



PERÚ

Instituto Nacional de Radio
y Televisión del PerúTV Perú
Radio Nacional
Radio La Crónica

RESOLUCIÓN DE PRESIDENCIA EJECUTIVA N° 106 -2018/IRTP

Lima, 16 NOV 2018



VISTO: El Memorando N° 068-2018-OIE/IRTP y el Memorando N° 332-2018-OIE/IRTP de la Oficina de Informática y Estadística; y,

CONSIDERANDO:

Que, mediante Decreto Legislativo N° 829 se crea el Instituto Nacional de Radio y Televisión del Perú (en adelante IRTP) que tiene por finalidad ejecutar actividades y acciones a nivel nacional de difusión de contenidos educativos, informativos, culturales y de esparcimiento, para lo cual, tiene a su cargo la operación de los medios de radiodifusión sonora y por televisión de propiedad del Estado, asumiendo la titularidad de las frecuencias correspondientes;

Que, mediante Resolución Ministerial N° 004-2016-PCM, de fecha 08 de enero de 2016, 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 2° Edición", en todas las entidades integrantes del Sistema Nacional de Informática, con la finalidad de coadyuvar con la infraestructura de Gobierno Electrónico, por considerar la seguridad de la información como un componente crucial para dicho objetivo;

Que, a través de Resolución de Presidencia Ejecutiva N° 051-2018/IRTP, de fecha 14 de junio de 2018, se conformó el Comité de Seguridad de la Información del IRTP, el mismo que con Actas de Aprobación N° 001-2018 y N° 002-2018, acordó elevar a la Alta Dirección para su aprobación, las propuestas de los siguientes documentos: "Plan de Implementación del Sistema de Gestión de Seguridad de la Información", "Alcance del Sistema de Gestión de Seguridad de la Información", "Políticas y Objetivos de Seguridad de la Información", "Roles y Responsabilidades del Sistema de Gestión de Seguridad de la Información", los mismos que fueran presentadas por el Oficial de Seguridad de la Información designado mediante Resolución de Presidencia Ejecutiva N° 068-2018/IRTP;

Que, el numeral 5.2 de la Norma Técnica Peruana dispone que la Alta Dirección debe establecer una política de seguridad de la información que sea apropiada al propósito de la organización, la cual incluya objetivos de seguridad de la información o proporcione el marco de referencia para fijar los mismos, así como, los compromisos de satisfacer requisitos aplicables relacionados a la seguridad de la información, y de mejora continua del sistema de gestión de seguridad de la información, y, que la citada política debe estar disponible como información documentada, comunicada dentro de la organización y disponible a las partes interesadas, según sea apropiado;

Que, asimismo, el numeral 5.3 de la Norma Técnica Peruana establece que la Alta Dirección debe asegurar que las responsabilidades y la autoridad para los roles relevantes a la seguridad de la información estén asignadas y comunicadas, debiendo establecer la responsabilidad y autoridad para garantizar que el sistema de seguridad de la información este conforme a los requisitos de la Norma Técnica Peruana antes citada, y reportar sobre el desempeño del Sistema de Gestión de Seguridad de la Información a la Alta Dirección;



PERÚ

Instituto Nacional de Radio
y Televisión del Perú

TV Perú
Radio Nacional
Radio La Crónica



Que, el numeral 6.2 de la Norma Técnica Peruana dispone que la organización debe planificar la forma de lograr los objetivos de la seguridad de la información, considerando para ello, los siguientes aspectos: acciones, recursos, responsables, plazos y forma de evaluación de los resultados;

Que, mediante el Memorando N° 332-2018-OIE/IRTP, la Oficina de Informática y Estadística sustenta la necesidad de aprobar, con eficacia anticipada, los documentos denominados: "Plan de Implementación del Sistema de Gestión de Seguridad de la Información", "Alcance del Sistema de Gestión de Seguridad de la Información", "Políticas y Objetivos de Seguridad de la Información", "Roles y Responsabilidades del Sistema de Gestión de Seguridad de la Información", de conformidad con lo dispuesto por los artículos 7 y 17 del Texto único Ordenado de la Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N° 00-2018-MC;

Que, de conformidad con lo dispuesto por la Resolución N° 004-2016-PCM, el Texto Único Ordenado de la Ley N° 27444, "Ley del Procedimiento Administrativo General", aprobado por Decreto Supremo N° 006-2017-JUS; y, en uso de las facultades conferidas por el Reglamento de Organización y Funciones del IRTP, aprobado mediante Decreto Supremo N° 056-2001-ED y modificado por Decreto Supremo N° 006-2018-MC;

SE RESUELVE:

Artículo 1°. - Aprobar el "Plan de Implementación del Sistema de Gestión de Seguridad de la Información", con eficacia anticipada al 15 de agosto de 2018, el mismo que en anexo forma parte integrante de la presente Resolución.

Artículo 2°. - Aprobar los documentos denominados "Alcance del Sistema de Gestión de Seguridad de la Información", "Políticas y Objetivos de Seguridad de la Información", "Roles y Responsabilidades del Sistema de Gestión de Seguridad de la Información", con eficacia anticipada al 27 de agosto de 2018, los mismos que en anexo forman parte integrante de la presente Resolución.

Artículo 3°. - Disponer que el Oficial de Seguridad de la Información realice las coordinaciones y acciones necesarias para el cumplimiento de los documentos aprobados mediante la presente Resolución.

Regístrese, comuníquese y cúmplase;

HUGO COYA HONORES
Presidente Ejecutivo
I.R.T.P.





Instituto Nacional de Radio y Televisión del Perú

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

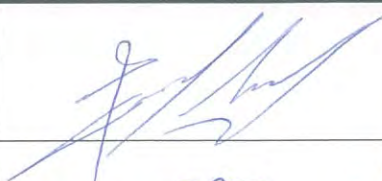
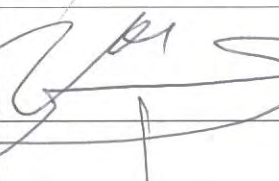
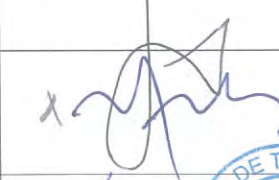
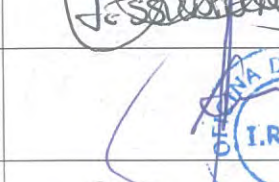
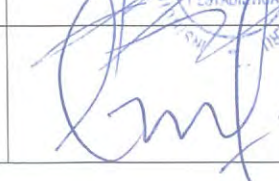
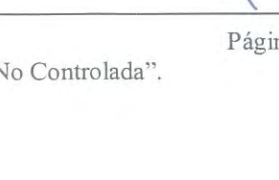
SGSI-PLA-18-001



"Esta es una copia no controlada, se advierte al lector que su contenido puede ser objeto de modificaciones posteriores a la fecha de elaboración sin que se le pueda informar directamente de tales cambios. En ese caso, antes de tomar decisiones basadas en el contenido del presente documento, verifique que la copia sigue vigente."



IRTP	PLAN	CÓDIGO: SGSI-PLA-18-001
	Plan de Implementación del SGSI	VERSIÓN: 01

ETAPA	RESPONSABLE	VISTO BUENO / SELLO
Elaborado por: 13/08/18	Oficial de Seguridad de la Información	
Revisado por: 14/08/18	Gerente de Administración y Finanzas	
	Gerente de Televisión	
	Gerente de Prensa	
	Gerente Técnico	
	Gerente de Radio	
	Gerente de Comercialización	
	Gerente de Teleeducación	
	Director de la Oficina General de Planificación y Desarrollo	
	Jefe de la Oficina de Filiales	
	Director de la Oficina General de Asesoría Legal	
Aprobado por: 15/08/18	Jefe de la Oficina de Informática y Estadística	
	Titular de la Entidad	



IRTP	PLAN	CÓDIGO: SGSI-PLA-18-001
	Plan de Implementación del SGSI	VERSIÓN: 01

I. OBJETO

Definir el Plan de Implementación del Sistema de Gestión de Seguridad de la Información (SGSI) que permita identificar las vulnerabilidades y amenazas que ponen en riesgo la confidencialidad, integridad y disponibilidad de la información en los procesos misionales del Instituto Nacional de Radio y Televisión del Perú.

