RESOLUCIÓN DE GERENCIA GENERAL

Lima, 04 DIC. 2019 N° 112 -2019-SERVIR-GG

Vistos: el Memorando N° 1023-2019-SERVIR/GG-OGAF de la Oficina General de Administración y Finanzas, el Informe N° 165-2019-SERVIR/GG-OGAF/SJTI de la Subjefatura de Tecnologías de Información, el Memorando N° 317-2019-SERVIR/GG-OPP de la Oficina de Planeamiento y Presupuesto, y;

CONSIDERANDO:

Que, mediante Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado, se declara al Estado peruano en proceso de modernización en sus diferentes instancias, dependencias, entidades, organizaciones y procedimientos, con la finalidad de mejorar la gestión pública y construir un Estado democrático, descentralizado y al servicio del ciudadano;

Que, la Política Nacional de Gobierno Electrónico, aprobada con Decreto Supremo N° 081-2013-PCM, prevé determinados lineamientos estratégicos para el Gobierno Electrónico, entre otros el relacionado con la seguridad de la información, el mismo que busca preservar la confidencialidad, integridad y disponibilidad de la Información; debiendo definirse lineamientos con el objetivo de mitigar el riesgo de exposición de información sensible del ciudadano;

Que, mediante Resolución Ministerial N° 004-2016-PCM, modificada por Resolución Ministerial N° 166-2017-PCM y Resolución Ministerial N° 087-2019-PCM, se aprobó el uso obligatorio de la Norma Técnica Peruana NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición, en todas las entidades integrantes del Sistema Nacional de Informática;

Que, la referida Norma Técnica especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información, también incluye requisitos para la evaluación y tratamiento de los riesgos de seguridad de la información orientados a las necesidades de la organización, el que comprende el Anexo A, que detalla los objetivos de control y controles de riesgos;

Que, en ese marco legal, la Subjefatura de Tecnologías de la Información de la Oficina General de Administración y Finanzas, propone la aprobación de los procedimientos denominados: "Gestión de Incidentes y Debilidades de Seguridad de la Información" y "Gestión de Riesgos y oportunidades de Seguridad de la Información", elaborados por el Oficial de Seguridad de la Información;

Que, de acuerdo con los pasos 1 y 2 del numeral 6.2.3 de la Norma Técnica Nº 001-2018-SGP, Norma Técnica para la implementación de la gestión por procesos en las entidades de la administración pública, aprobada por Resolución de Secretaría de Gestión Pública Nº 006- 2018-PCM/SGP, la elaboración de los procedimientos se encuentra a cargo del dueño del proceso y es aprobada de manera formal por la máxima autoridad administrativa de la entidad;

Que, por Memorando N° 317-2019-SERVIR/GG-OPP la Oficina de Planeamiento y Presupuesto, emitió opinión técnica favorable a las propuestas de procedimientos denominados: "Gestión de Incidentes y Debilidades de Seguridad de la Información" y "Gestión de Riesgos y oportunidades de Seguridad de la Información";

Con la visación de la Oficina General de Administración y Finanzas, la Oficina de Planeamiento y Presupuesto, y de la Oficina de Asesoría Jurídica; y,

De conformidad con lo establecido en el Decreto Supremo N° 081-2013-PCM, que aprobó la Política Nacional de Gobierno Electrónico; la Resolución Ministerial N° 004-2016-PCM y modificatorias, que aprobó el uso obligatorio de la Norma Técnica Peruana NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición, en todas las entidades integrantes del Sistema Nacional de Informática; la Norma Técnica Nº 001- 2018-SGP, Norma Técnica para la implementación de la gestión por procesos en las entidades de la administración pública, aprobada por Resolución de Secretaría de Gestión Pública Nº 006-2018-PCM/SGP; y el Reglamento de Organización y Funciones de la Autoridad Nacional del Servicio Civil — SERVIR aprobado por Decreto Supremo Nº 062-2008-PCM y modificatorias.

SE RESUELVE:

Artículo Primero.- Aprobar los procedimientos denominados: "Gestión de Incidentes y Debilidades de Seguridad de la Información" (código SJTI-PR-07, versión 01), y "Gestión de riesgos y oportunidades de Seguridad de la Información" (código SJTI-PR-08, versión 01); los mismos que como anexo forman parte de la presente Resolución.

Artículo Segundo.- Disponer que la Oficina General de Administración y Finanzas a través de la Subjefatura de Tecnologías de la Información realice las acciones necesarias para el cumplimiento y difusión de los Procedimientos aprobados en el artículo 1 de la presente Resolución.

Artículo Tercero.- Disponer la publicación de la presente Resolución en el Portal Institucional de SERVIR (www.servir.gob.pe).

Regístrese y comuníquese.

LILIANA SÁNCHEZ RUIZ
Gerente General (e)
AUTORIDAD NACIONAL DEL SERVICIO CIVIL

servir

HERRAMIENTA DEL PERÚ QUE CRECE

GESTIÓN DE INCIDENTES Y DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN

Procedimiento: SJTI-PR-07

Versión: 01

SUBJEFATURA DE TECNOLOGÍAS DE LA INFORMACIÓN

Elaborado por: Wilmer Balbín Balbín **Cargo:** Oficial de Seguridad de la Información **Fecha:** 29 OCT. 2019	**Firma:** AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° W. Balbín SJTI
Revisado: Fidel Flores Loayza **Cargo:** Coordinador de Modernización Institucional **Fecha:** 14 NOV. 2019	**Firma:** AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° F. FLORES OPP
Revisado por: Luis Ángel Espinal Redondez **Cargo:** Ejecutivo de la Jefatura de Tecnologías de Información **Fecha:** 29 OCT. 2019	**Firma:** AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° L. Espinal SJTI
Revisado por: Miguel Ángel Burgos Gallegos **Cargo:** Jefe de la Oficina de Administración y Finanzas (e) **Fecha:** 15 NOV. 2019	**Firma:** AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° M. Burgos OGAF
Aprobado por: Liliana Sánchez Ruiz **Cargo:** Gerente General (e) **Fecha:** 02 DIC. 2019	**Firma:** LILIANA SÁNCHEZ RUIZ Gerente General (e) AUTORIDAD NACIONAL DEL SERVICIO CIVIL

ÍNDICE

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° W. Balbín SJTI

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° L. Espinal SJTI

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° M. Burgos OGAF

I. OBJETIVO

Establecer las directrices y lineamientos para asegurar una adecuada identificación, reporte y consiguiente remediación de los incidentes y debilidades de seguridad de la información que podrían impactar negativamente a los activos de información de la Autoridad Nacional del Servicio Civil – SERVIR.

II. ALCANCE

La presente normativa abarca a todos los Órganos y Unidades Organicas de la Autoridad Nacional del Servicio Civil - SERVIR, asi como sobre sus proveedores, que en el desarrollo de sus funciones, responsabilidades y actividades encomendadas, accedan, utilicen conserven o realicen cualquier otra forma de tratamiento sobre la información almacenada en formato físico, magnético, electrónico, óptico o cualquier otro existente, almacenado o no en dispositivo o recurso infórmatico.

III. BASE NORMATIVA

3.1. Ley N° 30057, Ley del Servicio Civil.
3.2. Ley N.° 29733, Ley de Protección de Datos Personales.
3.3. Decreto Legislativo N° 1023, Decreto Legislativo que crea la Autoridad Nacional del Servicio Civil, rectora del Sistema Administrativo de Gestión de Recursos Humanos y modificatorias.
3.4. Decreto Supremo N° 062-2008-PCM, que aprueba el Reglamento de Organización y Funciones de la Autoridad Nacional del Servicio Civil – SERVIR y modificatorias.
3.5. Decreto Supremo N° 040-2014-PCM, aprueba el Reglamento General de la Ley del Servicio Civil.
3.6. Decreto Supremo N.° 003-2013-JUS, que aprueba el Reglamento de la Ley N.° 29733, Ley de Protección de Datos Personales.
3.7. Decreto Supremo Nº 051-2018-PCM Decreto Supremo que crea el Portal del software Público Peruano y establece disposiciones adicionales sobre el software Público Peruano.
3.8. Resolución Ministerial N° 004-2016-PCM, modificada por la Resolución Ministerial N° 166-2017-PCM aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 Tecnología de la Información Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información 2da. Edición", en todas las entidades integrantes del Sistema Nacional de Informática y modificatorias.
3.9. Resolución Ministerial N° 166-2017-PCM, que modifica el artículo 5 de la Resolución Ministerial N° 004-2016-PCM referente al Comité de Gestión de Seguridad de la Información.
3.10. Resolución Ministerial Nº 087-2019-PCM aprueba disposiciones sobre la conformación y funciones del Comité de Gobierno Digital.
3.11. Resolución de Presidencia Ejecutiva N° 051-2019-SERVIR-PE, que formaliza la aprobación del Plan Estratégico Institucional de la Autoridad Nacional del Servicio Civil – SERVIR extendido en su horizonte temporal para el periodo 2017-2022.
3.12. Resolución de Presidencia Ejecutiva N° 158-2019-SERVIR-PE, se aprueba la reconformación del Comité de Gobierno Digital de la Autoridad Nacional del Servicio Civil – SERVIR.

IV. DEFINICIONES

4.1. **Evento de seguridad de información**
Ocurrencia identificada de un estado de un sistema, servicio o que indica una posible violación de la política de seguridad de la información o la falla de medidas de seguridad (controles), o una situación previamente desconocida que pueda ser relevante para la seguridad.

4.2. **Debilidad de Seguridad de la Información**
Deficiencia que pueden ser explotadas por amenazas.

4.3. **Incidente de seguridad de información**
Es indicado por un único o una serie de eventos indeseados o inesperados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones de negocio y de amenazar la seguridad de la información.

4.4. **SERVIR**
Autoridad Nacional del Servicio Civil - SERVIR

4.5. **SJTI**
Subjefatura de Tecnologías de la Información.

V. REFERENCIAS

5.1. SJTI-MN-01 Manual del Sistema de Gestión de Seguridad de la Información
5.2. SJTI-MN-02 Manual de Lineamientos de Seguridad de la Información

VI. RESPONSABLES

6.1. Ejecutivo de la Subjefatura de la Tecnologías de la Información, es responsable de asegurar el cumpliminento del presente procedimiento, asimismo de asegurar su actualización y difusión.

6.2. Oficial de Seguridad de la Información, es responsable:
- Definir el flujo de reporte de incidentes y debilidades de seguridad de la información.
- Efectuar las acciones a fin de fortalecer las capacidades del personal, proveedores de servicio de SERVIR, permitiendo que estos puedan identificar y reportar los incidentes y debilidades de seguridad de la información.
- Gestionar los incientes y debilidades de seguridad de la información reportados a fin que estos no vuelvan a ocurrir, implementando las medidas correctivas necesarias.

