de Documentos Normativos, aprobada mediante Resolución de Gerencia General N° 029-IGP/2020, la Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado, la Resolución Ministerial N° 119-2018-PCM; la Resolución de Secretaría de Gestión Publica N° 006-2018-PCM/SGP y la Resolución de Gerencia General N° 029-IGP/2020;

SE RESUELVE:

**Artículo 1**.- Aprobar el Procedimiento PR 001-2020-IGP, denominado "Procedimiento de Metodología de Gestión de Riesgos de Seguridad de la Información del Instituto Geofísico del Perú", que como anexo forma parte integrante de la presente Resolución de Gerencia General.

**Artículo 2**.- Disponer la publicación de la presente Resolución de Gerencia General en el Portal Institucional del Instituto Geofísico del Perú (www.gob.pe/igp).

**Artículo 3**.- Notificar la presente Resolución a los interesados.

**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: 27/10/2020 14:10:29-0500

IGP
V.B.
Firmado digitalmente por:
DELGADO ORTEGA Edgar FAU 20131367008 hard
Motivo: Doy V° B°
Fecha: 27/10/2020 13:09:21-0500

# PROCEDIMIENTO PR 001-2020-IGP

# METODOLOGÍA DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Versión 01

# PROCEDIMIENTO PR 001-2020-IGP

# METODOLOGÍA DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

| VERSIÓN | FECHA | DESCRIPCIÓN |
|---|---|---|
| 1 | 13/oct/2020 | Documento Inicial |
| **FORMULADO**<br>**OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN Y DATOS GEOFÍSICOS** | **REVISADO Y VISADO**<br>**OFICINA DE PLANEAMIENTO Y PRESUPUESTO** | **REVISADO Y VISADO**<br>**OFICINA DE ASESORÍA JURÍDICA** |
| IGP<br>Firmado digitalmente por: LUNA GUZMAN Maria Rosa FAU 20131367008 soft<br>Motivo: Soy el Autor del Documento<br>Fecha: 27/10/2020 11:59:18-0500 | IGP<br>Firmado digitalmente por: DELGADO ORTEGA Edgar FAU 20131367008 hard<br>Motivo: Soy el autor del documento<br>Fecha: 13/10/2020 22:47:56-0500 | |
| **APROBADO**<br>**GERENCIA GENERAL** | **REVISADO Y VISADO**<br>**(DENOMINACIÓN DE ORGANO/UNIDAD ORGANICA)** | **REVISADO Y VISADO**<br>**(DENOMINACIÓN DE ORGANO/UNIDAD ORGANICA)** |
| | | |

# METODOLOGÍA DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

IGP Instituto Geofísico del Perú

**FICHA TÉCNICA DEL PROCEDIMIENTO**

| DATOS DEL PROCEDIMIENTO | | | |
|---|---|---|---|
| Nombre del procedimiento | Metodología de Gestión de Riesgos de Seguridad de la Información | Objetivo del procedimiento | Establecer la metodología de gestión de riesgos de seguridad de la información en el marco del Sistema de Gestión de Seguridad de la Información (SGSI) del IGP, incluyendo identificar, analizar, evaluar y dar tratamiento a los riesgos de seguridad de la información según el alcance del Sistema de Gestión de Seguridad de la Información 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 | E.04 | Alcance del procedimiento | El presente procedimiento es de cumplimiento obligatorio para la Oficina de Tecnología de Información y Datos Geofísicos – OTIDG y abarca las unidades de organización y procesos involucrados en el Sistema de Gestión de la Seguridad de la Información, bajo el alcance que se haya aprobado para este. |
| Versión | 1 | | |

| **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. |
| DIRECTIVA Nº 001-2019- IGP/GG-OPP | Aprobación, Modificación o Derogación de Documentos Normativos del Instituto Geofísico del Perú – IGP |
| RESOLUCIÓN DE PRESIDENCIA N° 036-IGP/2020 | Conformación y funciones del CGD. |
| Norma ISO 27001:2013 | Requisito 6.1 Acciones para abordar los riesgos y las oportunidades, 6.1.2 Evaluación del riesgo de la seguridad de la información, 6.1.3 Tratamiento de riesgos de la seguridad de la información. |

| **Siglas y Definiciones (Abreviaturas y acrónimos)** |
|---|
| IGP: Instituto Geofísico del Perú |
| SGSI: Sistema de Gestión de la Seguridad de la Información |
| CGD: Comité de Gobierno Digital. |