II. AMBITO DE APLICACIÓN

Comprende a todos los colaboradores del Instituto Nacional de Radio y Televisión del Perú, que forman parte del alcance o que se encuentran involucrados directamente en el proceso de Implementación del Sistema de Gestión de Seguridad de la Información.

III. BASE NORMATIVA

- 3.1 Resolución Ministerial N° 004-2016-PCM que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2da Edición"; en todas las entidades integrantes del Sistema Nacional de Informática.
- 3.2 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.
- 3.3 Decreto Supremo N° 016-2017-PCM que aprueba la Estrategia Nacional de Datos Abiertos Gubernamentales del Perú 2017-2021.
- 3.4 Ley N° 27806 – Ley de Transparencia y Acceso a la Información Pública y su reglamento.
- 3.5 Ley N° 29733 – Ley de Protección de Datos Personales, su reglamento y su directiva.
- 3.6 Ley N° 27815 – Ley del Código de Ética de la Función Pública.

IRTP	PLAN	CÓDIGO: SGSI-PLA-18-001
	Plan de Implementación del SGSI	VERSIÓN: 01

IV. SIGLAS Y ABREVIATURAS

- **ISO:** International Organization for Standardization (Organización Internacional de Normalización)
- **IEC:** International Electrotechnical Commission (Comisión Electrotécnica Internacional)
- **IRTP:** Instituto Nacional de Radio y Televisión del Perú.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.

V. DEFINICIONES

- **Activo:** Es cualquier recurso que genere valor para la institución. Dentro de los activos informáticos se encuentran las bases de datos, sistemas operativos, software, aplicaciones, códigos fuentes, dispositivos de redes y comunicaciones, etc.
- **Activos de Información:** Recursos humanos, tecnológicos, administrativos, etc., que participan en el tratamiento de la información.
- **Amenaza:** Causa potencial de un incidente no deseado, el cual puede causar daño a un sistema u organización.
- **Autenticidad:** Permite que la información transmitida o intercambiada provenga de fuentes auténticas y de quienes dicen ser que son.
- **Cifrado:** Es una forma de tratamiento que permite que la información electrónica sea leíble y modificada sólo por las personas autorizadas, asegurando así su confidencialidad e integridad respectivamente.
- **Colaboradores:** Trabajadores del IRTP sujetos al régimen laboral del Decreto Legislativo N° 728 y Decreto Legislativo N° 1057, así como, proveedores de servicios bajo los alcances del Código Civil y Ley N° 30225, Ley de Contrataciones del Estado.
- **Comité de Gestión de Seguridad de la Información:** Es el comité que tiene por función gestionar la seguridad de la información en la institución. Se conforma por Resolución de Presidencia Ejecutiva.
- **Confidencialidad:** Garantizar que la información es accesible sólo para aquellos autorizados a tener acceso.
- **Control:** Son medidas que se implementan con el fin de mitigar los riesgos.
- **Disponibilidad:** Permite que la información esté disponible solamente a los usuarios autorizados en el tiempo que lo requieran.

IRTP	PLAN	CÓDIGO: SGSI-PLA-18-001
	Plan de Implementación del SGSI	VERSIÓN: 01

- **Impacto:** La consecuencia o consecuencias de un evento, expresado ya sea en términos cualitativos o cuantitativos.
- **Información:** Activo importante de toda organización, expresado mediante un conjunto de datos que se encuentra en diferentes medios lógicos y físicos, y en diferentes estados (almacenado, en transmisión y en procesamiento).
- **Integridad:** Permite que la información sea correcta y que no haya sido alterada por usuarios, entidades o procesos no autorizados.
- **No Repudio:** Garantizar que la transferencia de un mensaje ha sido enviado y recibido por entidades que son quienes dicen ser.
- **Oficial de Seguridad de la Información:** Responsable de coordinar la implementación del Sistema de Gestión de Seguridad de la Información en la Entidad.
- **Procedimiento:** Forma específica para llevar a cabo una actividad o proceso.
- **Proceso:** Conjunto de actividades, tareas y procedimientos organizados y repetibles que producen un resultado esperado.
- **Proyecto:** Actividad temporal para producir un producto, servicio, o resultado, que es único. Es temporal dado que tiene un comienzo y un fin definido, y por lo tanto tiene un alcance y recursos definidos.
- **Registro:** Documento que presenta resultados o proporciona evidencia de actividades desempeñadas.
- **Revisión:** Actividad que se realiza para determinar la idoneidad, la adecuación y la eficacia del tema estudiado para conseguir los objetivos establecidos.
- **Riesgo:** Probabilidad de que un evento, suceso o acontecimiento perjudicial o beneficioso, degrade o aumente el grado de la confidencialidad, integridad y disponibilidad de la información.
- **Sistema de Gestión de Seguridad de la Información:** Es un conjunto de procesos soportados por políticas, procedimientos, responsabilidades, actividades, programas, medios tecnológicos con la finalidad de mantener la confidencialidad, integridad y disponibilidad de la información en concordancia de los requisitos de negocio, regulaciones, leyes y partes contractuales.
- **Sistema de Información:** Es todo sistema soportado por una infraestructura tecnológica informática.
- **Vulnerabilidad:** Debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.

IRTTP	PLAN	CÓDIGO: SGSI-PLA-18-001
	Plan de Implementación del SGSI	VERSIÓN: 01

VI. IMPLEMENTACIÓN DEL SGSI

6.1 ENTREGABLES DEL SGSI

En la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), se elaborarán los siguientes documentos, ello sin excluir otros documentos que se consideren necesarios durante el proceso.

N°	NTP ISO/IEC 27001:2014	ENTREGABLE	DESCRIPCIÓN
1	Clausula 7.5 Información Documentada.	Procedimiento de Gestión Documental y Registro	Documento que establece los lineamientos para la elaboración, aprobación y actualización de los documentos y registros relacionados al SGSI.
2	Clausula 4.1 Comprender la organización y su contexto.	Análisis del Contexto de la Organización	Documento que establece el contexto interno y externo del IRTTP. Para asegurar que el SGSI este alineado con los objetivos institucionales y cumpla con las obligaciones legales y normativas relacionadas a la seguridad de la información.
3	Clausula 4.2 Comprender las necesidades y expectativas de las partes interesadas.	Necesidades y Expectativas de las Partes Interesadas	Documento que establece las partes interesadas (internas y externas), en la implementación del SGSI.
4	Clausula 4.3 Determinar el alcance del SGSI.	Alcance del SGSI	Documento que define en forma precisa la ubicación y los recursos que forman parte del alcance de la implementación del SGSI.
5	Clausula 5.1 Liderazgo y compromiso. Cláusula 5.2 Política.	Políticas y Objetivos de Seguridad de la Información	Documento clave que establece el marco normativo para gestionar la seguridad de la información en el IRTTP.