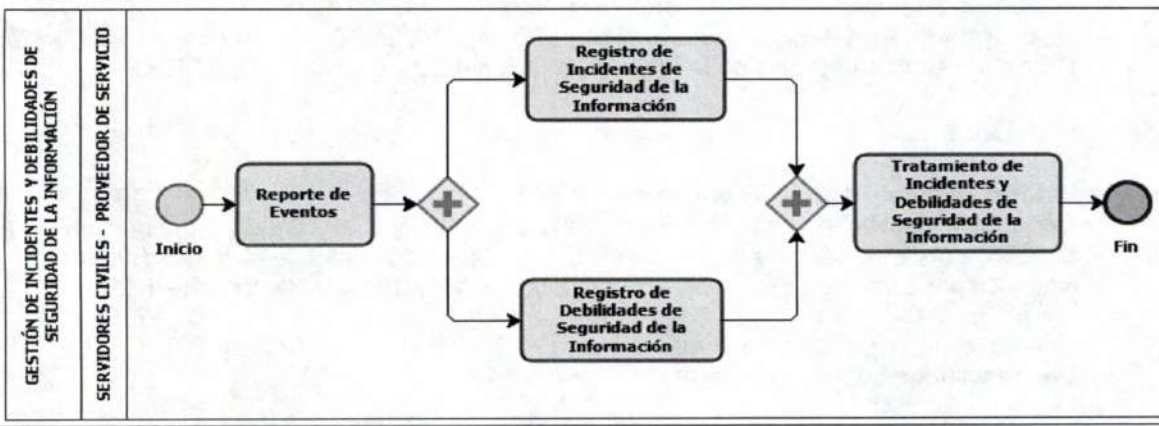
6.3. Los servidores, proveedores de servicio son responsables de identificar y reportar todo evento o debilidad de seguridad de la información que puedan presentarse en el desarrollo de sus actividades, dicha comunicación deberá ser efectuada al personal de soporte técnico de la Subjefatura de Tecnologías de la Información.

VII. FLUJO DEL PROCESO

7.1. GESTIÓN DE INCIDENTES Y DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN

PROVEEDOR	ENTRADA
Proceso de Gestión de incidentes y debilidades de seguridad de la información	Reporte de incidentes y debilidades de seguridad de la información

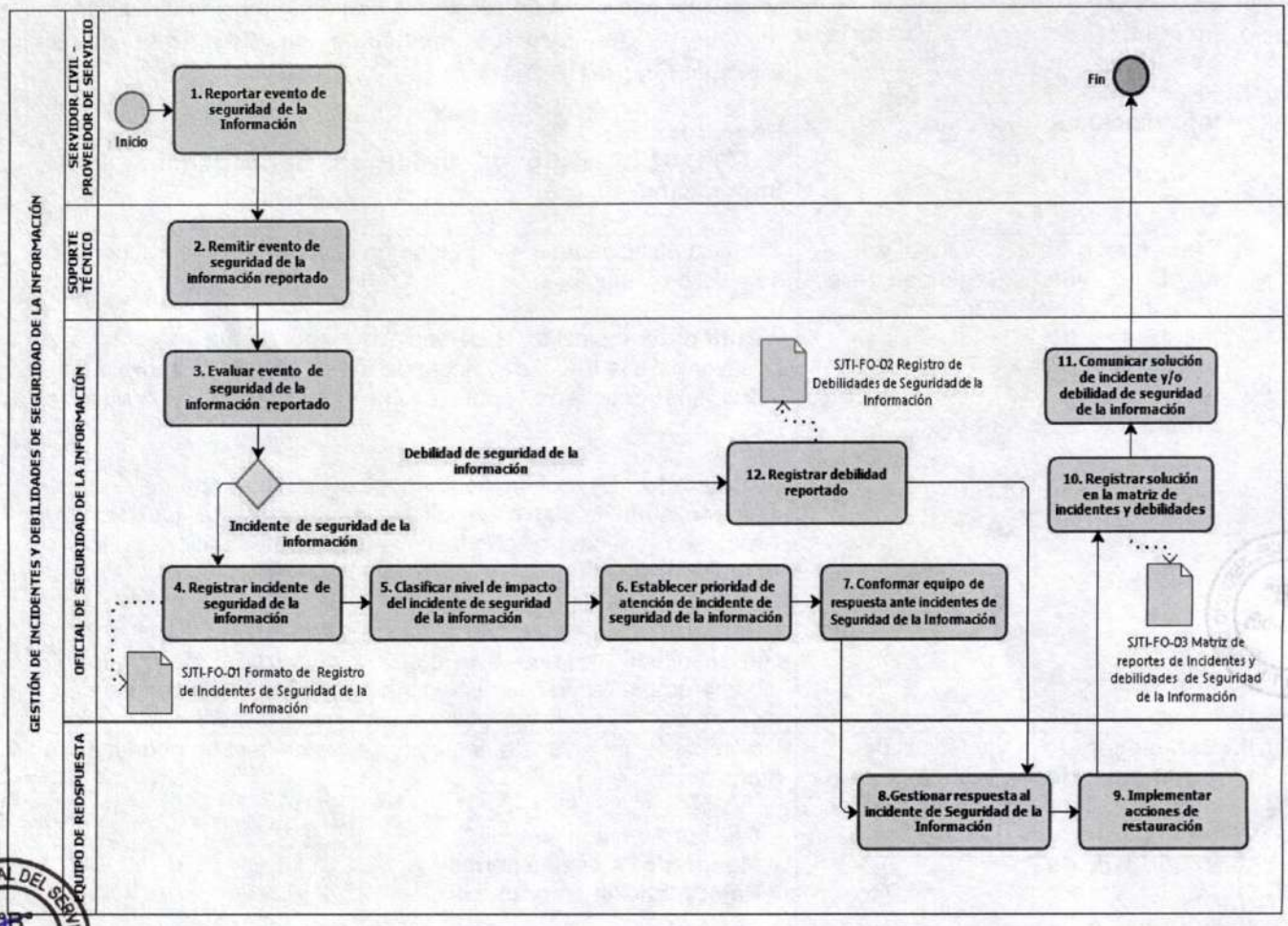
PROCESO



SALIDA	CLIENTE
Atención de incidentes y debilidades de Seguridad de la Información	Servidores Civiles y proveedores de servicio de SERVIR

VIII. DESARROLLO

8.1. FLUJOGRAMA



8.2. DESCRIPCIÓN

Actividad	Responsable	Descripción de las actividades
1. Reportar evento de seguridad de la información	Servidor Civil o Proveedor de Servicio	Reporta al personal de soporte técnico de la SJTI mediante correo electrónico, anexo telefónico o en forma presencial, el evento de seguridad de la información identificado, de acuerdo a la sede donde se generó el evento.
2. Remitir evento de seguridad de la información	Personal de Soporte Técnico	Remite el reporte de evento de seguridad de la información al Oficial de Seguridad de la Información.
3. Evaluar evento de Seguridad de la Información	Oficial de Seguridad de la Información	Evalua el evento de seguridad de la información reportado: - Si es un incidente de seguridad de la información, pasa a la actividad 4 para ser registrado. - Si es una debilidad de seguridad de la información, pasa a la actividad 12 para ser registrado.

Actividad	Responsable	Descripción de las actividades
4. Registrar Incidente de Seguridad de la Información	Oficial de Seguridad de la Información	Registra el incidente de seguridad de la información utilizando el formato de **Registro de Incidentes de Seguridad de la Información (SJTI-FO-01).** **Registros:** **SJTI-FO-01 Registro de Incidentes de Seguridad de la Información**
5. Clasificar el nivel de impacto del Incidente de seguridad de la Información	Oficial de Seguridad de la Información	Clasifica el incidente de seguridad de la información de acuerdo a su nivel de impacto: - **Crítico:** Es un incidente potencial que representa una amenaza mayor para la Entidad y afecta de forma inmediata a uno o más recursos críticos o pone en peligro información crítica o confidencial. - **Moderado:** Es un incidente que se puede representar una amenaza mayor y su materialización puede afectar a uno o mas recursos críticos o poner en peligro información crítica o confidencial. - **Bajo:** Es un incidente que podría ser una amenaza menor o es el resultado de una actividad no autorizada, pero que no compromete recursos crítico o información crítica o confidencial.
6. Establecer prioridad de atención de incidente de seguridad de la información	Oficial de Seguridad de la Información	De acuerdo al nivel de impacto se establece la prioridad de atención: - **Crítico:** Atención inmediata - **Moderado:** Atención normal - **Bajo:** Atención programada
7. Conformar equipo de respuesta ante incidentes de Seguridad de la Información	Oficial de seguridad de la Información	Conformará un equipo de respuesta ante incidentes de seguridad de la información con servidores civiles de SERVIR de acuerdo al incidente identificado, del cual el Oficial de Seguridad de la Información también formará parte.
8. Gestionar respuesta al incidente de Seguridad de la Información	Equipo de Respuesta	Establecerá acciones que permitan que el incidente no se propague y pueda generar mayores daños. La contención del incidente variará de acuerdo al incidente y a los criterios que el equipo de respuestas ante incidentes determine, priorizando siempre la preservación de la evidencia a fin de realizar los análisis respectivos.
9. Implementar acciones de restauración	Equipo de Respuesta	Una vez que el incidente de seguridad de la información haya sido controlado, y de acuerdo a los resultados de la investigación, él equipo de respuestas ante incidentes de seguridad de la nformación debe establecer acciones para que prevengan la ocurrencia de incidencias de este tipo a futuro.

Actividad	Responsable	Descripción de las actividades
10. Registrar solución en la matriz de incidentes y debilidades	Oficial de Seguridad de la Información	Registra las actividades realizadas en el formato de **Matriz de reportes de incidentes y debilidades de seguridad de la información (SJTI-FO-03).** Este registro srivirá **como** lecciones aprendidas para establecer las acciones a implementar ante la ocurrencia de incidentes similares que se susciten en SERVIR. **Registro:** **SJTI-FO-03 Registro de registro de Incidentes y debilidades de Seguridad de la Información**
11.Comunicar la solución	Oficial de Seguridad de la Información	Comunica la solución del incidente al servidor civil afectado.
12.Registrar debilidades de Seguridad de la Información reportada	Oficial de Seguridad de la Información	Se registra la debilidad de seguridad de la información reportada en el formato de **Registro de debilidades de seguridad de la Información (SJTI-FO-02).** Una vez registrado la debilidad de seguridad de la información pasa a la actividad 8 para tratamiento. **Registro:** **SJTI-FO-02 Registro de debilidades de seguridad de la información**

IX. ANEXOS

9.1. Anexo N° 01:SJTI-FO-01 Registro de incidentes de seguridad de la información.
9.2. Anexo N° 02:SJTI-FO-02 Registro de debilidades de Seguridad de la información.
9.3. Anexo N° 03:SJTI-FO-03 Matríz de reportes de Incidentes y debilidades de seguridad de la información.