| |
|---|
| OTIDG: Oficina de Tecnología de Información y Datos Geofísicos |
| 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. |
| Activo: Cualquier cosa que tenga un valor tangible o intangible para una organización. Los activos tangibles incluyen los activos humanos, físicos y ambientales. Los activos intangibles incluyen información, marca y reputación |
| Aceptación de riesgos: Decisión informada para tomar un riesgo en particular. La aceptación del riesgo puede ocurrir sin el tratamiento del riesgo o durante el proceso de tratamiento de riesgos. Los riesgos aceptados están sujetos a supervisión y revisión. |
| Amenaza: Causa potencial de un incidente no deseado, que puede resultar en daño a un sistema u organización. |
| Análisis de riesgo: Proceso de comprender la naturaleza del riesgo y determinar el nivel de riesgo. El análisis de riesgos proporciona las bases para la evaluación del riesgo y para tomar las decisiones sobre el tratamiento del riesgo. El análisis de riesgo incluye la estimación del riesgo. |
| Confidencialidad: Propiedad de que la información no esté disponible o sea revelada a personas no autorizadas, las entidades o procesos. |
| Consecuencia: Resultado de un evento que afecta a los objetivos. Un evento puede conducir a una serie de consecuencias. Una consecuencia puede ser cierta o incierta, y puede tener efectos positivos o negativos sobre la consecución de los objetivos. Las consecuencias pueden ser expresadas cualitativa o cuantitativamente. Las consecuencias iniciales pueden convertirse en reacciones en cadena. |
| 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. |
| Criterios de riesgo: Términos de referencia contra los cuales se evalúa la importancia de un riesgo. Los criterios de riesgo se basan en los objetivos de la organización, y el contexto externo e interno. Los criterios de riesgo se pueden obtener de normas, leyes, políticas y otros requisitos. |
| Disponibilidad: Propiedad de la información de ser accesible y utilizable por petición de una entidad autorizada. |
| Evaluación del riesgo: Proceso de la comparación de los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable. La evaluación de riesgos ayuda a la decisión sobre el tratamiento del riesgo. |

| |
|---|
| Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. |
| Identificación del riesgo: Proceso que comprende la búsqueda, el reconocimiento y la descripción de los riesgos. La identificación de riesgos consiste en la identificación de las fuentes de riesgo, eventos/sucesos, sus causas y sus consecuencias potenciales. La identificación de riesgos puede implicar datos históricos, análisis teórico, opiniones informadas y de expertos; así como necesidades de las partes interesadas. |
| Integridad: Propiedad de exactitud y lo completitud de la información. |
| Nivel de riesgo: Magnitud de un riesgo, expresados en términos de la combinación de las consecuencias y de su probabilidad. |
| 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. |
| Proceso de gestión de riesgos: Aplicación sistemática de políticas, procedimientos y prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto e identificación, análisis, evaluación, tratamiento, monitoreo y revisión de riesgos. |
| Propietario del Activo: Las personas, así como otras entidades que hayan aprobado la responsabilidad de gestión del ciclo de vida de los activos, califican para ser asignadas como propietarios de activos. |
| Propietario del riesgo: Persona o entidad que tiene la responsabilidad y la autoridad para gestionar un riesgo. |
| Riesgo: Efecto de la incertidumbre. Un efecto es una desviación de lo esperado, ya sea positiva o negativa. La incertidumbre es el estado, aunque sea parcial, de la carencia de información relacionada con la comprensión o conocimiento de un evento, su consecuencia, o su probabilidad. Con frecuencia, el riesgo se caracteriza por referencia a los eventos potenciales y consecuencias, o una combinación de éstos. Con frecuencia, el riesgo se expresa en términos de una combinación de las consecuencias de un evento (incluyendo cambios en las circunstancias) y la probabilidad asociada a que ocurra. En el contexto de los sistemas de gestión de seguridad de la información, los riesgos de seguridad de la información pueden ser expresados como efecto de la incertidumbre en los objetivos de seguridad de la información. Un |