La reproducción total o parcial de este documento, constituye una "Copia No Controlada"

Página 7 de 12



IRTP	PLAN	CÓDIGO: SGSI-PLA-18-001
	Plan de Implementación del SGSI	VERSIÓN: 01

6	Clausula 5.3 Roles, Autoridad y Responsabilidades organizacionales.	Roles y Responsabilidades del SGSI	Documento que define la estructura organizacional para la dirección, gestión y operación de la seguridad de la información en el IRTP.
7	Clausula 6.1 Acciones para tratar los riesgos y las oportunidades.	Metodología de Gestión de Riesgos	Documento que describe los métodos y parámetros para la identificación, análisis evaluación y tratamiento de los riesgos de seguridad de la información.
8	Clausula 6.1.2 Valoración del riesgo de seguridad de la información.	Matriz de Análisis y Evaluación de Riesgos	Matriz resultante del análisis y evaluación de los riesgos de seguridad de la información en el IRTP.
9		Informe de Gestión de Riesgos de Seguridad de la Información	Documento que incluye la información generada en el proceso de gestión de riesgos.
10	Clausula 6.1.3 Tratamiento de Riesgos de seguridad de la información.	Declaración de Aplicabilidad	Documento que contiene los controles del Anexo A de la NTP ISO/IEC 27001:2014 y justifica la inclusión o exclusión de su implementación.
11		Plan de Tratamiento de Riesgos de Seguridad de la Información	Documento que especifica un plan de trabajo priorizado de los controles que deben implementarse como resultado de la gestión de riesgos.
12	Clausula 7.3 Concientización.	Plan de Concientización, Capacitación y Evaluación en Seguridad de la Información.	Documento que especifica un plan de formación en seguridad de la información.
13	Clausula 7.4 Comunicación	Plan de Operación y Comunicaciones del SGSI	Documento que describe como se efectuarán las comunicaciones internas y externas en relación al Sistema de Gestión de Seguridad de la Información.



IRTP	PLAN	CÓDIGO: SGSI-PLA-18-001
	Plan de Implementación del SGSI	VERSIÓN: 01

14	Clausula 9.1 Monitoreo, Medición, Análisis y Evaluación.	Informe de Medición y Monitoreo del SGSI	Documento que describe el proceso para evaluar el cumplimiento de los indicadores establecidos para el SGSI.
15	Clausula 9.2 Auditoria Interna.	Procedimiento de Auditoria Interna del SGSI	Documento que describe como se realizará la Auditoria Interna, se redactará el programa de Auditoria Interna y se informará el Resultado de la misma.
16	Clausula 9.3 Revisión por la Gerencia.	Procedimiento de Revisión por la Dirección del SGSI	Documento que describe como se realizará la revisión por parte del Titular de la Entidad para asegurar la eficacia y efectividad del SGSI.
17	Clausula 10.1 No conformidades y Acción Correctiva.	Plan de Acciones Correctivas del SGSI	Documento que describe el proceso de implementación de las acciones correctivas.

6.2 ORGANIZACIÓN DEL PLAN DE IMPLEMENTACIÓN

La implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en el IRTP, se llevará a cabo por un equipo organizado de la siguiente forma:

- **Responsable del Proyecto:** El rol recae sobre el Presidente Ejecutivo del IRTP.
- **Coordinador del Proyecto:** Rol desempeñado por el Oficial de Seguridad de la Información, responsable de la elaboración de los entregables durante las etapas del SGSI. Quien gestionará las acciones necesarias para la implementación del SGSI y coordinará con los Gerentes/ Jefes de los procesos que forman parte del alcance del SGSI.
- **Equipo de Trabajo:** Conformado por el Comité de Gestión de Seguridad de la Información. Tomará decisiones durante la implementación del SGSI.

La reproducción total o parcial de este documento, constituye una "Copia No Controlada"



PLAN	CÓDIGO: SGSI-PLA-18-001
	VERSIÓN: 01

6.3 RIESGOS DEL PLAN DE IMPLEMENTACIÓN DEL SGSI

La Implementación del Sistema de Gestión de Seguridad de la Información (SGSI), contribuye al cambio de la cultura organizacional en todos los niveles de la Institución.

A continuación, se detallan algunos riesgos que se puedan presentar durante la implementación del SGSI, y como estos serían abordados.

RIESGOS	ACCIONES DE MITIGACIÓN
Falta de compromiso del equipo del proyecto	El titular de la entidad aprobará la Política y Objetivos de Seguridad de la información que incluyan el compromiso de toda la institución para la correcta implementación del Sistema de Gestión de Seguridad de la Información (SGSI).
Falta de recursos asignados al proyecto, implementación de controles de costo elevado.	La implementación exitosa de controles puede verse afectada por recorte presupuestal de los recursos asignados por el Estado, el proyecto debe contemplar medidas a corto y largo plazo en el caso se requiera una inversión considerable.
Ampliación de los plazos de presentación de los entregables	El Oficial de Seguridad de la Información supervisará que todas las actividades sean realizadas dentro de los plazos definidos y solicitará a tiempo la intervención del titular de la entidad en el Comité de Gestión de Seguridad de la Información, de ser necesario.
Cambios en los integrantes del equipo del proyecto	Por temas de gestión administrativa se puede ver afectado el equipo de trabajo. Por ello el Comité de Gestión de Seguridad de la Información se creó en base a los puestos y no en base a los colaboradores directamente.



IRTP	PLAN	CÓDIGO: SGSI-PLA-18-001
	Plan de Implementación del SGSI	VERSIÓN: 01

6.4 ACCIONES PREVIAS Y PERMANENTES

Para el Inicio de la Implementación del SGSI

- Compromiso del Titular de la Entidad: Con la finalidad de respaldar al equipo y las medidas aprobadas en el Comité de Gestión de Seguridad de la Información.
- Análisis Inicial de Brechas de Seguridad de la Información: Con la finalidad de determinar el status actual de la institución en relación al cumplimiento de la NTP ISO/IEC 27001:2014.

Durante la Implementación del SGSI

- Auditoria Informática: Que permitirá establecer indicadores de cumplimiento y de gestión.
- Fortalecimiento de capacidades: De los colaboradores claves en temas de seguridad de la información.

6.5 METODOLOGÍA

Para la implementación del SGSI se empleará la metodología PDCA (Plan, Do, Check, Act), también llamada ciclo de DEMING, que impulsa el mejoramiento continuo de procesos y consiste en los siguientes pasos:

- PLAN (Planear): Reconocer una oportunidad y planificar el cambio.
- DO (Hacer): Probar el cambio.
- CHECK (Verificar): Revisar la prueba, analizar los resultados e identificar lo aprendido.
- ACT (Actuar): Tomar acción basada en las lecciones aprendidas. Si el cambio fue exitoso, incorporar lo aprendido, de lo contrario intentar un plan diferente.

6.6 CRONOGRAMA DE ACTIVIDADES

En la siguiente tabla se detalla el cronograma de actividades del Plan de Implementación del Sistema de Gestión de Seguridad de la Información (SGSI).