X. CUADRO DE CONTROL DE CAMBIOS

VERSIÓN ANTERIOR	CAMBIOS	CARGO DE QUIEN MODIFICÓ
-	-	-

ANEXO N° 01
REGISTRO DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

servir HERRAMIENTA DEL PERÚ QUE CRECE	FORMATO	Código	SJTI-FO-01
	REGISTRO DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Versión	01
		Página	1 de 1

N°:	FECHA REPORTE:	HORA REPORTE:
DURACIÓN:	FECHA SOLUCIÓN:	HORA SOLUCIÓN:

DESCRIPCIÓN DEL INCIDENTE

NIVEL DE IMPACTO:	ALTO	☐	MODERADO	☐	BAJO	☐
PRIORIDAD DE ATENCIÓN:	ALTO	☐	MODERADO	☐	BAJO	☐

REPORTADO POR:

NOMBRES Y APELLIDOS:
CARGO:
ÓRGANO Y/O UNIDAD ORGANICA:
CORREO ELECTRONICO INSTITUCIONAL:
ANEXO:

EQUIPO DE RESPUESTA ANTE INCIDENTES

N°	NOMBRES Y APELLIDOS	ORGANO Y/O UNIDAD ORGANICA	CARGO	FIRMA

ACCIONES DE RESPUESTA AL INCIDENTE

N°	ACCIONES INMEDIATAS	FECHA	RESPONSABLE	RESPONSABLE DE SEGUIMIENTO

servir HERRAMIENTA DEL PERÚ QUE CRECE	FORMATO	Código	SJTI-FO-01
	REGISTRO DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Versión	01
		Página	1 de 2

CAUSA RAIZ DEL INCIDENTE

IMPACTO DEL SERVICIO O PROCESO

ACTIVO DE INFORMACIÓN AFECTADO

EVIDENCIA RECOLECTADA

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° W. Balbín SJTI

CONTROLES A IMPLEMENTAR PARA LA ERRADICACIÓN

N°	DETALLE	FECHA	RESPONSABLE	FIRMA

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° L. Estrada SJTI

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° M. Bargos OGAF

ANEXO N° 02
REGISTRO DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN

servir HERRAMIENTA DEL PERÚ QUE CRECE	FORMATO	Código	SJTI-FO-02
	REGISTRO DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	Versión	01
		Página	1 de 1

N°:	FECHA:	HORA:

DESCRIPCIÓN DE LA DEBILIDAD

REPORTADO POR:
NOMBRES Y APELLIDOS:
CARGO:
ÓRGANO Y/O UNIDAD ORGANICA:
CORREO ELECTRONICO INSTITUCIONAL:
ANEXO:

CONTROLES A IMPLEMENTAR

N°	CONTROLES A IMPLEMENTAR	PLAZO	RESPONSABLE	SEGUIMIENTO

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° W. Balbín SJTI

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° Espinal SJTI

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° M. Burgos OGAF

ANEXO N° 03
MATRIZ DE REPORTES DE INCIDENTES Y DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN

servir HERRAMIENTA DEL PERÚ QUE CRECE	FORMATO	Código:	SJTI-FO-03
	MATRIZ DE REPORTES DE INCIDENTES Y DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	Versión:	01
		Página:	1 de 1

N°	FUENTE	MES	INCIDENTES / DEBILIDAD	REPORTADO POR	SEDE	ACTIVO IMPACTADO	DESCRIPCIÓN DE SUCESO	CAUSA RAIZ	ESTADO	SOLUCIÓN REALIZADA

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° W. Balbin SJTI

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° L. Espital SJTI

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° M. Burgos OGAF

Formato: Digital	**La impresión de este documento desde la Intranet constituye una "COPIA NO CONTROLADA" a excepción de que se indique lo contrario.**	Clasificación: Uso Interno

HERRAMIENTA DEL PERÚ QUE CRECE

GESTIÓN DE RIESGOS Y OPORTUNIDADES DE SEGURIDAD DE LA INFORMACIÓN

Procedimiento: SJTI-PR-08

Versión: 01

SUBJEFATURA DE TECNOLOGÍAS DE LA INFORMACIÓN

Elaborado por: Wilmer Balbín Balbín **Cargo:** Oficial de Seguridad de la Información **Fecha:** 29 OCT. 2019	**Firma:** V°B° W. Balbín SJTI
Revisado: Fidel Flores Loayza **Cargo:** Coordinador de Modernización Institucional **Fecha:** 14 NOV. 2019	**Firma:** V°B° MODERNIZACIÓN OPP
Revisado por: Luis Ángel Espinal Redondez **Cargo:** Ejecutivo de la Jefatura de Tecnologías de Información **Fecha:** 29 OCT. 2019	**Firma:** V°B° L. Espinal SJTI
Revisado por: Miguel Ángel Burgos Gallegos **Cargo:** Jefe de la Oficina de Administración y Finanzas (e) **Fecha:** 15 NOV. 2019	**Firma:** V°B° M. Burgos OGAF
Aprobado por: Liliana Sánchez Ruiz **Cargo:** Gerente General (e) **Fecha:** 02 DIC. 2019	**Firma:** LILIANA SÁNCHEZ RUIZ Gerente General (e) AUTORIDAD NACIONAL DEL SERVICIO CIVIL

ÍNDICE

I. OBJETIVO

Establecer las bases para la adecuada gestión de riesgos y oportunidades de seguridad de la información a fin de garantizar la confidencialidad, integridad y disponibilidad de los activos de información de propiedad de la Autoridad Nacional del Servicio Civil – SERVIR.

II. ALCANCE

El presente procedimiento se aplica a los activos de información de aquellos procesos que forman parte del Sistema de Gestión de Seguridad de la Información.

III. BASE NORMATIVA

3.1. Ley N° 30057, Ley del Servicio Civil.
3.2. Ley N.° 29733, Ley de Protección de Datos Personales.
3.3. Decreto Legislativo N° 1023, Decreto Legislativo que crea la Autoridad Nacional del Servicio Civil, rectora del Sistema Administrativo de Gestión de Recursos Humanos y modificatorias.
3.4. Decreto Supremo N° 062-2008-PCM, que aprueba el Reglamento de Organización y Funciones de la Autoridad Nacional del Servicio Civil – SERVIR y modificatorias.
3.5. Decreto Supremo N° 040-2014-PCM, aprueba el Reglamento General de la Ley del Servicio Civil.
3.6. Decreto Supremo N.° 003-2013-JUS, que aprueba el Reglamento de la Ley N.° 29733, Ley de Protección de Datos Personales.
3.7. Decreto Supremo Nº 051-2018-PCM Decreto Supremo que crea el Portal del software Público Peruano y establece disposiciones adicionales sobre el software Público Peruano.
3.8. Resolución Ministerial N° 004-2016-PCM, modificada por la Resolución Ministerial N° 166-2017-PCM aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 Tecnología de la Información Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información 2da. Edición", en todas las entidades integrantes del Sistema Nacional de Informática y modificatorias.
3.9. Resolución Ministerial N° 166-2017-PCM, que modifica el artículo 5 de la Resolución Ministerial N° 004-2016-PCM referente al Comité de Gestión de Seguridad de la Información.
3.10. Resolución Ministerial Nº 087-2019-PCM aprueba disposiciones sobre la conformación y funciones del Comité de Gobierno Digital.
3.11. Resolución de Presidencia Ejecutiva N° 051-2019-SERVIR-PE, que formaliza la aprobación del Plan Estratégico Institucional de la Autoridad Nacional del Servicio Civil – SERVIR extendido en su horizonte temporal para el periodo 2017-2022.
3.12. Resolución de Presidencia Ejecutiva N° 158-2019-SERVIR-PE, se aprueba la reconformación del Comité de Gobierno Digital de la Autoridad Nacional del Servicio Civil – SERVIR.

IV. DEFINICIONES

Se ha utilizado los términos y definiciones de la ISO/IEC 27000, tales como:

4.1. Activo de Información
Información que tiene valor para la Entidad, pudiendo además ser aquel recurso (humano, tecnológico, etc.) que efectúa tratamiento directo o indirecto de la información que soporta uno o más procesos de la Entidad.

4.2. Amenaza
Cualquier acción o evento que pueda ocasionar consecuencia adversa.

4.3. Análisis de Riesgo
Identificar y evaluar el nivel de riesgo, tomando en cuenta los activos expuestos o amenazados.

4.4. Clasificación de Activo de Información
Categorización de los activos de información que tienen valor para la Entidad.

4.5. Confidencialidad
Característica/propiedad por el cual la Información no está disponible o revelada a individuos o entidad no autorizados

4.6. Disponibilidad
Característica/propiedad por la cual la información permanece accesible y disponible para su uso cuando lo requiera una persona o entidad autorizada.

4.7. Equipo de Riesgo
Equipo multidisciplinario conformado por servidores civiles y/o proveedores de servicios que realizan la gestión de riesgos de seguridad de la información.

4.8. Integridad
Característica/propiedad por la cual la información conserva su exactitud y se encuentra completa.

4.9. Impacto
Impacto o perjuicio que puede generar la amenaza más significativa en el activo de información, el nivel de impacto puede ser bajo, medio, alto.

4.10. Probabilidad
Medida del grado de posibilidad de que una amenaza explote una vulnerabilidad.

4.11. Propietario del activo de información
Una persona, cargo, proceso o grupo de trabajo designado por la organización, quien tiene la responsabilidad de definir los controles y/o lineamientos para el cuidado de los activos de información, bajo su responsabilidad.

4.12. Propietario del riesgo
Persona que tiene la responsabilidad y la autoridad para gestionar un riesgo. Dueño del Proceso.

4.13. Riesgo
Efecto de incertidumbre sobre los objetivos. Un efecto de desviación de aquello que se espera, sea positivo, negativo o ambos.

4.14. Riesgo residual
Riesgo que permanece después de implementar las actividades relacionadas con el tratamiento de un riesgo.

4.15. SERVIR
Autoridad Nacional del Servicio Civil

4.16. SGSI
Sistema de Gestión de Seguridad de la Información.

4.17. SJTI
Subjefatura de Tecnologías de la Información

4.18. Valoración de riesgos de seguridad de la información
Proceso que consiste en la identificación, análisis y evaluación de riesgos de seguridad de la información.

4.19. Valoración de oportunidades de seguridad de la información
Proceso que consiste en la identificación, análisis y evaluación de oportunidad de seguridad de la información.

4.20. Tratamiento de riesgo de seguridad de la información
Proceso de selección e implementación de controles para minimizar el riesgo de seguridad de la información.

4.21. Tratamiento de oportunidad de seguridad de la información
Proceso de selección e implementación de controles para lograr beneficios de seguridad de la información.

4.22. Vulnerabilidad
Debilidad de un activo o de control que puede ser explotado por una o más amenazas.

V. REFERENCIAS

5.1. SJTI-MN-01, Manual del Sistema de Gestión de Seguridad de la Información.

VI. RESPONSABLES

6.1. El Oficial de Seguridad de la Información es responsable de:

- Realizar talleres para el equipo de riesgo designado por el responsable del Órgano y/o Unidad Orgánica para el desarrollo de la gestión de riesgos y oportunidades de seguridad de la información.

- Revisar y actualizar el presente procedimiento como consecuencia del ciclo natural de mejora continua del proceso de gestión de riesgos y oportunidades de seguridad de la información, o por cambios en los aspectos del entorno de la Entidad, según sea necesario y apropiado.

6.2. El Equipo de Riesgo es responsable de:

- Participar en los talleres para la gestión de riesgos y oportunidades de seguridad de la información.
- Identificar los riesgos y oportunidades de seguridad de la información de los procesos que se encuentran en sus Órganos y/o Unidades Orgánicas.

6.3. El Propietario del Riesgo es responsable de:

- Aprobar la información documentada resultante del proceso de gestión de riesgos y oportunidades de seguridad de la información.
- Decidir el criterio para la aceptación de riesgos y oportunidades de seguridad de la información y los niveles de riesgo aceptables.

6.4. El Comité de Gobierno Digital es el responsable de:

- Revisar los resultados de la gestión de riesgos y oportunidades de seguridad de la información y el estado de implementación del plan de tratamiento de riesgos y oportunidades de seguridad de la información.