| |
|---|
| riesgo específico para la seguridad de la información se asocia con la posibilidad de que las amenazas exploten vulnerabilidades de un activo de información o un grupo de activos de información, con consecuencias negativas para la organización. |
| Riesgo Inherente: Es el riesgo en su estado natural, antes de considerar los controles que tenga asociados. Este se obtiene del producto de la probabilidad de que se materialice y el impacto que podría ocasionar. |
| Riesgo residual: Riesgo que queda después del tratamiento del riesgo. |
| 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. |
| Tratamiento del riesgo: Proceso para modificar el riesgo. El tratamiento del riesgo puede implicar:<br>- Evitar el riesgo al decidir no iniciar o continuar con la actividad que da lugar al riesgo;<br>- Tomar o aumentar del riesgo con el fin de perseguir una oportunidad;<br>- Eliminación de la fuente de riesgo;<br>- El cambio de la probabilidad;<br>- El cambio de las consecuencias;<br>- Compartiendo el riesgo con la otra parte o partes (incluyendo los contratos y la financiación del riesgo);<br>- Retener el riesgo por elección informada.<br>Tratamientos de riesgo que tienen que ver con las consecuencias negativas se refieren a veces como "riesgo mitigación", "eliminación de riesgos", "prevención de riesgos" y "reducción del riesgo". El tratamiento del riesgo puede crear nuevos riesgos o modificar los riesgos existentes. |
| 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** |
| Información Documentada del IGP | DIRECTIVA Nº 001-2019- IGP/GG-OPP Aprobación, Modificación o Derogación de Documentos Normativos del Instituto Geofísico del Perú - IGP |
| Responsabilidad sobre el Sistema de Gestión de la Seguridad de la Información del IGP | RESOLUCIÓN DE PRESIDENCIA N° 036-IGP/2020, sobre la conformación y funciones del CGD. |
| Procesos vinculados al alcance del Sistema de Gestión de la Seguridad de la Información | MP Nº 001-2019-IGP/GG-OPP Mapa de Procesos |
| Alcance del SGSI | Alcance del Sistema de Gestión de Seguridad de la Información |

| ACTIVIDADES (Actividad, Unidad de Organización y Responsable) | | | |
|---|---|---|---|
| **Nº** | **Descripción de la Atividad** | **Unidad de Organización (*)** | **Responsable** |
| **1** | **Comunicar y consultar.**<br>El Oficial de Seguridad de la Información del IGP deberá fomentar y coordinar la participación y acciones de todas las unidades organizacionales y partes externas implicadas en la gestión de riesgos de la seguridad de la información, a través de reuniones y talleres participativos. | CGD | Oficial de Seguridad de la Información |
| **2** | **Comunicar y consultar.**<br>El Oficial de Seguridad de la Información del IGP, deberá comunicar al Comité de Gobierno Digital – CDG:<br>• El inicio de cada ciclo de gestión de riesgos de seguridad de la información (ordinariamente con frecuencia anual y de manera extraordinaria cuando existan cambios relevantes u ocurra un incidente de seguridad de la información)<br>• La planificación y el desarrollo de las actividades de acuerdo con la metodología del presente procedimiento. | CGD | Oficial de Seguridad de la Información |
| **3** | **Comunicar y consultar.**<br>Implementar el canal de comunicación y consulta que abarque la gestión de riesgos de seguridad de la información en el IGP, mediante el correo electrónico soporteti@igp.gob.pe | OTIDG | Jefa de la OTIDG |

| | | | |
|---|---|---|---|
| **4** | **Revisar el contexto.**<br>Al inicio de cada ciclo de gestión de riesgos de seguridad de la información, el Comité de Gobierno Digital - CDG debe evaluar los cambios en el contexto interno y externo de la institución a través de la revisión de:<br>• **PR Nº 002-F01 Contexto de la Organización**<br>• objetivos y estrategias, así como también las disposiciones legales, reglamentarias, necesidades y expectativas que son relevantes para el desarrollo del proceso de gestión de riesgos, asegurando que el SGSI pueda lograr los resultados deseados | CGD | Oficial de Seguridad de la Información |
| **5** | **Identificar los riesgos.**<br>Identificar, registrar, clasificar y valorar los activos de información, según el formato:<br>• **PR Nº 00X-F01 Gestión de Activos de Información**<br>y los siguientes anexos:<br>• **Anexo I - Clasificación de los activos de información**.<br>• **Anexo II - Escala de valoración de activos de información**.<br>Para la valoración de activos se deberá tener en cuenta también lo siguiente:<br>• Los activos son valorados sin tener en consideración la existencia de controles (políticas, mecanismos de respaldos de los activos, planes de contingencia, etc.)<br>• Para la valoración de un activo, se considera la dependencia que puede tener en relación con otros activos, ya que esto puede influenciar en los valores.<br>• La valoración puede ser realizada durante entrevistas o talleres con el personal involucrado dentro del alcance establecido dentro del SGSI. | Unidades de Organización / CGD | Propietario del activo / Oficial de Seguridad de la Información |