CRONOGRAMA DE IMPLEMENTACIÓN DEL SGSI

ACTIVIDAD	INICIO DEL PLAN	DURACIÓN DEL PLAN	AÑO		2018					2019		
			MES	DURACIÓN	Agosto	Setiembre	Octubre	Noviembre	Diciembre	Enero	Febrero	Marzo
					1	2	3	4	5	6	7	8
INICIO DEL PROYECTO												
FASE I- ESTABLECER EL SGSI (PLANIFICAR)	1	4										
Procedimiento de Gestión Documental y Registro	1	1										
Análisis del Contexto de la Organización	1	1										
Necesidades y Expectativas de las Partes Interesadas	1	1										
Alcance del SGSI	1	1										
Política y Objetivos de Seguridad de la Información	1	1										
Roles y Responsabilidades del SGSI	1	1										
Metodología de Gestión de Riesgos	1	1										
Matriz de Análisis y Evaluación de Riesgos	2	3										
Informe de Gestión de Riesgos de Seguridad de la Información	4	1										
Declaración de Aplicabilidad	4	1										
FASE II- IMPLEMENTAR Y OPERAR EL SGSI (HACER)	4	3										
Políticas específicas de seguridad de información	4	2										
Plan de Tratamiento de Riesgos de Seguridad de la Información	5	1										
Plan de Concientización, Capacitación y Evaluación en Seguridad de la Información	6	1										
Plan de Operación y Comunicaciones del SGSI	6	1										
FASE III- MONITOREAR Y REVISAR EL SGSI (VERIFICAR)	6	3										
Informe de Medición y Monitoreo del SGSI	6	2										
Procedimiento de Auditoría Interna del SGSI	7	1										
Procedimiento de Revisión por la Dirección del SGSI	8	1										
FASE IV- MANTENER Y MEJORAR EL SGSI (ACTUAR)	8	1										
Plan de Acciones Correctivas del SGSI	8	1										
CIERRE DEL PROYECTO	0	1										



Instituto Nacional de Radio y Televisión del Perú

ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

SGSI-DOC-18-003G



"Esta es una copia no controlada, se advierte al lector que su contenido puede ser objeto de modificaciones posteriores a la fecha de elaboración sin que se le pueda informar directamente de tales cambios. En ese caso, antes de tomar decisiones basadas en el contenido del presente documento, verifique que la copia sigue vigente."

IRTP	DOCUMENTO	CÓDIGO: SGSI-DOC-18-003
	Alcance del SGSI	VERSIÓN: 01

ETAPA	RESPONSABLE	VISTO BUENO / SELLO
Elaborado por: 20/08/18	Oficial de Seguridad de la Información	
Revisado por: 24/08/18	Gerente de Administración y Finanzas	
	Gerente de Televisión	
	Gerente de Prensa	
	Gerente Técnico	
	Gerente de Radio	
	Gerente de Comercialización	
	Gerente de Teleeducación	
	Director de la Oficina General de Planificación y Desarrollo	
	Jefe de la Oficina de Filiales	
	Director de la Oficina General de Asesoría Legal	
	Jefe de la Oficina de Informática y Estadística	
Aprobado por: 27/08/18	Titular de la Entidad	

IRTTP	DOCUMENTO	CÓDIGO: SGSI-DOC-18-003
	Alcance del SGSI	VERSIÓN: 01

HOJA DE CONTROL DE CAMBIOS

Versión	Fecha	Justificación (1)	Texto Modificado (2)	Responsable (3)
01		Versión Inicial		

Notas:

- 1) Justificación de la nueva versión del documento puede darse en los casos de: Modificación, Actualización o Reformulación.
- 2) Señalar el numeral, sección y párrafo exacto en donde se ha modificado.
- 3) Señalar quién ha solicitado el cambio.

La reproducción total o parcial de este documento, constituye una "Copia No Controlada".

Página 3 de 8



IRTP	DOCUMENTO	CÓDIGO: SGSI-DOC-18-003
	Alcance del SGSI	VERSIÓN: 01

I. OBJETO

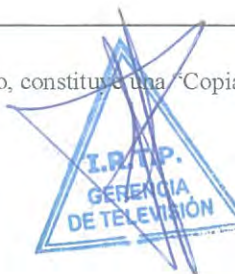
Establecer el alcance del Sistema de Gestión de Seguridad de la Información, tomando en cuenta el contexto y las partes interesadas.

II. AMBITO DE APLICACIÓN

El presente documento se aplica a todo el Sistema de Gestión de Seguridad de la Información. Los usuarios de este documento son todas las partes interesadas e involucrados en la implementación del Sistema de Gestión.

III. BASE NORMATIVA

- 3.1 Resolución Ministerial N° 004-2016-PCM que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2da Edición"; en todas las entidades integrantes del Sistema Nacional de Informática.
- 3.2 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.
- 3.3 Decreto Supremo N° 016-2017-PCM que aprueba la Estrategia Nacional de Datos Abiertos Gubernamentales del Perú 2017-2021.
- 3.4 Ley N° 27806 – Ley de Transparencia y Acceso a la Información Pública y su reglamento.
- 3.5 Ley N° 29733 – Ley de Protección de Datos Personales, su reglamento y su directiva.
- 3.6 Ley N° 27815 – Ley del Código de Ética de la Función Pública.



IRTP	DOCUMENTO	CÓDIGO: SGSI-DOC-18-003
	Alcance del SGSI	VERSIÓN: 01

IV. SIGLAS Y ABREVIATURAS

- **ISO:** International Organization for Standardization (Organización Internacional de Normalización)
- **IEC:** International Electrotechnical Commission (Comisión Electrotécnica Internacional)
- **IRTP:** Instituto Nacional de Radio y Televisión del Perú.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.

V. DEFINICIONES

- **Activo:** Es cualquier recurso que genere valor para la institución. Dentro de los activos informáticos se encuentran las bases de datos, sistemas operativos, software, aplicaciones, códigos fuentes, dispositivos de redes y comunicaciones, etc.
- **Activos de Información:** Recursos humanos, tecnológicos, administrativos, etc., que participan en el tratamiento de la información.
- **Amenaza:** Causa potencial de un incidente no deseado, el cual puede causar daño a un sistema u organización.
- **Autenticidad:** Permite que la información transmitida o intercambiada provenga de fuentes auténticas y de quienes dicen ser que son.
- **Cifrado:** Es una forma de tratamiento que permite que la información electrónica sea leíble y modificada sólo por las personas autorizadas, asegurando así su confidencialidad e integridad respectivamente.
- **Colaboradores:** Trabajadores del IRTP sujetos al régimen laboral del Decreto Legislativo N° 728 y Decreto Legislativo N° 1057, así como, proveedores de servicios bajo los alcances del Código Civil y Ley N° 30225, Ley de Contrataciones del Estado.
- **Comité de Gestión de Seguridad de la Información:** Es el comité que tiene por función gestionar la seguridad de la información en la institución. Se conforma por Resolución de Presidencia Ejecutiva.
- **Confidencialidad:** Garantizar que la información es accesible sólo para aquellos autorizados a tener acceso.
- **Control:** Son medidas que se implementan con el fin de mitigar los riesgos.
- **Disponibilidad:** Permite que la información esté disponible solamente a los usuarios autorizados en el tiempo que lo requieran.

La reproducción total o parcial de este documento, constituye una "Copia No Controlada".

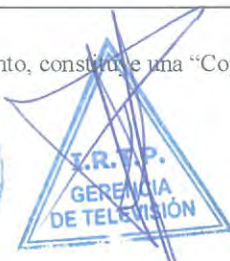
Página 5 de 8



	DOCUMENTO	CÓDIGO: SGSI-DOC-18-003
	Alcance del SGSI	VERSIÓN: 01



- **Impacto:** La consecuencia o consecuencias de un evento, expresado ya sea en términos cualitativos o cuantitativos.
- **Información:** Activo importante de toda organización, expresado mediante un conjunto de datos que se encuentra en diferentes medios lógicos y físicos, y en diferentes estados (almacenado, en transmisión y en procesamiento).
- **Integridad:** Permite que la información sea correcta y que no haya sido alterada por usuarios, entidades o procesos no autorizados.
- **No Repudio:** Garantizar que la transferencia de un mensaje ha sido enviado y recibido por entidades que son quienes dicen ser.
- **Oficial de Seguridad de la Información:** Responsable de coordinar la implementación del Sistema de Gestión de Seguridad de la Información en la Entidad.
- **Procedimiento:** Forma específica para llevar a cabo una actividad o proceso.
- **Proceso:** Conjunto de actividades, tareas y procedimientos organizados y repetibles que producen un resultado esperado.
- **Proyecto:** Actividad temporal para producir un producto, servicio, o resultado, que es único. Es temporal dado que tiene un comienzo y un fin definido, y por lo tanto tiene un alcance y recursos definidos.
- **Registro:** Documento que presenta resultados o proporciona evidencia de actividades desempeñadas.
- **Revisión:** Actividad que se realiza para determinar la idoneidad, la adecuación y la eficacia del tema estudiado para conseguir los objetivos establecidos.
- **Riesgo:** Probabilidad de que un evento, suceso o acontecimiento perjudicial o beneficioso, degrade o aumente el grado de la confidencialidad, integridad y disponibilidad de la información.
- **Sistema de Gestión de Seguridad de la Información:** Es un conjunto de procesos soportados por políticas, procedimientos, responsabilidades, actividades, programas, medios tecnológicos con la finalidad de mantener la confidencialidad, integridad y disponibilidad de la información en concordancia de los requisitos de negocio, regulaciones, leyes y partes contractuales.
- **Sistema de Información:** Es todo sistema soportado por una infraestructura tecnológica informática.
- **Vulnerabilidad:** Debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.