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° W. Balbín SJTI

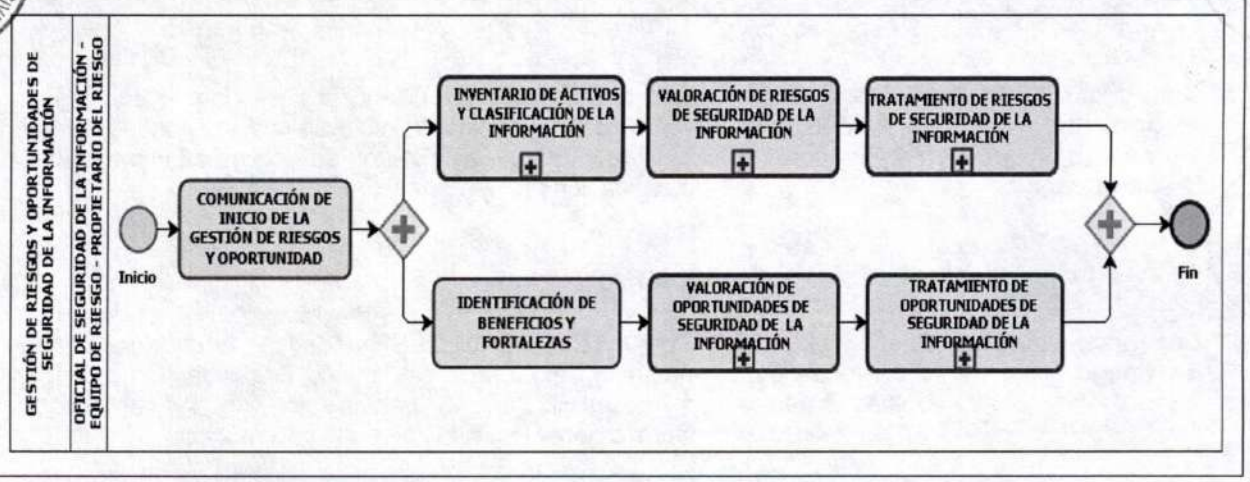
VII. FLUJO DEL PROCESO

7.1. GESTIÓN DE RIESGOS Y OPORTUNIDADES DE SEGURIDAD DE LA INFORMACIÓN

PROVEEDOR	ENTRADA
Proceso que implemente el Sistema de Gestión de Seguridad de la Información	Inventario de activos de información, beneficios y fortalezas de Seguridad de la Información.

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° L. Espinal SJTI

PROCESO

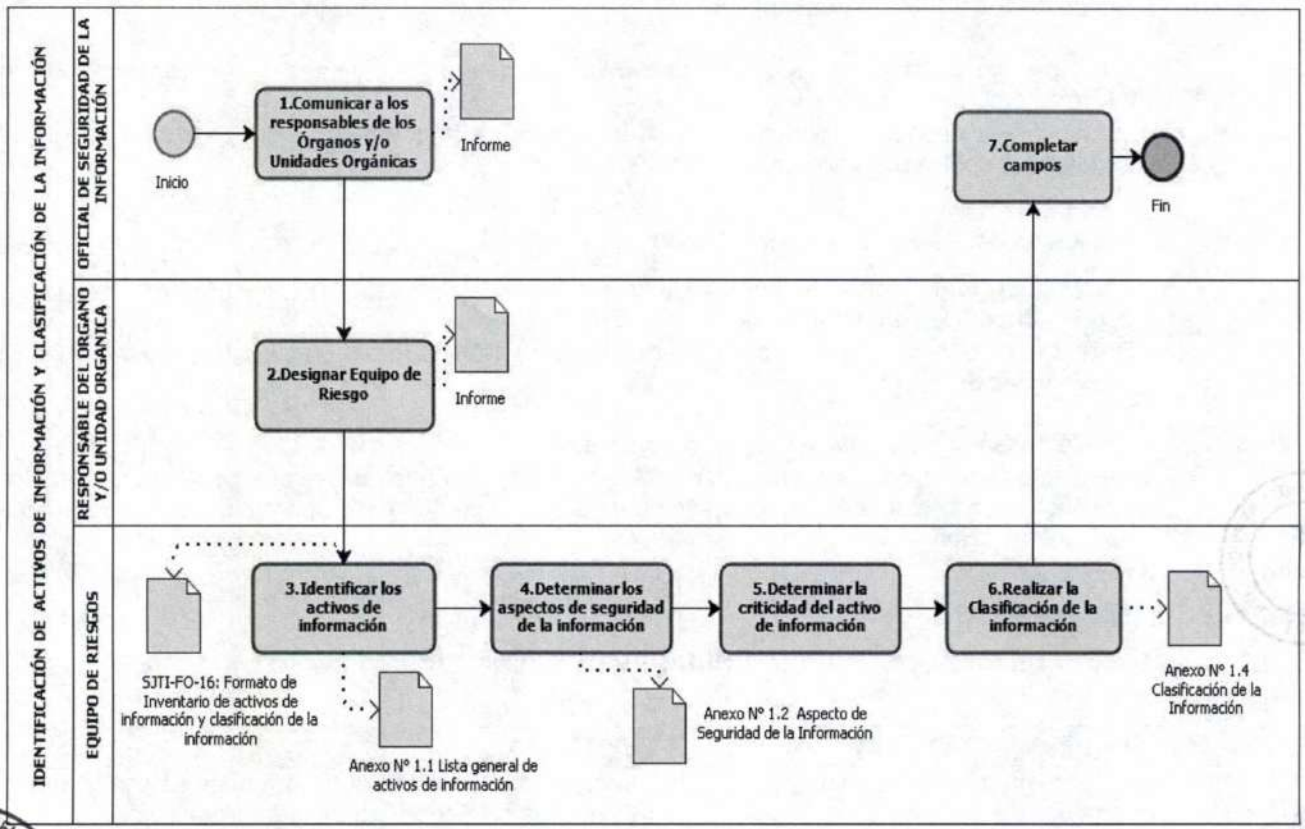


SALIDA	CLIENTE
Plan de tratamiento de riesgos y oportunidades de Seguridad de la Información	Responsable del proceso que implemente el Sistema de Gestión de Seguridad de la Información

VIII. DESARROLLO

8.1. IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN Y CLASIFICACIÓN DE LA INFORMACIÓN

8.1.1. FLUJOGRAMA



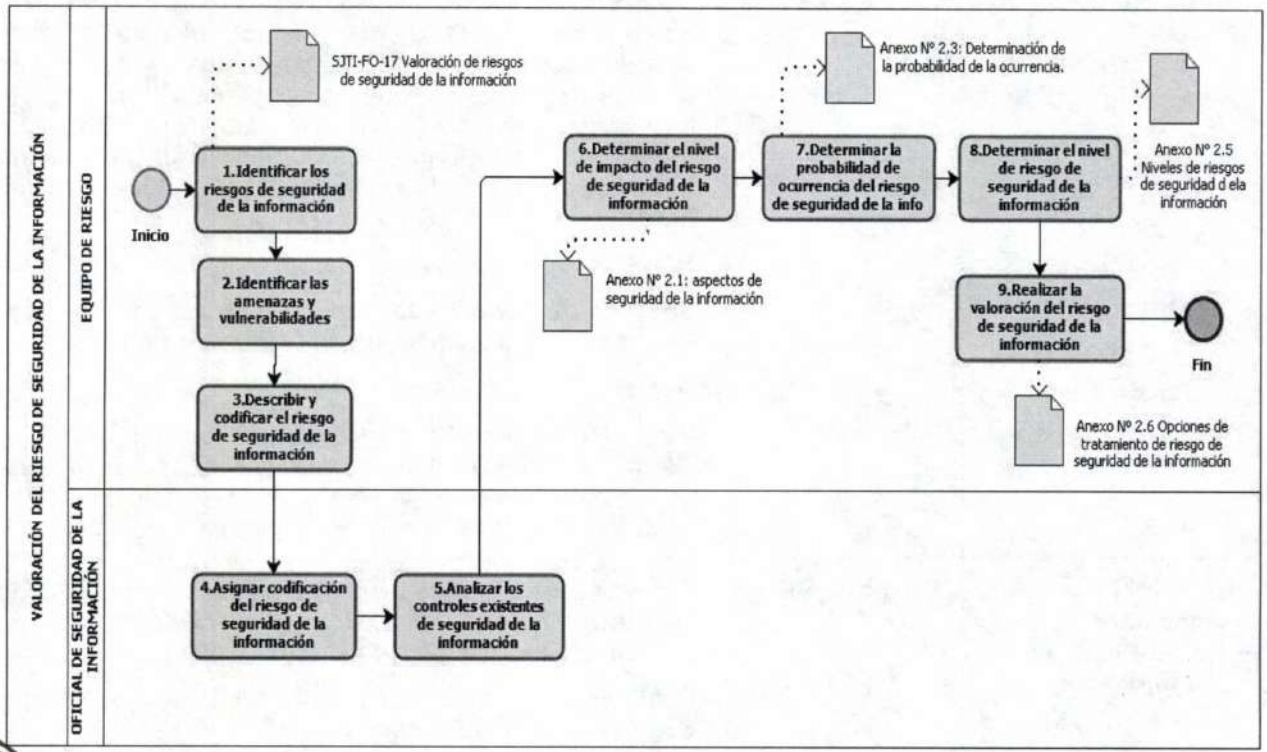
8.1.2. DESCRIPCIÓN

Actividad	Responsable	Descripción de las actividades
1. Comunicar al responsable del Órgano y/o Unidad Orgánica	Oficial de Seguridad de la Información	Comunica mediante informe al responsable del Órgano y/o Unidad Orgánica el inicio de las actividades para el desarrollo de la identificación de activos de información y clasificación de la información. **Registro:** **Informe.**
2. Designar Equipo de Riesgo	Responsable del Órgano y/o Unidad Orgánica	Comunica al Oficial de Seguridad de la Información que personal del Órgano y/o Unidad Orgánica participará en el desarrollo de la identificación de los activos de información y clasificación de la información. **Registro:** **Informe.**

Actividad	Responsable	Descripción de las actividades
3. Identificar los activos de información	Equipo de Riesgo	Identifica los activos de información utilizando la **lista general de activos de información (Anexo N° 1.1),** asimismo, completa los siguientes campos: proceso, tipo de activo, categoría del activo, nombre del activo, descripción del activo, propietario del activo, ubicación física/lógica en el formato de **Inventario de activos de información y clasificación de la información (SJTI-FO-16).** **Registro:** **SJTI-FO-16: Formato de inventario de activos de información y clasificación de la información.** **Nota:** Para la identificación de los activos de información y clasificación de la información y gestión de riesgos se considera el contexto interno y externo, así como, las necesidades y expectativas de las partes interesadas.
4. Determinar los aspectos de seguridad de la Información	Equipo de Riesgo	Determina los aspectos de seguridad de la información de los activos de información, relacionados a la confidencialidad, integridad y disponibilidad. Para eso utiliza el **Anexo N° 1.2: Aspectos de Seguridad de la información.**
5. Determinar la criticidad del activo de información	Equipo de Riesgo Oficial de Seguridad de la Información	El Equipo de riesgo con el apoyo del Oficial de Seguridad de la Información determina la criticidad del activo de información de acuerdo a cinco (05) categorías: - **Muy Crítico.** - **Crítico.** - **Moderado.** - **Menor.** - **No significativo.** Su valor se determina de acuerdo a los aspectos de seguridad indicada en el punto 4.
6. Realizar la Clasificación de la información	Equipo de Riesgo	Realiza la clasificación de la información utilizando el cuadro de clasificación de la información (Anexo N° 1.4) en tres (03) categorías: - **Confidencial.** - **Interna.** - **Pública.**
7. Completar campos	Oficial de Seguridad de la Información	Será encargado de completar los demás campos del formato de Inventario de activos de información y clasificación de la información: Código del activo, fecha de registro del inventario, estado y fecha baja del activo. Los activos de información que tienen como nivel de criticidad: **Crítico y Muy Crítico** pasaran al proceso de identificación, análisis y evaluación de riesgos.