| | | | |
|---|---|---|---|
| **6** | **Identificar los riesgos.**<br>Clasificar los activos de tipo información, de acuerdo con el siguiente criterio, definido por su nivel de accesibilidad:<br><br>**Clasificación de Información**<br>**Pública**: Información cuyo contenido puede ser conocido y distribuido sin ninguna restricción.<br>**Confidencial**: Información accesible solo por la dirección o personal concreto.<br>**Interna**: Información accesible solo al personal de una organización o una unidad organizacional en particular. | Unidades de Organización / CGD | Propietario del activo / Oficial de Seguridad de la Información |
| **7** | **Identificar los riesgos.**<br>Utilizando el siguiente criterio:<br>• Los activos con una valoración mayor o igual a 4 serán considerados para la etapa de análisis y evaluación de riesgos de seguridad de la información.<br>identificar y distinguir los activos con escalas de valoración<br>• Alto (4)<br>• Muy Alto (5)<br>de modo que se asegure la identificación de riesgos para dichos activos. | Unidades de Organización / CGD | Propietario del activo / Oficial de Seguridad de la Información |

| | | | |
|---|---|---|---|
| **8** | **Identificar los riesgos.**<br>Para los activos con escalas de valoración Alto (4) y Muy Alto (5), identificar las vulnerabilidades de los activos de información, las causas o amenazas que puedan determinar la materialización de un evento de seguridad de la información, su posible consecuencia o afectación, relacionándolos con la identificación de riesgos de seguridad de la información. Todo lo anterior se realiza mediante la documentación de fuentes como:<br>• Entrevistas no estructuradas con los responsables de los activos<br>• El desarrollo del flujo de la información en el proceso<br>• Fuentes estadísticas y tendencias de los riesgos de seguridad y privacidad<br>• Observaciones de expertos y analistas,<br>Identificación de riesgos.<br>Documentar en:<br>• **PR Nº 00X-F02 Matriz de Riesgos de Seguridad de la Información**<br>para cada activo con escalas de valoración Alto y Muy Alto, la descripción del riesgo inherente, propietario de riesgo y los demás datos considerados en el formato. | Unidades de Organización / CGD | Propietario del activo / Oficial de Seguridad de la Información |
| **9** | **Identificar los riesgos.**<br>Documentar en:<br>• **PR Nº 00X-F02 Matriz de Riesgos de Seguridad de la Información**<br>para cada activo con escalas de valoración Alto y Muy Alto, la descripción del riesgo inherente, propietario de riesgo y los demás datos considerados en el formato. | Unidades de Organización / CGD | Propietario del activo / Oficial de Seguridad de la Información |

| | | | |
|---|---|---|---|
| **10** | **Analizar los riesgos.**<br>Comenzar el análisis de riesgo utilizando los criterios de probabilidad e impacto consignados en el<br>• **Anexo III Escalas de Probabilidad de Ocurrencias e Impacto del Riesgo de Seguridad de la Información** consignando el resultado de cada criterio en:<br>• **PR Nº 00X-F02 Matriz de Riesgos de Seguridad de la Información** | Unidades de Organización / CGD | Propietario del activo / Oficial de Seguridad de la Información |
| **11** | **Analizar los riesgos.**<br>Calcular nivel de riesgo inherente mediante el multiplicación de los valores de probabilidad e impacto según:<br>• **Anexo IV Cálculo del Nivel de Riesgo de Seguridad de la Información y Criterios Para su Tratamiento** | Unidades de Organización / CGD | Propietario del activo / Oficial de Seguridad de la Información |
| **12** | **Analizar los riesgos.**<br>Identificar los controles existentes o implementar nuevos controles realizando la identificación del tipo de control y la evaluación de controles, según:<br>• **Anexo V Tipos de Controles y Evaluación de Controles** | Unidades de Organización / CGD | Propietario del activo / Oficial de Seguridad de la Información |