IRTP	DOCUMENTO	CÓDIGO: SGSI-DOC-18-003
	Alcance del SGSI	VERSIÓN: 01

VI. DEFINICIÓN DEL ALCANCE DEL SGSI

El Sistema de Gestión de Seguridad de la Información (SGSI) implementado en el Instituto Nacional de Radio y Televisión del Perú (IRTP), en cumplimiento de la norma ISO/IEC 27001:2014, tiene como alcance el siguiente proceso:

“Verificación y control de la información necesaria para la producción y difusión de contenidos audiovisuales culturales orientados a los niños, niñas y juventud peruana (Canal IPe)”.

En el alcance del SGSI se asegurará la confidencialidad, disponibilidad e integridad de la información que está comprendida en el proceso citado. Adicional a ello el IRTP incrementará los niveles de confianza de la ciudadanía con el aumento del valor del contenido audiovisual y mejora de la imagen de la institución con el respaldo del cumplimiento de la norma ISO/IEC 27001:2014.

VII. UBICACIÓN FÍSICA/ LOCALIZACIÓN

El Alcance del Sistema de Gestión de Seguridad de la Información a implementar en el Instituto Nacional de Radio y Televisión del Perú (IRTP) será desarrollado en las siguientes localizaciones:

	Departamento	Sede	Dirección
1	Urb. Santa Beatriz Lima - Perú	Edificio TV Perú	Av. José Gálvez # 1040
2	Urb. Santa Beatriz Lima - Perú	Edificio Administrativo	Av. Paseo de la República N°1110

VIII. RECURSOS

Contempla a los activos de información (recursos humanos, recursos tecnológicos, infraestructura física) que participan en el proceso de “Verificación y control de la información necesaria para la producción y difusión de contenidos audiovisuales culturales orientados a los niños, niñas y juventud peruana”.

La reproducción total o parcial de este documento, constituye una “Copia No Controlada”.

Página 7 de 8

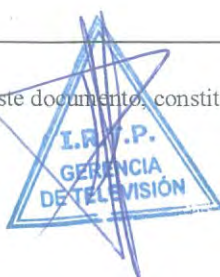


IRTP	DOCUMENTO	CÓDIGO: SGSI-DOC-18-003
	Alcance del SGSI	VERSIÓN: 01

IX. PARTES INTERESADAS RELEVANTES PARA EL SGSI Y SUS REQUERIMIENTOS

Las siguientes son las partes interesadas identificadas frente al SGSI y sus requerimientos:

Parte Interesada	Requerimientos
Entes de Control	Cumplimiento de la legislación y regulación vigentes
Titular de la Entidad	Contar con altos estándares en seguridad de la información.
Colaboradores	Obtener un enfoque integrado de seguridad de la información en los procesos internos de la institución.
Proveedores	Tener un proceso ágil y estandarizado en cuanto a bienes y servicios.
Ciudadanos	Obtener un servicio de calidad en términos de seguridad de la información.





Instituto Nacional de Radio y Televisión del Perú

POLÍTICA Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

SGSI-POL-18-001



"Esta es una copia no controlada, se advierte al lector que su contenido puede ser objeto de modificaciones posteriores a la fecha de elaboración sin que se le pueda informar directamente de tales cambios. En ese caso, antes de tomar decisiones basadas en el contenido del presente documento, verifique que la copia sigue vigente."

IRTP	POLÍTICA	CÓDIGO: SGSI-POL-18-001
	Política y Objetivos de SI	VERSIÓN: 01

ETAPA	RESPONSABLE	VISTO BUENO / SELLO
Elaborado por: 21/08/18	Oficial de Seguridad de la Información	
Revisado por: 24/08/18	Gerente de Administración y Finanzas	
	Gerente de Televisión	
	Gerente de Prensa	
	Gerente Técnico	
	Gerente de Radio	
	Gerente de Comercialización	
	Gerente de Teleeducación	
	Director de la Oficina General de Planificación y Desarrollo	
	Jefe de la Oficina de Filiales	
	Director de la Oficina General de Asesoría Legal	
	Jefe de la Oficina de Informática y Estadística	
Aprobado por: 24/08/18	Titular de la Entidad	

IRTP	POLÍTICA	CÓDIGO: SGSI-POL-18-001
	Política y Objetivos de SI	VERSIÓN: 01



HOJA DE CONTROL DE CAMBIOS

Versión	Fecha	Justificación (1)	Texto Modificado (2)	Responsable (3)
01		Versión Inicial		

Notas:

- 1) Justificación de la nueva versión del documento puede darse en los casos de: Modificación, Actualización o Reformulación.
- 2) Señalar el numeral, sección y párrafo exacto en donde se ha modificado.
- 3) Señalar quién ha solicitado el cambio.

La reproducción total o parcial de este documento constituye una "Copia No Controlada"

Página 3 de 7





IRTP	POLÍTICA	CÓDIGO: SGSI-POL-18-001
	Política y Objetivos de SI	VERSIÓN: 01



I. OBJETO

Establecer una Política y Objetivos de Seguridad de la Información alineada al propósito y los objetivos estratégicos del Instituto Nacional de Radio y Televisión del Perú, en cumplimiento de la normatividad vigente.



II. AMBITO DE APLICACIÓN

La presente política es de cumplimiento obligatorio para todos los colaboradores del IRTP, indistintamente de su régimen laboral, modalidad de contratación o nivel jerárquico; así como por las personas naturales o jurídicas que prestan servicios o tengan acceso a la información de la institución.

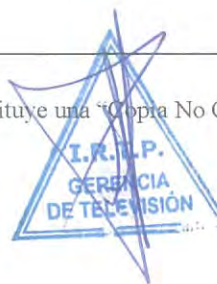


III. BASE NORMATIVA

- 3.1 Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2da Edición"; en todas las entidades integrantes del Sistema Nacional de Informática.
- 3.2 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.
- 3.3 Decreto Supremo N° 016-2017-PCM, que aprueba la Estrategia Nacional de Datos Abiertos Gubernamentales del Perú 2017-2021.
- 3.4 Ley N° 27806 – Ley de Transparencia y Acceso a la Información Pública y su reglamento.
- 3.5 Ley N° 29733 – Ley de Protección de Datos Personales, su reglamento y su directiva.
- 3.6 Ley N° 27815 – Ley del Código de Ética de la Función Pública.



La reproducción total o parcial de este documento, constituye una "Copia No Controlada".