8.2. VALORACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

8.2.1. FLUJOGRAMA



8.2.2. DESCRIPCIÓN

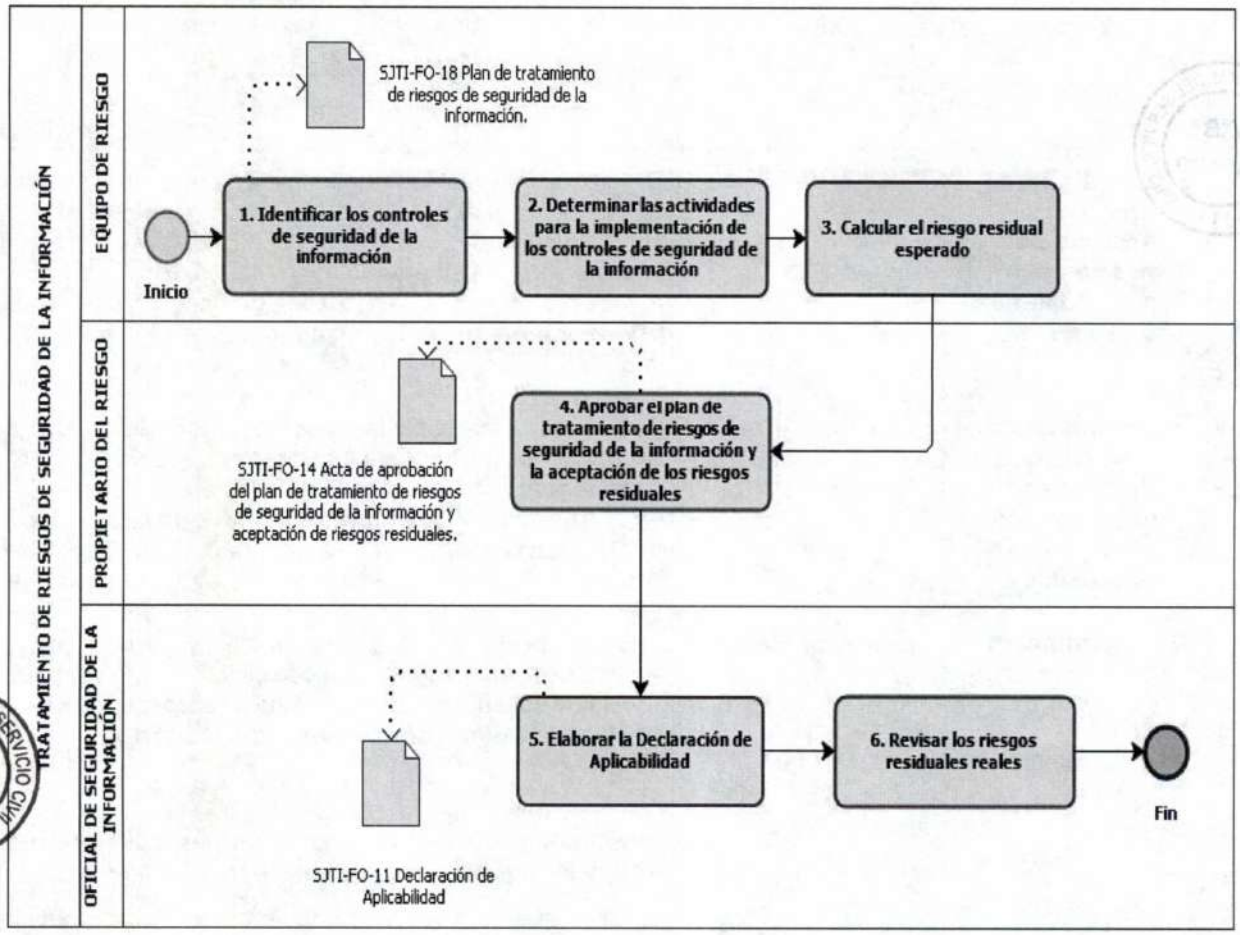
Actividad	Responsable	Descripción de las actividades
1. Identificar los riesgos de seguridad de la información	Equipo de Riesgo	Realiza la identificación de los riesgos de seguridad de la información utilizando el formato de **valoración de riesgos de seguridad de la información (SJTI-FO-17).** **Registro:** **SJTI-FO-17 Valoración de riesgos de seguridad de la información.**
2. Identificar las amenazas y vulnerabilidades	Equipo de Riesgo	En esta actividad se identifican las amenazas potenciales de los activos de información que tienen como nivel de criticidad Crítico y Muy Crítico, asimismo, se identifica sus vulnerabilidades más importantes que pueden ser explotadas por las amenazas identificadas.
3. Describir y codificar el riesgo de seguridad de la información	Equipo de Riesgo	Con el apoyo del Oficial de Seguridad de la Información se describe el nombre del riesgo, en base a la amenaza y vulnerabilidad identificadas en las actividades 2.

Actividad	Responsable	Descripción de las actividades
4. Asignar codificación del riesgo de seguridad de la información	Oficial de Seguridad de la Información	Asignará un código que hace referencia al riesgo de seguridad de la información identificado y la identificación del propietario del riesgo.
5. Analizar los controles existentes de seguridad de la información	Oficial de Seguridad de la Información	Analiza los controles existentes de seguridad de la información que se encuentran o no implementados, asimismo, se mide el cumplimiento del control y efectividad. **Nota:** El cumplimiento del control y la efectividad de los controles se mide de acuerdo a los siguientes puntos: **% Cumplimiento** / **Efectividad** 0% / No Existe 1% – 60% / Débil 61% - 89% / Moderado 90% - 100% / Fuerte
6. Determinar el nivel de impacto del riesgo de seguridad de la información	Equipo de Riesgo	Determina el nivel de impacto del riesgo de seguridad de la información asociado con la pérdida de la confidencialidad, integridad y disponibilidad de la información, considerando los criterios establecidos en el **Anexo N° 2.1: aspectos de seguridad de la información,** y a la efectividad de los controles implementados.
7. Determinar la probabilidad de ocurrencia del riesgo de seguridad de la información	Equipo de Riesgo	Determina la probabilidad de ocurrencia del riesgo de seguridad de la información en caso que este ocurra, considerando los criterios de clasificación establecidos en el **Anexo N° 2.3: Determinación de la probabilidad de la ocurrencia,** y a la efectividad de los controles implementados.
8. Determinar el nivel de riesgo de seguridad de la información	Equipo de Riesgo	Determina el nivel de riesgo de seguridad de la información en base a la probabilidad por el impacto, considerado en los criterios establecidos en el **Anexo N° 2.5: Niveles de riesgos de seguridad de la información.** Los riesgos de seguridad de la información considerados con los niveles de **Intolerante (rango 10 – 15)** y **Moderado (rango 9)** pasaran a tratamiento. En caso que se decida no implementar los controles de seguridad de la información valorados como **Intolerante (rango 10 – 15)** y **Moderado (rango 9)**, el propietario del riesgo se hace responsable de las consecuencias de este riesgo.
9. Realizar la	Equipo de Riesgo	Realiza la valoración del riesgo de seguridad de la

Actividad	Responsable	Descripción de las actividades
valoración del riesgo de seguridad de la información		información identificado en la actividad 8. La valoración del riesgo se determina las siguientes opciones de tratamiento: - **Aceptar** - **Compartir** - **Reducir** - **Evitar** La descripción de las opciones de tratamiento se considera en el **Anexo N° 2.6 Opciones de tratamiento de riesgo de seguridad de la información.**

8.3. TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

8.3.1. FLUJOGRAMA



AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° W. Balbín SJTI

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° J. Espinal SJTI

8.3.2. DESCRIPCIÓN

Actividad	Responsable	Descripción de las actividades
1. Identificar los controles de seguridad de la información	Oficial de Seguridad de la Información	Identifica los controles de seguridad de la información que permitirán mitigar los riesgos identificados en la evaluación de riesgos de seguridad de la información a través del formato **Plan de tratamiento de riesgos de seguridad de la información (SJTI-FO-09).** Para efectos de la definición de controles, se adoptara la norma técnica peruana "NTP ISO/IEC 27002:2017 Tecnología de la información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información". **Registro:** **SJTI-FO-18 Plan de tratamiento de riesgos de seguridad de la información.**
2. Determinar las actividades para la implementación de los controles de seguridad de la información	Equipo de Riesgo	Determina las actividades a realizar para la implementación de los controles de seguridad de la información establecidos en la actividad 1, asimismo, se registra al responsable de realizar la implementación, el Órgano y/o Unidad Orgánica encargado, el tiempo que tomará realizar la implementación de los controles, la priorización de la implementación de los controles, el estado de avance y porcentaje de avance de la implementación. **Nota:** La implementación de los controles de seguridad de la información se priorizará de acuerdo al mayor rango de nivel de riesgos de seguridad de la información alcanzado.
3. Calcular el riesgo residual esperado	Equipo de Riesgo	Calcula el riesgo residual esperado que se lograría con la implementación de los controles de seguridad de la información indicados en la actividad 1. El riesgo residual esperado se obtiene del producto de la probabilidad y el impacto, asimismo, el impacto está relacionado con los aspectos de seguridad de la información, la confidencialidad, integridad y disponibilidad. **Nota:** El nivel del riesgo residual esperado debe ser aceptable es decir **Moderado (rango 6 – 8)** o **Tolerable (rango 1 – 5)**, en caso no fuera así, se deberá revisar las actividades de tratamiento hasta alcanzar un nivel del riesgo residual aceptable.
4. Aprobar el plan de tratamiento de riesgos de seguridad de la información y la aceptación de los riesgos residuales	El propietario del Riesgo	Aprueba el plan de tratamiento de riesgo y la aceptación de los riesgos residuales a través del **Acta de aprobación del plan de tratamiento de riesgos de seguridad de la información y riesgos residuales (SJTI-FO-14).** Para dicha actividad el Oficial de Seguridad de la Información realizará las coordinaciones con el responsable del proceso y el propietario del riesgo.