| | | | |
|---|---|---|---|
| **13** | **Valorar los riesgos.**<br>Utilizar tres valores:<br>• Alto<br>• Moderado<br>• Bajo<br>Los valores iguales y por debajo del moderado serán considerados riesgos aceptables o tolerables, los cuales no representan mayor afectación al cumplimiento de los objetivos actuales del SGSI.<br>Los riesgos de seguridad de la información valorados como "alto" se considerarán no tolerables y deberán abordarse a través de su tratamiento.<br>Considerar:<br>• Anexo **IV Cálculo del Nivel de Riesgo de Seguridad de la Información y Criterios Para su Tratamiento**<br>Esto se reflejará y consolidará en:<br>• **PR Nº 00X-F02 Matriz de Riesgos de Seguridad de la Información**<br>Con la conformidad del propietario de cada activo. Estos resultados se notificarán y presentarán al Comité de Gobierno Digital. | Unidades de Organización / CGD | Propietario del activo / Oficial de Seguridad de la Información |
| **14** | **Valorar los riesgos.**<br>Evaluar los riesgos identificados como aceptables en el siguiente ciclo de gestión de riesgos o como mínimo anualmente para verificar si continúan con los valores de probabilidad e impacto consignados originalmente o si deben ser modificados. | Unidades de Organización / CGD | Propietario del activo / Oficial de Seguridad de la Información |

| | | | |
|---|---|---|---|
| **15** | **Tratamiento de riesgos.**<br>Determinar el tratamiento, incluyendo los controles a implementarse (según corresponda) para abordar cada riesgo no tolerable según, consignándolo en:<br>• **PR Nº 00X-F03 Tratamiento de riesgos de seguridad de la información** | Unidades de Organización / CGD | Propietario del activo / Oficial de Seguridad de la Información |
| **16** | **Seguimiento y revisión.**<br>Realizar el seguimiento periódico al Tratamiento de Riesgo, considerando los estados definidos según el anexo **VI Estados de Seguimiento.** | CGD | Oficial de Seguridad de la Información |
| **17** | **Seguimiento y revisión.**<br>Realizar el seguimiento y revisión de la implementación de los controles del SGSI, cuyo resultado será informado al Comité de Gobierno Digital - CDG mediante presentaciones en las sesiones ordinarias. | CGD | Oficial de Seguridad de la Información |
| **18** | **Seguimiento y revisión.**<br>Tras la implementación de los controles, determinar el riesgo residual según el<br>• **Anexo VII Determinación del Riesgo Residual.**<br>Documentar el resultado en:<br>• **PR Nº 00X-F02 Matriz de Riesgos de Seguridad de la Información** | Unidades de Organización / CGD | Propietario del activo / Oficial de Seguridad de la Información |
| **19** | **Seguimiento y revisión.**<br>Informar al Comité de Gobierno Digital - CDG el resultado del análisis, evaluación y tratamiento de los riesgos, por lo menos una (1) vez al año. | CGD | Oficial de Seguridad de la Información |
| Fin del procedimiento | | | |

| DOCUMENTOS QUE SE GENERAN (Documento de salida del procedimiento) |
|---|
| -PR Nº 00X-F01 Gestión de Activos de Información |
| -PR Nº 00X-F02 Matriz de Riesgos de Seguridad de la Información |
| -PR Nº 00X-F02 Matriz de Riesgos de Seguridad de la Información |

## ANEXO I - CLASIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN

| TIPO DE ACTIVO | DESCRIPCIÓN |
|---|---|
| **Arquitectura del sistema** | Elementos que permiten estructurar el sistema, definiendo su arquitectura interna y sus relaciones con el exterior. |
| **Datos / Información** | Los datos son el corazón que permite a una organización prestar sus servicios. La información es un activo abstracto que será almacenado en equipos o soportes de información (normalmente agrupado como archivos o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos. |
| **Claves criptográficas** | La criptografía se emplea para proteger el secreto o autenticar a las partes. Las claves criptográficas, combinando secretos e información pública, son esenciales para garantizar el funcionamiento de los mecanismos criptográficos. |
| **Servicios** | Función que satisface una necesidad de los usuarios (del servicio). Esta sección contempla servicios prestados por el sistema. |
| **Software - Aplicaciones informáticas** | Con múltiples denominaciones (programas, aplicativos, desarrollos, etc.), se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.<br>No preocupa en este apartado el denominado “código fuente" o programas que serán datos de interés comercial, a valorar y proteger como tales. Dicho código aparecería como datos. |
| **Equipamiento informático (hardware)** | Dícese de los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos. |
| **Redes de comunicaciones** | Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro. |
| **Soportes de información** | Aquí se consideran dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo. |
| **Equipamiento auxiliar** | Consignamos otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos. |
| **Instalaciones** | En este epígrafe entran los lugares donde se hospedan los sistemas de información y comunicaciones |
| **Personas** | En sección aparecen las personas relacionadas con los sistemas de información |