IRTP	POLÍTICA	CÓDIGO: SGSI-POL-18-001
	Política y Objetivos de SI	VERSIÓN: 01

IV. SIGLAS Y ABREVIATURAS

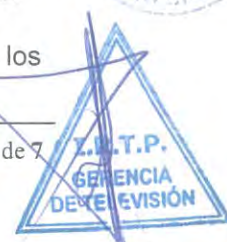
- **ISO:** International Organization for Standardization (Organización Internacional de Normalización)
- **IEC:** International Electrotechnical Commission (Comisión Electrotécnica Internacional)
- **IRTP:** Instituto Nacional de Radio y Televisión del Perú.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.

V. DEFINICIONES

- **Activo:** Es cualquier recurso que genere valor para la institución. Dentro de los activos informáticos se encuentran las bases de datos, sistemas operativos, software, aplicaciones, códigos fuentes, dispositivos de redes y comunicaciones, etc.
- **Activos de Información:** Recursos humanos, tecnológicos, administrativos, etc., que participan en el tratamiento de la información.
- **Amenaza:** Causa potencial de un incidente no deseado, el cual puede causar daño a un sistema u organización.
- **Autenticidad:** Permite que la información transmitida o intercambiada provenga de fuentes auténticas y de quienes dicen ser que son.
- **Cifrado:** Es una forma de tratamiento que permite que la información electrónica sea leíble y modificada sólo por las personas autorizadas, asegurando así su confidencialidad e integridad respectivamente.
- **Colaboradores:** Trabajadores del IRTP sujetos al régimen laboral del Decreto Legislativo N° 728 y Decreto Legislativo N° 1057, así como, proveedores de servicios bajo los alcances del Código Civil y Ley N° 30225, Ley de Contrataciones del Estado.
- **Comité de Gestión de Seguridad de la Información:** Es el comité que tiene por función gestionar la seguridad de la información en la institución. Se conforma por Resolución de Presidencia Ejecutiva.
- **Confidencialidad:** Garantizar que la información es accesible sólo para aquellos autorizados a tener acceso.
- **Control:** Son medidas que se implementan con el fin de mitigar los riesgos.
- **Disponibilidad:** Permite que la información esté disponible solamente a los usuarios autorizados en el tiempo que lo requieran.

La reproducción total o parcial de este documento constituye una "Copia No Controlada"

Página 5 de 7

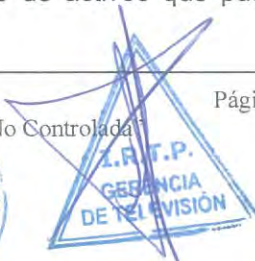




IRTP	POLÍTICA	CÓDIGO: SGSI-POL-18-001
	Política y Objetivos de SI	VERSIÓN: 01

- **Impacto:** La consecuencia o consecuencias de un evento, expresado ya sea en términos cualitativos o cuantitativos.
- **Información:** Activo importante de toda organización, expresado mediante un conjunto de datos que se encuentra en diferentes medios lógicos y físicos, y en diferentes estados (almacenado, en transmisión y en procesamiento).
- **Integridad:** Permite que la información sea correcta y que no haya sido alterada por usuarios, entidades o procesos no autorizados.
- **No Repudio:** Garantizar que la transferencia de un mensaje ha sido enviado y recibido por entidades que son quienes dicen ser.
- **Oficial de Seguridad de la Información:** Responsable de coordinar la implementación del Sistema de Gestión de Seguridad de la Información en la Entidad.
- **Procedimiento:** Forma específica para llevar a cabo una actividad o proceso.
- **Proceso:** Conjunto de actividades, tareas y procedimientos organizados y repetibles que producen un resultado esperado.
- **Proyecto:** Actividad temporal para producir un producto, servicio, o resultado, que es único. Es temporal dado que tiene un comienzo y un fin definido, y por lo tanto tiene un alcance y recursos definidos.
- **Registro:** Documento que presenta resultados o proporciona evidencia de actividades desempeñadas.
- **Revisión:** Actividad que se realiza para determinar la idoneidad, la adecuación y la eficacia del tema estudiado para conseguir los objetivos establecidos.
- **Riesgo:** Probabilidad de que un evento, suceso o acontecimiento perjudicial o beneficioso, degrade o aumente el grado de la confidencialidad, integridad y disponibilidad de la información.
- **Sistema de Gestión de Seguridad de la Información:** Es un conjunto de procesos soportados por políticas, procedimientos, responsabilidades, actividades, programas, medios tecnológicos con la finalidad de mantener la confidencialidad, integridad y disponibilidad de la información en concordancia de los requisitos de negocio, regulaciones, leyes y partes contractuales.
- **Sistema de Información:** Es todo sistema soportado por una infraestructura tecnológica informática.
- **Vulnerabilidad:** Debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.

La reproducción total o parcial de este documento, constituye una Copia No Controlada



IRTP	POLÍTICA	CÓDIGO: SGSI-POL-18-001
	Política y Objetivos de SI	VERSIÓN: 01

VI. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El Instituto Nacional de Radio y Televisión del Perú en su calidad de organismo público encargado de la difusión de contenidos educativos, informativos, culturales y de esparcimiento, se compromete a preservar la información de manera íntegra y disponible a usuarios autorizados, promoviendo a sus administrados una cultura de seguridad acorde con las necesidades de la entidad. Para tal efecto, adoptará estándares internacionales que permitan la continuidad de las operaciones y la mejora continua del SGSI, a fin de ofrecer un servicio de calidad a beneficio de la ciudadanía a través de sus diversas plataformas de comunicación.

VII. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

- Mantener la información íntegra y disponible a usuarios autorizados mediante los mecanismos del Sistema de Gestión de Seguridad de la Información.
- Asegurar la gestión oportuna de los riesgos para reducir los incidentes de seguridad de la información.
- Mejorar el desempeño del Sistema de Gestión de seguridad de la información con el fin de fortalecer la gestión institucional.
- Desarrollar el compromiso y competencias de los colaboradores del IRTP respecto a Seguridad de la Información.

VIII. SANCIONES

En el supuesto que los colaboradores del IRTP incumplan las disposiciones contenidas en la presente política, incurrirán en falta disciplinaria que se imputará y sancionará de acuerdo a lo dispuesto en la Ley N° 27815, Ley del Código de Ética de la Función Pública y la Ley N° 30057, Ley del Servicio Civil.

IX. REVISIONES

La presente política se revisará por lo menos una vez al año, cuando ocurran cambios significativos que afecten al Sistema de Gestión de Seguridad de la Información o cuando el Comité de Gestión de Seguridad de la Información lo vea pertinente para asegurar su conveniencia, adecuación y eficacia continua.

X. DIFUSIÓN

La presente política y objetivos será difundida a todos los colaboradores del IRTP.

La reproducción total o parcial de este documento, constituye una "Copia No Controlada".

Página 7 de 7



Instituto Nacional de Radio y Televisión del Perú

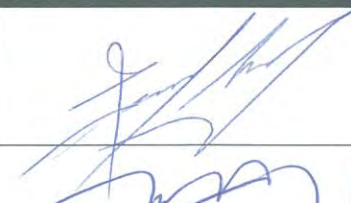
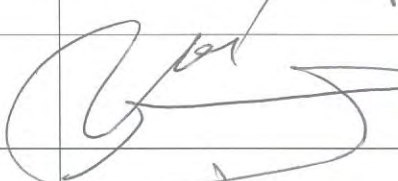
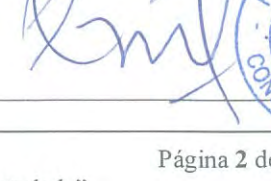
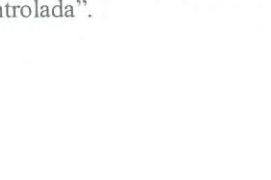
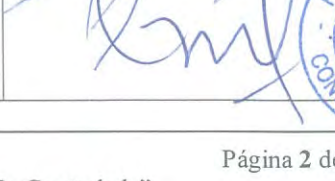
ROLES Y RESPONSABILIDADES DEL SGSI

SGSI-DOC-18-004



"Esta es una copia no controlada, se advierte al lector que su contenido puede ser objeto de modificaciones posteriores a la fecha de elaboración sin que se le pueda informar directamente de tales cambios. En ese caso, antes de tomar decisiones basadas en el contenido del presente documento, verifique que la copia sigue vigente."