AUTORIDAD NACIONAL DEL SERVICIO CIVIL VºBº W. Balbín SJTI

AUTORIDAD NACIONAL DEL SERVICIO CIVIL VºBº L. Espinal SJTI

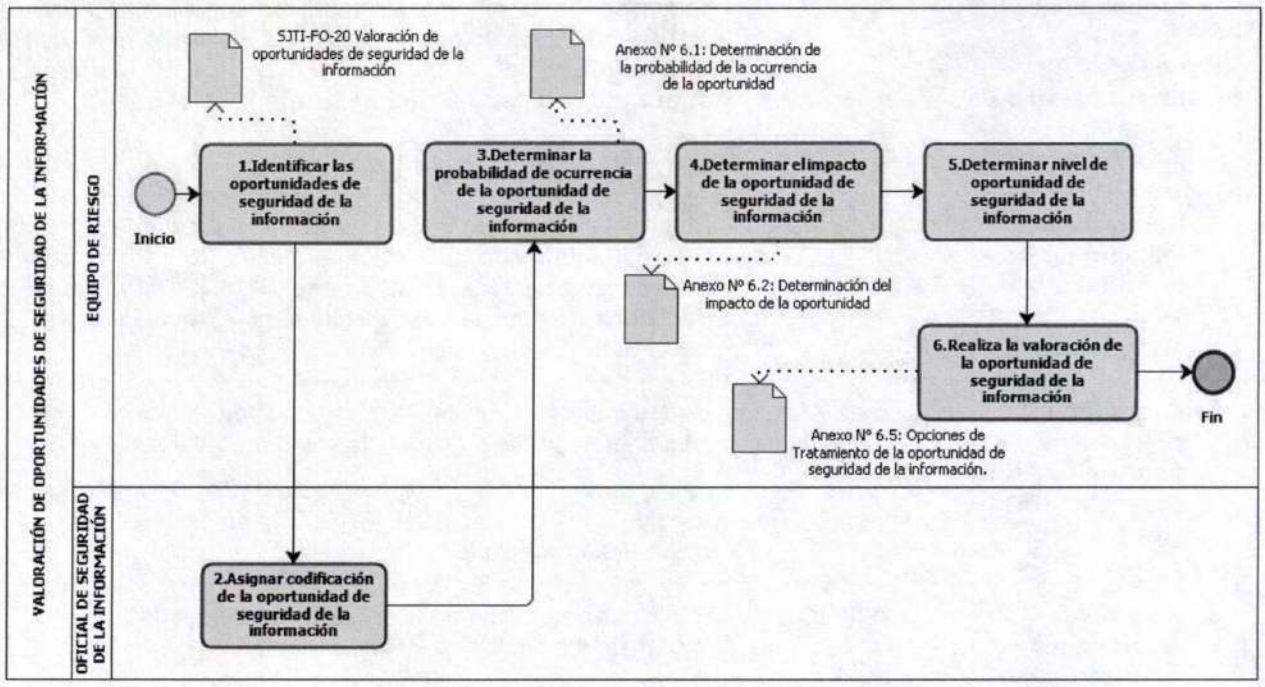
Actividad	Responsable	Descripción de las actividades
		Nota: El Oficial de Seguridad de la Información mantendrá custodia de los registros de la información documentada. **Registros:** **SJTI-FO-14 Acta de aprobación del plan de tratamiento de riesgos de seguridad de la información y aceptación de riesgos residuales.**
5. Elaborar la declaración de aplicabilidad	Oficial de Seguridad de la Información	Elabora el documento de "Declaración de Aplicabilidad" a través del formato **Declaración de Aplicabilidad (SJTI-FO-11)**, este documento enlista los controles de seguridad de la información establecidos en el anexo "A" del Norma Técnica Peruana NTP-ISO/IEC 27001:2014, asimismo, incluye la justificación de la inclusión o exclusión de cada uno de ellos, así como el documento relacionado, que sustenta su cumplimiento. **Registro:** **SJTI-FO-11 Declaración de Aplicabilidad.**
6. Revisar los riesgos residuales reales	Oficial de Seguridad de la Información	Revisa el riesgo residual esperado posterior a la implementación del control de seguridad de la información, para verificar su eficacia y confirmar si se alcanzó el nivel de riesgo esperado, en el caso que no se logre, se tiene que evaluar y/o replantear el control.

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° W. Balbin SJTI

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° L. Espinal SJTI

8.4. VALORACIÓN DE OPORTUNIDADES DE SEGURIDAD DE LA INFORMACIÓN

8.4.1. FLUJOGRAMA



8.4.2. DESCRIPCIÓN

Actividad	Responsable	Descripción de las actividades
1. Identificar las oportunidades de seguridad de la información	Equipo de Riesgo	En esta actividad se identifica las oportunidades de seguridad de la información en base a los beneficios y fortalezas utilizando el formato **Valoración de oportunidades de seguridad de la información (SJTI-FO-20).** Asimismo, se establece los siguientes campos: - Proceso - Fuente de Oportunidad - Descripción de la Oportunidad - Beneficios - Fortalezas **Registro:** **SJTI-FO-20 Valoración de oportunidades de seguridad de la información.**
2. Asignar codificación de la oportunidad de seguridad de la información	Oficial de Seguridad de la Información	Asigna un código que hace referencia a la oportunidad de seguridad de la información identificado y la identificación del propietario de la oportunidad.

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° W. Balbín SJTI

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° L. Asunal SJTI

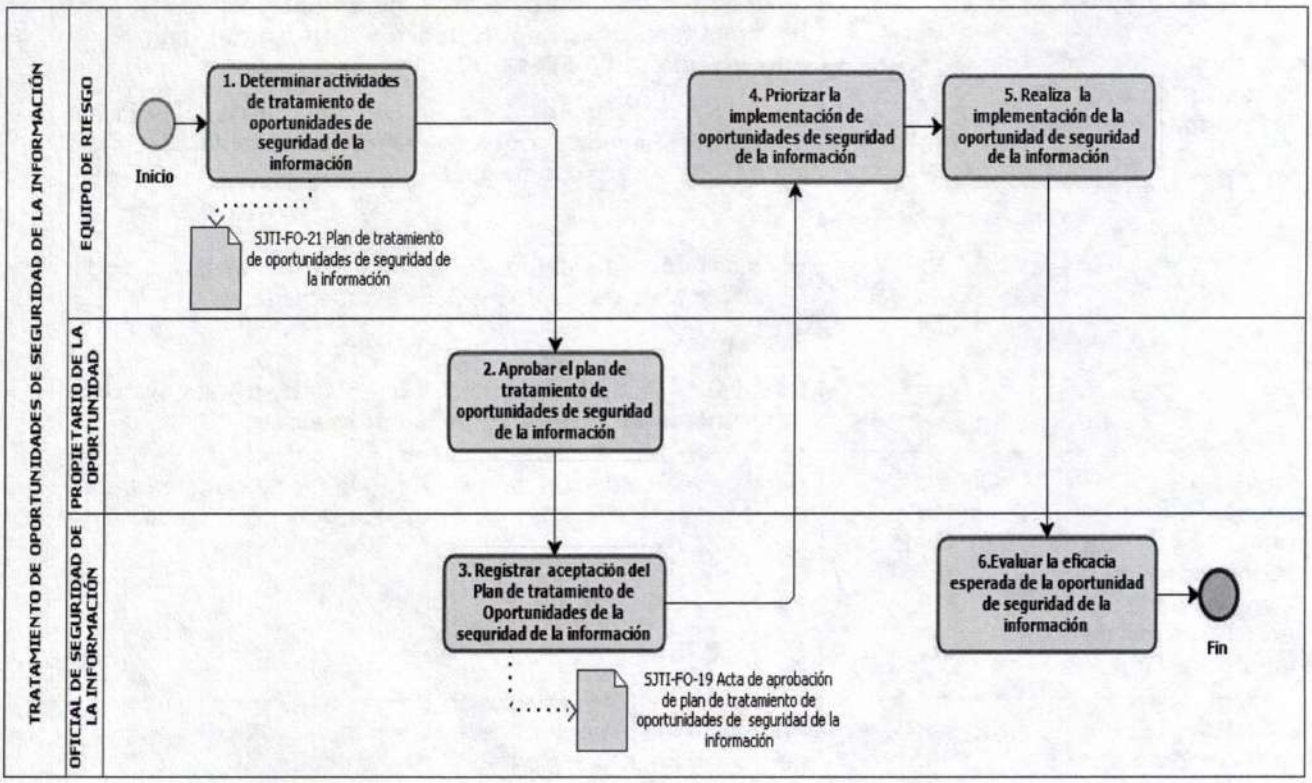
Actividad	Responsable	Descripción de las actividades
3. Determinar la probabilidad de ocurrencia de la oportunidad de seguridad de la información	Equipo de Riesgo	Determina la probabilidad de ocurrencia de la oportunidad de seguridad de la información, considerando los criterios de clasificación establecidos en el **Anexo N° 6.1: Determinación de la probabilidad de la ocurrencia de la oportunidad de seguridad de la información.**
4. Determinar el impacto de la oportunidad de seguridad de la información	Equipo de Riesgo	Determina el impacto de la oportunidad asociado al beneficio que obtendría con su implementación, considerando los criterios establecidos en el **Anexo N° 6.2: Determinación del impacto de la oportunidad de seguridad de la información.**
5. Determinar nivel de oportunidad de seguridad de la información	Equipo de Riesgo	Determina el nivel de oportunidad de seguridad de la información en base al impacto y a la probabilidad. Las oportunidades de seguridad de la información considerados con el nivel de **Relevante (rango 10 – 15)** pasaran a tratamiento.
6. Realiza la valoración de la oportunidad de seguridad de la información	Equipo de Riesgo	Realiza la valoración de la oportunidad de seguridad de la información identificado en la actividad 5. La valoración de la oportunidad de seguridad de la información se determina de las siguientes opciones de tratamiento: - **Explotar** - **Compartir** - **No Implementar** La descripción de las opciones de tratamiento se considera en el **Anexo N° 6.5: Opciones de Tratamiento de la oportunidad de seguridad de la información.**

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° W. Balbín SJTI

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° L. Espinal SJTI

8.5. TRATAMIENTO DE OPORTUNIDADES DE SEGURIDAD DE LA INFORMACIÓN

8.5.1. FLUJOGRAMA



8.5.2. DESCRIPCIÓN

Actividad	Responsable	Descripción de las actividades
1. **Determinar actividades de tratamiento de oportunidad de seguridad de la información**	Equipo de Riesgo	Determina las actividades a realizar para el tratamiento de las oportunidades de seguridad de la información, a través del formato de **Plan de tratamiento de oportunidades de seguridad de la información (SJTI-FO-21).** Asimismo, se registran los siguientes datos: - **Responsable**, quien se encargará de realizar la implementación de la oportunidad de seguridad de la información. - **Recursos**, personal que intervendrá en la implementación de la oportunidad de seguridad de la información. - **Presupuesto**, recurso financiero que costará la implementación de la oportunidad de seguridad de la información. - **Fecha inicio y fin**, que tomará realizar la implementación de la oportunidad de seguridad de la información. **Registro:** **SJTI-FO-21 Plan de tratamiento de oportunidades de seguridad de la información.**

Actividad	Responsable	Descripción de las actividades
2. Aprobar el plan de tratamiento de oportunidades de seguridad de la información	Propietario de la Oportunidad	Aprueba el plan de tratamiento de oportunidad de seguridad de la información, a través del **Acta de aprobación del plan de tratamiento de oportunidades de seguridad de la información (SJTI-FO-19).** Para dicha actividad el Oficial de Seguridad de la Información realizará las coordinaciones con el responsable del proceso y el propietario de la oportunidad. **Nota:** El Oficial de Seguridad de la Información mantendrá custodia de los registros de la información documentada. **Registros:** **SJTI-FO-19 Acta de aprobación del plan de tratamiento de oportunidad de seguridad de la información.**
3. Registrar aceptación del plan de tratamiento de oportunidades de seguridad de la información	Oficial de Seguridad de la Información	Registra la aceptación del plan de tratamiento de oportunidad de seguridad de la información aprobado por el propietario de la oportunidad.
4. Priorizar la implementación de oportunidades de seguridad de la información	Equipo de Riesgo	Prioriza la implementación de las oportunidades de seguridad de la información planteada y aprobada en el acta de aprobación del plan de tratamiento de oportunidad de seguridad de la información.
5. Realizar la implementación de la oportunidad de seguridad de la información	Equipo de Riesgo	Realiza la implementación de las oportunidades de seguridad de la información, asimismo, define el estado de la implementación y mide el porcentaje de avance de la implementación.
6. Evaluar la eficacia esperada de la oportunidad de seguridad de la información	Oficial de Seguridad de la Información	Evalúa la eficacia esperada de la oportunidad de seguridad de la información implementada.

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° W. Balbín SJTI

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° L. Espinal SJTI

IX. ANEXOS

9.1. Anexo N° 01: SJTI-FO-16 Inventario de activos de información y clasificación de la información.

9.1.1. Anexo N° 1.1: Lista general de activos de información.
9.1.2. Anexo Nº 1.2: Aspecto de seguridad de la información.
9.1.3. Anexo N° 1.3: Criticidad de activos de información.
9.1.4. Anexo Nº 1.4: Clasificación de la información.

9.2. Anexo Nº 02: SJTI-FO-17 Valoración de riesgos de seguridad de la información

9.2.1. Anexo Nº 2.1: Aspectos de Seguridad de la información.
9.2.2. Anexo Nº 2.2: Valor CID.
9.2.3. Anexo Nº 2.3: Determinación de la probabilidad de ocurrencia de riesgos de seguridad de la información.
9.2.4. Anexo Nº 2.4: Matriz de probabilidad e impacto.
9.2.5. Anexo Nº 2.5: Nivel de riesgo de seguridad de la información.
9.2.6. Anexo N° 2.6: Opciones de tratamiento de riesgos de seguridad de la información.