## ANEXO II - ESCALA DE VALORACIÓN DE ACTIVOS DE INFORMACIÓN

La Valoración del Activo de Información se realiza mediante la identificación del impacto para el IGP por la pérdida de las propiedades, principios o fundamentos de la Seguridad de la Información, teniendo en cuenta la siguiente tabla de criterios:

**Tabla No 1: Escala para la valoración de activo**

| Valor | Escala de valoración de activos | Descripción cualitativa de cada escala |
|---|---|---|
| **5** | **Muy Alto** | Este tipo de activo contiene la información más crítica (calificada vital o esencial) en tal sentido debe tener una mayor protección. A la información (calificada vital o esencial) sólo pueden tener acceso las personas que expresamente han declaradas usuarios legítimos de esta información, y con los privilegios asignados. El conocimiento o divulgación no autorizada de la información que gestiona este activo impacta negativamente. |
| **4** | **Alto** | Consideraremos a este activo que contiene la información que es utilizada por los funcionarios y/o servidores, para realizar sus labores en los procesos y que no puede ser conocida por terceros sin autorización del propietario del activo. Este tipo de activo es vital para la entrega de servicios de la entidad si estos dejaran de funcionar perjudicaría la imagen de la institución y la continuidad de las operaciones del día a día. |
| **3** | **Medio** | Estos activos contienen información que en ocasiones puede ser necesaria para la entrega de servicios pero que en otras ocasiones se podría considerar información solo histórica. |
| **2** | **Bajo** | Este tipo de activo no cubren ningún tipo de misión crítica para la organización, la pérdida de estos activos solo generaría una leve afectación sobre los servicios prestados. |
| **1** | **Muy Bajo** | Este activo no es relevante para la organización, por lo general aquí están activos de prueba o auxiliares que no forman parte de los servicios de la institución. |

## ANEXO III - ESCALAS DE PROBABILIDAD DE OCURRENCIAS E IMPACTO DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

Se evalúa la **probabilidad** de ocurrencia del riesgo, tomando en cuenta los controles existentes, de acuerdo con la tabla siguiente:

| NIVEL | PROBABILIDAD | DESCRIPCIÓN | FRECUENCIA |
|---|---|---|---|
| **1** | **Muy baja** | Puede que no se haya presentado u ocurrir solo en circunstancias excepcionales. | Nunca o no se ha presentado en los últimos 5 años |
| **2** | **Baja** | Pudo ocurrir en algún momento, es poco común o frecuente | Al menos una vez en los últimos 5 años |
| **3** | **Media** | Puede ocurrir en algún momento | Al menos una vez en los últimos 2 años |
| **4** | **Alta** | Ocurrirá en la mayoría de las circunstancias | Al menos una vez en el último año |

La valoración del **impacto** que la materialización del riesgo de seguridad de la información puede ocasionar a la institución, se representa con la descripción de los siguientes niveles:

| NIVEL | IMPACTO | DESCRIPCIÓN | SEGURIDAD DE LA INFORMACIÓN |
|---|---|---|---|
| 1 | **Insignificante** | Si el hecho llegara a presentarse tendría consecuencias o efectos mínimos sobre la organización | Afecta a una actividad del proceso. |
| 2 | **Menor** | Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la organización | Afecta a un grupo de trabajo, a una persona, grupo de personas o algunas actividades del proceso. |

| | | | |
|---|---|---|---|
| 3 | **Moderado** | Si el hecho llegara a presentarse tendría medianas consecuencias o efectos sobre la organización | Afecta un conjunto de datos personales o el proceso.<br>Afectación a alguna parte interesada pertinente.<br>Afectación a la reputación de la organización. |
| 4 | **Mayor** | Si el hecho llegara a presentarse tendría altas consecuencias o efectos sobre la organización. | Afecta varios conjuntos de datos personales o procesos de la organización o toda la organización.<br>Afectación a las principales partes interesadas pertinentes.<br>Afectación económica, presupuestal o multas por incumplimiento de la misión o del marco legal.<br>Afectación grave a la reputación y legitimidad de la organización.<br>Suspensión de las actividades misionales de la organización, comprometiendo su sostenibilidad. |