IRTTP	DOCUMENTO	CÓDIGO: SGSI-DOC-18-004
	Roles y Responsabilidades del SGSI	VERSIÓN: 01

ETAPA	RESPONSABLE	VISTO BUENO / SELLO
Elaborado por: 22/08/18	Oficial de Seguridad de la Información	
Revisado por: 24/08/18	Gerente de Administración y Finanzas	 
	Gerente de Televisión	 
	Gerente de Prensa	
	Gerente Técnico	 
	Gerente de Radio	 
	Gerente de Comercialización	 
	Gerente de Teleeducación	 
	Director de la Oficina General de Planificación y Desarrollo	 
	Jefe de la Oficina de Filiales	 
	Director de la Oficina General de Asesoría Legal	 
	Jefe de la Oficina de Informática y Estadística	 
Aprobado por: 27/08/18	Titular de la Entidad	 

IRTP	DOCUMENTO	CÓDIGO: SGSI-DOC-18-004
	Roles y Responsabilidades del SGSI	VERSIÓN: 01

HOJA DE CONTROL DE CAMBIOS

Versión	Fecha	Justificación (1)	Texto Modificado (2)	Responsable (3)
01		Versión Inicial		

Notas:

- 1) Justificación de la nueva versión del documento puede darse en los casos de: Modificación, Actualización o Reformulación.
- 2) Señalar el numeral, sección y párrafo exacto en donde se ha modificado.
- 3) Señalar quién ha solicitado el cambio.



IRTP	DOCUMENTO	CÓDIGO: SGSI-DOC-18-004
	Roles y Responsabilidades del SGSI	VERSIÓN: 01

I. OBJETO

Establecer la estructura organizacional para la gestión e implementación del Sistema de Gestión de Seguridad de la Información en el Instituto Nacional de Radio y Televisión del Perú a través de la definición de los principales roles y responsabilidades de los involucrados.



II. AMBITO DE APLICACIÓN

Comprende a todos los colaboradores del Instituto Nacional de Radio y Televisión del Perú, que forman parte del alcance o que se encuentran involucrados directamente en el proceso de Implementación del Sistema de Gestión de Seguridad de la Información.



III. BASE NORMATIVA

- 3.1 Resolución Ministerial N° 004-2016-PCM que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2da Edición"; en todas las entidades integrantes del Sistema Nacional de Informática.
- 3.2 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.
- 3.3 Decreto Supremo N° 016-2017-PCM que aprueba la Estrategia Nacional de Datos Abiertos Gubernamentales del Perú 2017-2021.
- 3.4 Ley N° 27806 – Ley de Transparencia y Acceso a la Información Pública y su reglamento.
- 3.5 Ley N° 29733 – Ley de Protección de Datos Personales, su reglamento y su directiva.
- 3.6 Ley N° 27815 – Ley del Código de Ética de la Función Pública.



IRTP	DOCUMENTO	CÓDIGO: SGSI-DOC-18-004
	Roles y Responsabilidades del SGSI	VERSIÓN: 01

IV. SIGLAS Y ABREVIATURAS

- **ISO:** International Organization for Standardization (Organización Internacional de Normalización)
- **IEC:** International Electrotechnical Commission (Comisión Electrotécnica Internacional)
- **IRTP:** Instituto Nacional de Radio y Televisión del Perú.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.

V. DEFINICIONES

- **Activo:** Es cualquier recurso que genere valor para la institución. Dentro de los activos informáticos se encuentran las bases de datos, sistemas operativos, software, aplicaciones, códigos fuentes, dispositivos de redes y comunicaciones, etc.
- **Activos de Información:** Recursos humanos, tecnológicos, administrativos, etc., que participan en el tratamiento de la información.
- **Amenaza:** Causa potencial de un incidente no deseado, el cual puede causar daño a un sistema u organización.
- **Autenticidad:** Permite que la información transmitida o intercambiada provenga de fuentes auténticas y de quienes dicen ser que son.
- **Cifrado:** Es una forma de tratamiento que permite que la información electrónica sea leíble y modificada sólo por las personas autorizadas, asegurando así su confidencialidad e integridad respectivamente.
- **Colaboradores:** Trabajadores del IRTP sujetos al régimen laboral del Decreto Legislativo N° 728 y Decreto Legislativo N° 1057, así como, proveedores de servicios bajo los alcances del Código Civil y Ley N° 30225, Ley de Contrataciones del Estado.
- **Comité de Gestión de Seguridad de la Información:** Es el comité que tiene por función gestionar la seguridad de la información en la institución. Se conforma por Resolución de Presidencia Ejecutiva.
- **Confidencialidad:** Garantizar que la información es accesible sólo para aquellos autorizados a tener acceso.
- **Control:** Son medidas que se implementan con el fin de mitigar los riesgos.
- **Disponibilidad:** Permite que la información esté disponible solamente a los usuarios autorizados en el tiempo que lo requieran.

La reproducción total o parcial de este documento, constituye una "Copia No Controlada".

Página 5 de 10





IRTP	DOCUMENTO	CÓDIGO: SGSI-DOC-18-004
	Roles y Responsabilidades del SGSI	VERSIÓN: 01

- **Impacto:** La consecuencia o consecuencias de un evento, expresado ya sea en términos cualitativos o cuantitativos.
- **Información:** Activo importante de toda organización, expresado mediante un conjunto de datos que se encuentra en diferentes medios lógicos y físicos, y en diferentes estados (almacenado, en transmisión y en procesamiento).
- **Integridad:** Permite que la información sea correcta y que no haya sido alterada por usuarios, entidades o procesos no autorizados.
- **No Repudio:** Garantizar que la transferencia de un mensaje ha sido enviado y recibido por entidades que son quienes dicen ser.
- **Oficial de Seguridad de la Información:** Responsable de coordinar la implementación del Sistema de Gestión de Seguridad de la Información en la Entidad.
- **Procedimiento:** Forma específica para llevar a cabo una actividad o proceso.
- **Proceso:** Conjunto de actividades, tareas y procedimientos organizados y repetibles que producen un resultado esperado.
- **Proyecto:** Actividad temporal para producir un producto, servicio, o resultado, que es único. Es temporal dado que tiene un comienzo y un fin definido, y por lo tanto tiene un alcance y recursos definidos.
- **Registro:** Documento que presenta resultados o proporciona evidencia de actividades desempeñadas.
- **Revisión:** Actividad que se realiza para determinar la idoneidad, la adecuación y la eficacia del tema estudiado para conseguir los objetivos establecidos.
- **Riesgo:** Probabilidad de que un evento, suceso o acontecimiento perjudicial o beneficioso, degrade o aumente el grado de la confidencialidad, integridad y disponibilidad de la información.
- **Sistema de Gestión de Seguridad de la Información:** Es un conjunto de procesos soportados por políticas, procedimientos, responsabilidades, actividades, programas, medios tecnológicos con la finalidad de mantener la confidencialidad, integridad y disponibilidad de la información en concordancia de los requisitos de negocio, regulaciones, leyes y partes contractuales.
- **Sistema de Información:** Es todo sistema soportado por una infraestructura tecnológica informática.
- **Vulnerabilidad:** Debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.