9.3. Anexo Nº 03: SJTI-FO-18 Plan de tratamiento de riesgos de seguridad de la información.
9.4. Anexo Nº 04: SJTI-FO-14 Acta de aprobación del plan de tratamiento de riesgos de seguridad de la información y aceptación de riesgos residuales.
9.5. Anexo Nº 05: SJTI-FO-11 Declaración de aplicabilidad.
9.6. Anexo N° 06: SJTI-FO-20 Valoración de oportunidades de seguridad de la información.

9.6.1. Anexo N° 6.1. Determinación de la probabilidad de ocurrencia de la oportunidad
9.6.2. Anexo N° 6.2. Determinación del impacto de la oportunidad
9.6.3. Anexo N° 6.3. Matriz de probabilidad e impacto
9.6.4. Anexo N° 6.4. Nivel de Oportunidad
9.6.5. Anexo N° 6.5. Opciones de tratamiento de la oportunidad de seguridad de la información.

9.7. Anexo N° 07: SJTI-FO-21 Plan de tratamiento de oportunidades de seguridad de la información.
9.8. Anexo N° 08: SJTI-FO-19 Acta de aprobación del plan de tratamiento de oportunidad de seguridad de la información.

X. CUADRO DE CONTROL DE CAMBIOS

VERSIÓN ANTERIOR	CAMBIOS	CARGO DE QUIEN MODIFICÓ
-	-	-

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° W. Balbín SJTI

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° L. Espinal SJTI

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° W. Balbín SJTI

ANEXO Nº 01:
SJTI-FO-16 INVENTARIO DE ACTIVOS DE INFORMACIÓN Y CLASIFICACIÓN DE LA INFORMACIÓN

servir HERRAMIENTA DEL PERÚ QUE CRECE	FORMATO	Código:	SJTI-FO-16
	INVENTARIO DE ACTIVOS DE INFORMACIÓN Y CLASIFICACIÓN DE INFORMACIÓN	Versión:	01
		Página:	1 de 1

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° L. Espinal SJTI

N°	CÓDIGO DEL ACTIVO	FECHA DE REGISTRO DEL INVENTARIO	PROCESO	TIPO DE ACTIVO	CATEGORIA DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	PROPIETARIO	UBICACIÓN		ASPECTOS DE SEGURIDAD			CRITICIDAD DEL ACTIVO	CLASIFICACIÓN DE LA INFORMACIÓN
									FISICA / LOGICA	ESPECIFICA	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD		

ANEXO Nº 1.1:
LISTA GENERAL DE ACTIVOS DE INFORMACIÓN

La identificación del activo de información se realiza a través de la siguiente lista.

TIPO	CATEGORIA
INFORMACIÓN	Información-Documento electrónico
	Información-Documento en papel
SOFTWARE	Software comercial o herramientas, utilitarios
	Software desarrollado por terceros
	Software desarrollado internamente
	Software de administración de Base de Datos
	Software - Otros
HARDWARE	Equipo de procesamiento
	Equipo virtual de cómputo
	Equipo de comunicación
	Equipo de almacenamiento
	Equipo de protección
	Sistemas de seguridad
	Otros Equipos
PERSONAS	Responsables de tomar decisiones (Directores, Sub Directores, Jefes, entre otros)
	Otros trabajadores
SERVICIOS	Procesamiento y comunicaciones
	Generales
	Otros servicios
INSTALACIONES	Sala de Servidores, Centro de Datos, Ambientes de Producción

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° W. Balbín SJTI

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° L. Espinal SJTI

ANEXO Nº 1.2:
ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN

Los aspectos de seguridad referente al activo de información se determinan de acuerdo a la siguiente escala:

ASPECTOS DE SEGURIDAD	VALOR	CLASIFICACIÓN	DEFINICIÓN
CONFIDENCIALIDAD (C)	3	ALTA	Información que sólo puede conocida o modificada por personal expresamente autorizado, controlado y debidamente identificado.
	2	MEDIA	Información que sólo puede ser conocida o modificada por personal de las áreas usuarias que la utilizan y modificada sólo por personas autorizadas e individualizadas.
	1	BAJA	Es la información que puede ser divulgada al público en general, pero que sólo puede ser modificada por personas autorizadas.
INTEGRIDAD (I)	3	ALTA	Información que, se encuentra definida por una disposición legal u obligación contractual para no ser modificada o es política de SERVIR.
	2	MEDIA	Información puede ser modificado por disposición legal o con autorización de nivel gerencial.
	1	BAJA	Información que, puede ser modificado por el propietario del mismo.
DISPONIBILIDAD (D)	3	ALTA	Información indispensable para la continuidad de SERVIR, no puede faltar por un período prolongado de tiempo o en horarios críticos.
	2	MEDIA	Información necesaria para la continuidad de SERVIR, pero existen canales alternativos para contrarrestar una pérdida de disponibilidad en un tiempo razonable.
	1	BAJA	Información que si no está disponible no compromete procesos operativos importantes

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° W. Balbín SJTI

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° L. Espinal SJTI

ANEXO Nº 1.3:
CRITICIDAD DEL ACTIVO

La criticidad del activo se determina de acuerdo a la siguiente escala:

CRITICIDAD DEL ACTIVO	CRITERIOS
NO SIGNIFICATIVO	Es cuando en el CID los valores son todos 1
MENOR	Es cuando en el CID al menos tiene un valor 2
MODERADO	Es cuando en el CID tiene dos valores 2
CRÍTICO	Es cuando en el CID al menos tiene un valor 3
MUY CRÍTICO	Es cuando en el CID tiene dos o tres valores 3

ANEXO Nº 1.4:
CLASIFICACIÓN DE LA INFORMACIÓN

La clasificación de la información se determina de acuerdo a la siguiente escala:

CRITERIOS DE LA VALORACIÓN	ATRIBUTOS
CONFIDENCIAL	Activos de información cuyo contenido no debe ser divulgado ni distribuido a personas que no sean autorizadas y cuya difusión genere un impacto importante en SERVIR entre ellas: pérdida económica, sanción legal o pérdida de imagen institucional.
INTERNA	Activos de información cuyo contenido sólo debe ser de uso y divulgación para el personal interno de SERVIR.
PÚBLICA	Información no sensible de acceso público y que su divulgación no genere impacto en SERVIR.

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° W. Balbín SJTI

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° L. Espinal SJTI

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° W. Balbin SJTI

ANEXO Nº 02:
SJTI-FO-17 VALORACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° L. Espinal SJTI

	FORMATO	Código	SJTI-FO-17
servir HERRAMIENTA DEL PERÚ QUE CRECE	VALORACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	Versión	1
		Página	1 de 1

PROCESO	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	AMENAZA	VULNERABILIDAD	NOMBRE DEL RIESGO	CÓDIGO DEL RIESGO	PROPIETARIO DEL RIESGO	CONTROLES EXISTENTES	EFECTIVIDAD	ASPECTOS DE SEGURIDAD				CONTROLES EXISTENTES	RIESGO EFECTIVO			VALORACIÓN
										C	I	D	VALOR CID		IMPACTO	PROBABILIDAD	NIVEL DE RIESGO	OPCIONES DE TRATAMIENTO

ANEXO Nº 2.1:
ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN

ASPECTOS DE SEGURIDAD	VALOR	CLASIFICACIÓN	DEFINICIÓN
CONFIDENCIALIDAD (C)	3	ALTA	Información que sólo puede conocida o modificada por personal expresamente autorizado, controlado y debidamente identificado.
	2	MEDIA	Información que sólo puede ser conocida o modificada por personal de las áreas usuarias que la utilizan y modificada sólo por personas autorizadas e individualizadas.
	1	BAJA	Es la información que puede ser divulgada al público en general, pero que sólo puede ser modificada por personas autorizadas.
INTEGRIDAD (I)	3	ALTA	Información que, se encuentra definida por una disposición legal u obligación contractual para no ser modificada o es política de SERVIR.
	2	MEDIA	Información puede ser modificado por disposición legal o con autorización de nivel gerencial.
	1	BAJA	Información que, puede ser modificado por el propietario del mismo.
DISPONIBILIDAD (D)	3	ALTA	Información indispensable para la continuidad de SERVIR, no puede faltar por un período prolongado de tiempo o en horarios críticos.
	2	MEDIA	Información necesaria para la continuidad de SERVIR, pero existen canales alternativos para contrarrestar una pérdida de disponibilidad en un tiempo razonable.
	1	BAJA	Información que si no está disponible no compromete procesos operativos importantes

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° W. Balbín SJTI

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° L. Espinal SJTI

ANEXO Nº 2.2:
VALOR CID

ASPECTO DE SEGURIDAD			NIVEL DE IMPACTO	DESCRIPCIÓN
C	I	D		
3	3	3	**ALTA (3)**	Afecta considerablemente la confidencialidad y/o la integridad y/o la disponibilidad de la información de SERVIR, pudiendo ocasionar la paralización del proceso.
3	3	2		
3	2	3		
2	3	3		
3	3	1		
3	1	3		
1	3	3		
3	2	2	**MEDIA (2)**	Afecta moderadamente la confidencialidad y/o la integridad y/o la disponibilidad de la información SERVIR, pudiendo ocasionar retrasos en el desarrollo del proceso.
2	3	2		
2	2	3		
3	2	1		
3	1	2		
2	3	1		
2	1	3		
1	3	2		
1	2	3		
3	1	1		
1	3	1		
1	1	3		
2	2	2		
2	2	1		
2	1	2		
1	2	2		
2	1	1	**BAJA (1)**	Afecta ligeramente la confidencialidad y/o la integridad y/o la disponibilidad de la información SERVIR o al desarrollo del proceso.
1	2	1		
1	1	2		
1	1	1		

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° W. Balbín SJTI

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° L. Espinal SJTI

ANEXO Nº 2.3:
DETERMINACIÓN DE LA PROBABILIDAD DE OCURRENCIA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

VALOR	CLASIFICACIÓN	DEFINICIÓN	OCURRENCIA	FRECUENCIA
1	CASI NULA	El evento puede ocurrir bajo circunstancias excepcionales.	No se presentó en los últimos años.	5% ≤ de frecuencia
2	BAJA	El evento puede ocurrir alguna vez.	Al menos 1 vez en los últimos 2 años.	[5% - 10%] > de frecuencia
3	MEDIA	El evento puede ocurrir en algún momento del año.	Por lo menos 1 vez al año.	[10% - 20%] > de frecuencia
4	MODERADA	El evento probablemente ocurrirá con cierta periodicidad.	Por lo menos 1 vez cada trimestre.	[20% - 30%] > de frecuencia
5	ALTA	Se espera que el evento ocurra con mayor regularidad.	Por lo menos 1 vez al mes.	30% ≥ de frecuencia

ANEXO Nº 2.4:
MATRIZ DE PROBABILIDAD E IMPACTO

RIESGO = PROBABILIDAD X IMPACTO

			PROBABILIDAD				
			CASI NULA	BAJA	MEDIA	MODERADA	ALTA
			1	2	3	4	5
IMPACTO	BAJA	1	TOLERABLE	TOLERABLE	TOLERABLE	TOLERABLE	TOLERABLE
			1	2	3	4	5
	MEDIA	2	TOLERABLE	TOLERABLE	MODERADO	MODERADO	INTOLERABLE
			2	4	6	8	10
	ALTA	3	TOLERABLE	MODERADO	MODERADO	INTOLERABLE	INTOLERABLE
			3	6	9	12	15

ANEXO Nº 2.5:
NIVEL DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN

NIVEL DE RIESGO	MEDIDA DE CONTROL
INTOLERABLE (10 – 15)	Se deben establecer nuevos controles y/o estrategias para controlar el riesgo, en el corto plazo.
MODERADO (6 – 9)	Los servicios pueden proceder de manera regular; sin embargo, se podrían establecer nuevos controles y/o estrategias a largo plazo.
TOLERABLE (1 – 5)	Los servicios pueden proveerse sin controles adicionales. Considerar todos los costos/beneficios que se pueden obtener. No es necesario definir nuevas estrategias.