## ANEXO IV CÁLCULO DEL NIVEL DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CRITERIOS PARA SU TRATAMIENTO

Con base en la determinación de la probabilidad y la valoración del impacto, se **calcula** el nivel de riesgo multiplicando ambos factores.

| Nivel de Riesgo = Impacto x Probabilidad |
|---|

### Valoración del Riesgo y Criterios Para su Tratamiento

Se considera que la probabilidad de que la amenaza identificada explote la vulnerabilidad y el impacto resultante sobre el activo evaluado, determina el nivel de riesgo, interpretado en las siguientes zonas de riesgo de acuerdo con el siguiente Mapa de Calor:

| Impacto<br>Probabilidad | Mayor (4) | Moderado (3) | Menor (2) | Insignificante (1) |
|---|---|---|---|---|
| Alta (4) | Alto (16) | Alto (12) | Alto (8) | Moderado (4) |
| Media (3) | Alto (12) | Alto (9) | Moderado (6) | Moderado (3) |
| Baja (2) | Alto (8) | Moderado (6) | Moderado (4) | Bajo (2) |
| Muy baja (1) | Moderado (4) | Moderado (3) | Bajo (2) | Bajo (1) |

Según la valoración, se establece la tolerancia a los riesgos y las acciones requeridas, tipificadas según la siguiente tabla:

| **Nivel del Riesgo de Seguridad de la Información** | | **Valor Asignado** | **Acción Requerida** |
|---|---|---|---|
| **Riesgo Alto** | No tolerable | Mayor a 6 | Evitar el riesgo empleando controles que busquen reducir el nivel de probabilidad. Reducir el riesgo empleando controles orientados a minimizar el impacto si el riesgo se materializa. Compartir o transferir el riesgo mediante la ejecución de pólizas. |
| **Riesgo Moderado** | Tolerable | 3 a 6 | Evitar o mitigar el riesgo mediante medidas adecuadas y aprobadas, que permitan llevarlo a la zona de riesgo moderado. Compartir o transferir el riesgo. Fortalecer los controles |

| | | | |
|---|---|---|---|
| | | | existentes o agregar nuevos controles. |
| **Riesgo Bajo** | | 0 a 2 | Asumir o aceptar el riesgo. Mantener mitigado el riesgo con actividades propias del proceso, manteniendo controles pre-existentes. |

**Los criterios para el tratamiento de riesgos de seguridad de la información son los siguientes:**

| Criterios | Explicación del criterio |
|---|---|
| Evitar el Riesgo | Esta estrategia consiste en no iniciar o no continuar con la actividad, eliminar la amenaza o proteger el proceso del impacto que puede generar el riesgo. Por ejemplo:<br>• La cancelación de una actividad o conjunto de actividades que generan el riesgo.<br>• Modificaciones de las condiciones en la que funciona la organización. |
| Mitigar el riesgo | Esta estrategia consiste en implementar medidas o controles para disminuir la posibilidad de ocurrencia o el impacto del riesgo. Por ejemplo:<br>• Eliminar la fuente del riesgo.<br>• Cambiar la probabilidad.<br>• Cambiar la consecuencia. |
| Aceptar el riesgo | Esta estrategia consiste en reconocer el riesgo y sus consecuencias y no tomar ninguna medida a menos que el riesgo se materialice. La estrategia de aceptar el riesgo implica que periódicamente se deberá revisar la amenaza para asegurarse que no ha aumentado significativamente.<br>Los riesgos a ser aceptados deberán ser aprobados formalmente. |
| Transferir el riesgo (Compartir) | Esta estrategia consiste en trasladar el impacto de una amenaza a un tercero, junto con la responsabilidad de la respuesta. El trasladar o compartir el riesgo no implica que deje de ser propietario de riesgo ni eliminar el riesgo. |

| | |
|---|---|
| | Entre las actividades que se pueden implementar tenemos:<br>• El uso de seguros.<br>• El uso de garantías de cumplimiento. |