IRTP	DOCUMENTO	CÓDIGO: SGSI-DOC-18-004
	Roles y Responsabilidades del SGSI	VERSIÓN: 01

VI. ESTRUCTURA ORGANIZACIONAL



En el marco de la gestión de Seguridad de la Información, el Titular de la Entidad define los siguientes roles y responsabilidades entre los diferentes niveles directivos y operativos de la organización:

- Comité de Gestión de Seguridad de la Información
- Oficial de Seguridad de la Información
- Propietarios de la Información
- Custodios de la Información
- Usuarios
- Auditor Líder
- Auditor Interno
- Auditado



VII. ROLES Y RESPONSABILIDADES



7.1

COMITÉ DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El artículo 5A de la Resolución Ministerial N° 004-2016-PCM, incorporado mediante la Resolución Ministerial N° 166-2017-PCM, establece las siguientes responsabilidades a cargo del Comité de Gestión de Seguridad de la información:

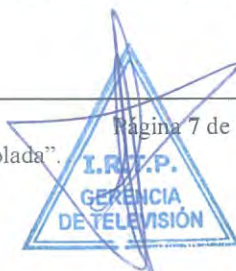
- a) Proponer la política y objetivos de seguridad de la información alineados con el Plan Estratégico Institucional, con la Política Nacional de Gobierno Electrónico y regulación en el ámbito de seguridad de la información.
- b) Promover y gestionar la implementación del Sistema de Gestión de Seguridad de la Información.
- c) Promover la gestión de seguridad de la información en los procesos y cultura organizacional.
- d) Gestionar la asignación del personal y recursos necesarios para la implementación del Sistema de Gestión de Seguridad de la Información.
- e) Difundir la importancia de una efectiva gestión de seguridad de la información a las partes interesadas, en conformidad con los requisitos del Sistema de Gestión de Seguridad de la Información.
- f) Evaluar el desempeño del Sistema de Gestión de Seguridad de la Información.
- g) Otras funciones que se le asigne en el ámbito de su competencia y aquellas concordantes con la materia.



La reproducción total o parcial de este documento, constituye una "Copia No Controlada".



[Handwritten signature]





IRTP	DOCUMENTO	CÓDIGO: SGSI-DOC-18-004
	Roles y Responsabilidades del SGSI	VERSIÓN: 01

7.2 OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

Coordinador del plan de Implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en el Instituto Nacional de Radio y Televisión del Perú (IRTP), tiene como responsabilidades:

- a) Participar en la creación y revisión de las políticas, lineamientos, metodologías, procedimientos y planes referidos a la seguridad de la información.
- b) Supervisar el cumplimiento de las políticas, procedimientos y controles de seguridad de la información.
- c) Coordinar con los propietarios y custodia de la información para la elaboración del inventario de activos de la información y ejecución de la gestión de riesgos.
- d) Informar los resultados de su gestión al Comité de Gestión de Seguridad de la Información.
- e) Dar seguimiento a los incidentes de seguridad de la información, evaluar riesgos y eventuales impactos.
- f) Evaluar, coordinar y monitorear la implementación de los controles relacionados al SGSI.
- g) Supervisar y apoyar en la difusión de los temas de seguridad de la información.
- h) Brindar capacitación en temas de Seguridad de la Información.
- i) Otras funciones relacionadas a la naturaleza de su trabajo.

7.3 PROPIETARIOS DE LA INFORMACIÓN

Son los responsables de la información que se genera y se utiliza en las operaciones de su Unidad Orgánica. Tienen como responsabilidades:

- a) Participar en la identificación de los activos de información y en las actividades de análisis, evaluación y tratamiento de riesgos.
- b) Revisión periódica de la clasificación y etiquetado de la información con el propósito de verificar que cumpla con los requerimientos de la Entidad.
- c) Sugerir y apoyar en la elaboración de lineamientos y procedimientos de seguridad de la información dentro de sus respectivas áreas y procesos.
- d) Revisar periódicamente los niveles de acceso a los sistemas de información a su cargo.
- e) Supervisar y verificar la aplicación de los controles de seguridad con el custodio de la información.



IRTP	DOCUMENTO	CÓDIGO: SGSI-DOC-18-004
	Roles y Responsabilidades del SGSI	VERSIÓN: 01

7.4 CUSTODIOS DE LA INFORMACIÓN



Son los encargados de la administración diaria de la seguridad de los activos de la información y el monitoreo del cumplimiento de las políticas y los controles de seguridad en los activos de información que se encuentran bajo su administración, y tiene como responsabilidades:

- Administrar los controles relevantes a la seguridad de la información, acorde a las medidas de tratamiento de la información especificadas por los propietarios de la información.
- Cumplir con los controles implementados para la protección de los activos de información asignados para su custodia.
- Colaborar en la investigación de los incidentes de seguridad de la información.
- Identificar oportunidades de mejora y comunicarlas al Oficial de Seguridad de la Información.

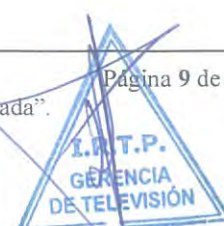


7.5 USUARIOS



Son los colaboradores del Instituto Nacional de Radio y Televisión del Perú (IRTP), indistintamente del régimen laboral, modalidad de contratación o nivel jerárquico; así como por las personas naturales o jurídicas que prestan servicios, quienes utilizan la información en actividades habituales y se encuentran obligados a respetar las normas establecidas por la Institución. Tienen como responsabilidades:

- Cumplir con las políticas, lineamientos y procedimientos de seguridad de la información.
- Mantener la confidencialidad de las contraseñas para el acceso a las aplicaciones, sistemas de información y recursos informáticos.
- Utilizar la información del Instituto Nacional de Radio y Televisión del Perú (IRTP), únicamente para los propósitos autorizados.
- Participar en los entrenamientos, capacitación y programas de sensibilización en temas de seguridad de la información.
- Reportar cualquier incidente, potencial incidente u oportunidades de mejora de seguridad de la información.



**IRTP****DOCUMENTO****CÓDIGO:
SGSI-DOC-18-004****Roles y Responsabilidades del SGSI****VERSIÓN: 01****7.6 AUDITOR LIDER**

Es el encargado de encabezar el equipo de auditores internos. Tiene como responsabilidades:

- a) Convocar y realizar la reunión de apertura de auditoría.
- b) Realizar la reunión de cierre de acuerdo al plan de auditoría.
- c) Planificar y dirigir todas las actividades de la auditoría.
- d) Ser independiente del área o proceso comprendido dentro del alcance de la auditoría, no auditar su propio trabajo.

**7.7 AUDITOR INTERNO**

Es el responsable de preparar y llevar a cabo el proceso de auditoría interna para determinar el grado en el cual el sistema de gestión de seguridad de la información cumple con los requisitos de la Norma Técnica Peruana ISO/IEC 27001:2014. Tiene como responsabilidades:

- a) Revisar la documentación y evidencias de cumplimiento dentro del alcance del SGSI.
- b) Llevar a cabo las reuniones de levantamiento de información con el personal involucrado, para corroborar o extender sus indagaciones.
- c) Mantener imparcialidad, objetividad y ser independiente del área o proceso comprendido dentro del alcance de la auditoría, no auditar su propio trabajo.
- d) Otras funciones en el ámbito de su competencia.

7.8 AUDITADO

Es cualquier colaborador del Instituto Nacional de Radio y Televisión del Perú (IRTP), que se encuentra sujeto a una revisión por parte del equipo de auditores. Tiene como responsabilidad proporcionar al equipo auditor la información necesaria y objetiva para asegurar un proceso de auditoría eficiente y eficaz.