ANEXO Nº 2.6:

OPCIONES DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

OPCIONES DE TRATAMIENTO	DESCRIPCIÓN
ACEPTAR	En los casos, en que bajo determinadas circunstancias no se encuentran controles para reducir el riesgo, o el costo de implantar el control es mayor que las consecuencias del riesgo, o el riesgo resulta de nivel bajo o casi nula, es posible que la decisión de aceptar el riesgo y vivir con las consecuencias sea la más adecuada.
REDUCIR	Para todos aquellos riesgos donde la opción de reducirlos se ha tomado, se deben implementar controles apropiados para poder reducirlos al nivel que se haya definido como aceptable.
COMPARTIR	Compartir el riesgo es una opción cuando para SERVIR es difícil reducir o controlar el riesgo a un nivel aceptable.
EVITAR	La opción de evitar el riesgo, describe cualquier acción a cambiar actividades, o la manera de desempeñar una actividad en particular, para así evitar la presencia del riesgo.

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° W. Baldín SJTI

ANEXO Nº 03:
SJTI-FO-18 PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

	FORMATO	Código:	SJTI-FO-18
servir HERRAMIENTA DEL PERÚ QUE CRECE	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	Versión:	02
		Página:	1 de 1

CONTROL REFERENCIA ISO 27001	ACTIVIDAD A REALIZAR	RESPONSABLE DE IMPLEMENTAR	ORGANO Y/O UNIDAD ORGANICA RESPONSABLE DE IMPLEMENTAR	FECHA DE INICIO DE LA IMPL.	FECHA FIN DE LA IMPL.	ESTADO	% AVANCE	RIESGO RESIDUAL ESPERADO							RIESGO RESIDUAL REAL								
								EFECTIVIDAD CONTROL	ASPECTOS DE SEGURIDAD			PROBABILIDAD	IMPACTO	RIESGO RESIDUAL	FECHA DE MEDICIÓN RESIDUAL	EFECTIVIDAD DEL CONTROL	ASPETOS DE SEGURIDAD			PROBABILIDAD	IMPACTO	REISGOS RESIDUAL REAL
									CONF.	INTE.	DISP.						CONF.	INTE.	DISP.			

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° Espinal SJTI

ANEXO 04:
SJTI-FO-14 ACTA DE APROBACIÓN DE PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y RIESGOS RESIDUALES

Órgano / Unidad Orgánica: _____

Proceso: _____

Fecha: _____

El Propietario de Riesgos de SERVIR, declara:

- Comprendemos y aprobamos el Plan de Tratamiento de Riesgos de Seguridad de la Información y, por tanto, nos comprometemos a la implementación.
- Que la aceptación de los riesgos es una decisión tomada con entera responsabilidad, en forma totalmente voluntaria y sin presiones.
- Reconocemos que la implementación de los controles para el tratamiento de riesgo es un proceso que reducirá la probabilidad o el impacto de los riesgos, por lo que su ejecución no hace que SERVIR sea vulnerable frente a los riesgos residuales.
- Aceptamos los riesgos residuales, producto de la implementación de los controles, decisión tomada con entera responsabilidad y en forma voluntaria.
- También entendemos que la aceptación de estos riesgos residuales y sus responsabilidades expirará en un año a partir de la fecha de firma de este documento, dado que tendrán que ser evaluados en una nueva gestión de riesgos, para el próximo periodo de operación del Sistema de Gestión de Seguridad de la Información.

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° W. Balbín SJTI

N°	CÓDIGO DE RIESGO (4)	NOMBRE DEL RIESGO (5)	NIVEL DE RIESGO (6)
1			
2			
3			

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° L. Espinal SJTI

_____

NOMBRE Y FIRMA DEL PROPIETARIO DEL RIESGO

ANEXO Nº 05:
SJTI-FO-11 DECLARACIÓN DE APLICABILIDAD

CLÁUSULA N°	OBJETIVOS DE CONTROL	CONTROL	APLICA SI/NO	JUSTIFICACIÓN DE LA INCLUSIÓN O EXCLUSIÓN	DOCUMENTO RELACIONADO
A.5	**POLÍTICAS DE SEGURIDAD DE INFORMACIÓN**				
	A.5.1 Dirección de Gestión para la Seguridad de Información	A.5.1.1 Políticas de seguridad de información			
		A.5.1.2 Revisión de las políticas de seguridad de información			

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° W. Balbin SJTI

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° Espinal SJTI

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° W. Balbín SJTI

ANEXO Nº 06:
SJTI-FO-20 VALORACIÓN DE OPORTUNIDADES DE SEGURIDAD DE LA INFORMACIÓN

	FORMATO	Código:	SJTI-FO-20
servir HERRAMIENTA DEL PERÚ QUE CRECE	VALORACIÓN DE OPORTUNIDADES DE SEGURIDAD DE LA INFORMACIÓN	Versión:	01
		Página:	1 de 1

IDENTIFICACION DE OPORTUNIDADES								ANALISIS DE OPORTUNIDADES					VALORACION DE OPORTUNIDADES
FECHA DE IDENTIFICACIÓN	PROCESO	FUENTE DE OPORTUNIDAD	CÓDIGO DE OPORTUNIDAD	OPORTUNIDAD	BENEFICIOS	FORTALEZA	DUEÑO DE OPORTUNIDAD	PROBABILIDAD	IMPACTO		NIVEL DE OPORTUNIDAD	NIVEL DE OPORTUNIDAD	MEDIDAS DE TRATAMIENTO

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° L. Regina SJTI

ANEXO Nº 6.1:
DETERMINACIÓN DE LA PROBABILIDAD DE OCURRENCIA DE LA OPORTUNIDAD DE SEGURIDAD DE LA INFORMACIÓN

VALOR	CLASIFICACIÓN	OCURRENCIA
1	CASI NULA	Sera difícil que se presente
2	BAJA	Se presenta en pocas ocasiones
3	MEDIA	Se presenta en algunas ocasiones
4	MODERADA	Mayormente está presente
5	ALTA	Siempre está presente

ANEXO Nº 6.2:
DETERMINACIÓN EL IMPACTO DE LA OPORTUNIDAD DE SEGURIDAD DE LA INFORMACIÓN

VALOR	CLASIFICACIÓN	DEFINICIÓN
1	BAJA	Su aprovechamiento beneficia ligeramente a la entidad o al desarrollo del proceso.
2	MEDIA	Su aprovechamiento beneficia moderadamente a la entidad o al desarrollo del proceso
3	ALTA	Su aprovechamiento beneficia considerablemente a la entidad o al desarrollo del proceso.

ANEXO Nº 6.3:
MATRIZ DE PROBABILIDAD E IMPACTO

OPORTUNIDAD = PROBABILIDAD X IMPACTO

			PROBABILIDAD				
			CASI NULA	BAJA	MEDIA	MODERADA	ALTA
			1	2	3	4	5
IMPACTO	BAJA	1	NO RELEVANTE	NO RELEVANTE	NO RELEVANTE	NO RELEVANTE	POCO REVELVANTE
			1	2	3	4	5
	MEDIA	2	NO RELEVANTE	NO RELEVANTE	POCO REVELVANTE	POCO REVELVANTE	REVELVANTE
			2	4	6	8	10
	ALTA	3	NO RELEVANTE	POCO REVELVANTE	POCO REVELVANTE	REVELVANTE	REVELVANTE
			3	6	9	12	15

ANEXO Nº 6.4:
NIVEL DE OPORTUNIDAD DE SEGURIDAD DE LA INFORMACIÓN

NIVEL DE OPORTUNIDAD	MEDIDA DE CONTROL
RELEVANTE (10 – 15)	Recomendable tomar la oportunidad
POCO RELEVANTE (5 – 9)	Es recomendable evaluar si se toma la oportunidad presentada
NO RELEVANTE (1 – 4)	Es recomendable no tomar en ese momento la oportunidad presentada, pudiendo tomar a largo plazo

ANEXO Nº 6.5:
OPCIONES DE TRATAMIENTO DE LA OPORTUNIDAD DE SEGURIDAD DE LA INFORMACIÓN

ESTRATEGIA	DESCRIPCIÓN
EXPLOTAR	Aumenta la posibilidad de la oportunidad, potenciándola.
COMPARTIR	Compartir un riesgo positivo con terceros aumenta la capacidad que salga adelante.
NO IMPLEMENTAR	Aceptar que viene una oportunidad, cuando se presente veremos cómo abordarla. Por ahora no representa un beneficio para la organización.

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° W. Balbín SJTI

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° L. Espinal SJTI

ANEXO Nº 07:

SJTI-FO-21 PLAN DE TRATAMIENTO DE OPORTUNIDADES DE SEGURIDAD DE LA INFORMACIÓN

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° W. Balbín SJTI

servir HERRAMIENTA DEL PERÚ QUE CRECE	FORMATO	Código:	SJTI-FO-21
	VALORACIÓN DE OPORTUNIDADES DE SEGURIDAD DE LA INFORMACIÓN	Versión:	01
		Página:	1 de 1

PLAN DE TRATAMIENTO DE OPORTUNIDADES DE SEGURIDAD DE LA INFORMACIÓN										
ACTIVIDADES	RESPONSABLES	RECURSOS	PRESUPUESTO	FECHA INICIO	FECHA FIN	APROBADO POR	PRIORIZACIÓN	IMPLEMENTACIÓN		EFICACIA ESPERADA
								ESTADO	% AVANCE	

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° L. Espinal SJTI

ANEXO Nº 08:

SJTI-FO-19 ACTA DE APROBACIÓN DEL PLAN DE TRATAMIENTO DE OPORTUNIDAD DE SEGURIDAD DE LA INFORMACIÓN.

Órgano / Unidad Orgánica: _____

Proceso: _____

Fecha: _____

El Propietario de la Oportunidad de SERVIR, declara:

- Comprendemos y aprobamos el Plan de Tratamiento de la Oportunidad de Seguridad de la Información y, por tanto, nos comprometemos.
- Que la aceptación de las oportunidades es una decisión tomada con entera responsabilidad, en forma totalmente voluntaria, sin presiones y en forma voluntaria.
- Reconocemos que la implementación de los controles para el tratamiento de las oportunidades es un proceso que incrementará la probabilidad de los beneficios y fortalezas a SERVIR.
- También entendemos que la aceptación de estas oportunidades y sus responsabilidades expirará en un año a partir de la fecha de firma de este documento, dado que tendrán que ser evaluados en una nueva gestión de riesgos y oportunidades, para el próximo periodo de operación del Sistema de Gestión de Seguridad de la Información.

N°	CÓDIGO DE LA OPORTUNIDAD	NOMBRE DE LA OPORTUNIDAD	NIVEL DE OPORTUNIDAD
1			
2			
3			

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° W. Balbín SJTI

_____

NOMBRE Y FIRMA DEL PROPIETARIO DE LA OPORTUNIDAD

AUTORIDAD NACIONAL DEL SERVICIO CIVIL V°B° L. Espinal SJTI