## ANEXO V TIPOS DE CONTROLES Y EVALUACIÓN DE CONTROLES

| Tipo de Control | Descripción |
|---|---|
| Controles Preventivos | Son controles proactivos que ayudan a prevenir un riesgo.<br><br>Ejemplos de controles preventivos son segregación de funciones, autorización apropiada, documentación adecuada control físico sobre activos. |
| Controles Detectivos | Estos proporcionan evidencia de que una pérdida ha ocurrido, pero no previenen que una pérdida ocurra. Estos controles proporcionan evidencia de que los controles preventivos estén funcionando al prevenir pérdidas. Ejemplos de controles detectivos son revisiones, análisis, reconciliaciones, inventario físicos y auditorías. |
| Controles Correctivos | Los controles correctivos son los que ayudan a la investigación y corrección de las causas del riesgo. |

**Se evalúan los controles en función de:**

**A. Efectividad del Control (Diseño del Control)**

Se refiere a cuán bien definido está el control a nivel teórico, es decir, si tal cual ha sido planteado y documentado logra mitigar la parte del riesgo para lo cual fue concebido.

**Valorización de la efectividad del control**

| Niveles | Descripción |
|---|---|
| Fuerte | • El control es totalmente automatizado.<br>• La responsabilidad del control está asignada individualmente y formalizada y se ha asumido claramente dicha responsabilidad.<br>• Procedimiento del control está documentado y actualizado |
| Moderado | • Control combinado (manual-automatizado).<br>• La responsabilidad del control esta oficialmente asignada. |

| | |
|---|---|
| | • Procedimiento del control no muy complejo.<br>• Procedimiento del control documentado y no actualizado. |
| Débil | • Control totalmente manual.<br>• La responsabilidad del control no está asignada.<br>• Procedimiento del control muy complejo.<br>• Procedimiento del control no documentado |

**B. Impacto del Control (Ejecución del Control)**

Se refiere a cuán bien opera el control en la realidad (performance), es decir, si se realiza con la debida frecuencia (oportunidad) y con el debido cuidado (adecuado).

**Valorización del Impacto del control**

| Niveles | Descripción |
|---|---|
| Fuerte | • Históricamente no se han detectado desviaciones del control.<br>• El control es autoevaluado regularmente.<br>• El Control es de aplicación continua y de frecuencia continua. |
| Moderado | • Históricamente se presentan muy pocas desviaciones del control.<br>• Ha sido auto evaluado con alguna frecuencia.<br>• El Control es discreto y periódico. |
| Débil | • Históricamente se presentan continuas desviaciones del control.<br>• Nunca ha sido autoevaluado.<br>• El Control es discreto (Muestreo) y esporádico. |

### C. Evaluación del Control

Los controles se evaluarán teniendo en cuenta los resultados obtenidos de la evaluación de su impacto y su efectividad.

**Evaluación del Control**

| **Efectividad** | **Impacto** | **Calificación de la** Evaluación del Control |
|---|---|---|
| Débil | Fuerte, Moderado o Débil | Débil |
| Fuerte, Moderado o Débil | Débil | Débil |
| Moderado | Fuerte | Fuerte |
| Fuerte | Moderado | Moderado |
| Fuerte | Fuerte | Fuerte |
| Moderado | Moderado | Moderado |

## ANEXO VI – ESTADOS DE SEGUIMIENTO

| Estado | Descripción |
|---|---|
| Pendiente | Se establecerá este estado una vez establecido los plazos que tomará la implementación del control. |
| En Proceso | Se establecerá este estado cuando ya se empezó con la implementación de acciones o controles establecidos. |
| Implementado | Se consignará este estado cuando ya se concluyó la implementación de las acciones de tratamiento del riesgo o controles |
| Suspendido | Se considera a aquellas acciones desestimadas. Se deberá justificar esta decisión, actualizar la estrategia de tratamiento y el valor de riesgo residual, de corresponder. |

## ANEXO VII - DETERMINACIÓN DEL RIESGO RESIDUAL

Para la determinación del riesgo residual se identificará si el control disminuye la probabilidad y el impacto o uno de ellos, una vez identificado se utilizará el siguiente cuadro:

| Calificación Total del Control | Probabilidad | Impacto |
|---|---|---|
| Fuerte | 2 niveles hacia abajo | 2 niveles hacia abajo |
| Moderado | 1 nivel hacia abajo | 1 nivel hacia abajo |
| Débil | 0 niveles hacia abajo | 0 niveles hacia abajo |