

PODER JUDICIAL DEL PERÚ
CONSEJO EJECUTIVO

**c) “Procedimiento de Identificación, Análisis y Evaluación de
Riesgos de Seguridad de la Información”**

R.A. N° 109-2016-CE-PJ

**MAYO 2016
LIMA – PERU**



1. OBJETIVO

Establecer una secuencia de actividades para la identificación, análisis y evaluación de los riesgos de seguridad de la información.

2. ALCANCE

Aplica a la evaluación de riesgos de seguridad de la información de los procesos definidos dentro del alcance del SGSI.

3. DEFINICIONES

3.1. **Activo de Información**¹: Todo aquello que tenga valor para la organización.

Tipos:

- Información, tal como una Base de Datos, un reporte, archivo de documentos.
- Software, tal como un programa de computadora
- Físicos, tal como una computadora
- Servicios, tal como courier, mantenimiento de computadoras
- Perfiles de Trabajo de las personas, tales como los puestos de trabajo que desempeñan las personas en sus entornos laborales.

3.2. **Amenaza**: es un evento que potencialmente puede causar daño. Para la identificación de las amenazas se utilizará la tabla de amenazas y vulnerabilidades (ver Anexo 01 - Tabla de Amenazas).

3.3. **Alcance del SGSI**: Determinación del ámbito de aplicación del SGSI en términos de conjuntos de procesos en la institución.

3.4. **Confidencialidad**: Propiedad que determina que la información no esté disponible, ni sea divulgada a personas, entidades o procesos no autorizados.

3.5. **Custodio**: Identifica a la persona o la entidad que tiene la responsabilidad de mantener los niveles de protección adecuados en base a las especificaciones dadas por el propietario.

3.6. **Disponibilidad**: Propiedad de la información de estar disponible y utilizable cuando lo requiera una entidad autorizada.

3.7. **Estimación del Riesgo**: proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

¹ Tener en cuenta el concepto de información del punto 3.10 de este documento.



- 3.8. Identificación de Riesgos:** proceso para encontrar, enumerar y caracterizar los elementos de riesgo.
- 3.9. Impacto:** es la consecuencia de la explotación de una vulnerabilidad por una amenaza debido a la falta o falla de controles, generando pérdida en confidencialidad, integridad y disponibilidad de la información u otros activos.
- 3.10. Información²:** La información es un activo que, al igual que otros activos comerciales importantes, es esencial para el negocio de una organización y por lo tanto necesita ser protegido de forma adecuada. La información puede ser almacenada en muchas formas, incluyendo: forma digital (por ejemplo, archivos de datos almacenados en medios electrónicos u ópticos), forma material (por ejemplo, en el papel), así como la información sin representación (conocimiento que los empleados tienen acerca de los procesos de la institución). La información puede ser transmitida por diversos medios, incluyendo: mensajería, comunicación electrónica o verbal.
- 3.11. Integridad:** Propiedad de salvaguardar la exactitud de la información.
- 3.12. Inventario de Activos:** Es un registro conformado por los activos de información que tienen valor para el Poder Judicial y que están dentro del alcance del SGSI.
- 3.13. Probabilidad:** es la posibilidad de que un evento cualquiera ocurra o no. A mayor probabilidad del evento existe más posibilidad de que ocurra, es decir, existen buenas razones para creer que sucederá.
- 3.14. Propietario del Activo de Información:** Identifica a la persona o la entidad que tiene la responsabilidad gerencial aprobada de controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos.
- 3.15. Riesgo:** es la probabilidad de que una amenaza en particular explote una vulnerabilidad causando un impacto negativo sobre los activos.
- 3.16. SGSI:** Sistema de Gestión de Seguridad de la Información, basado en la ISO/IEC 27001.
- 3.17. Usuarios de alcance del SGSI:** Usuarios de los procesos del alcance de implementación del SGSI.
- 3.18. Vulnerabilidad:** Una Vulnerabilidad es una debilidad que puede ser explotada por una amenaza. Para la identificación de las vulnerabilidades se utilizará la

² Extraído de la ISO 27000 “Tecnologías de la Información – Sistemas de Gestión de Seguridad de la Información – Información General y Vocabulario” – punto 3.2.2

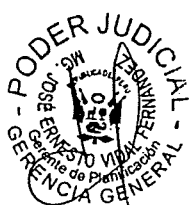
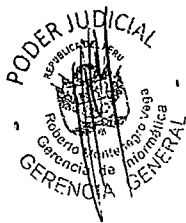
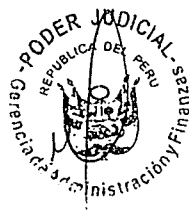
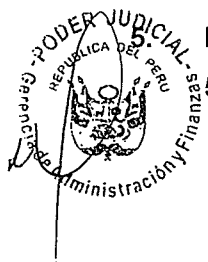




tabla de amenazas y vulnerabilidades (ver Anexo 02 - Tabla de Vulnerabilidades).

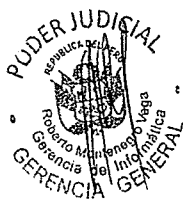
4. DOCUMENTOS A CONSULTAR

- M-01-2016-CGSI-GG-P-PJ Manual del SGSI.
- P-02-2016-CGSI-GG-CE-PJ Procedimiento de Identificación de Activos de Información
- Norma ISO/IEC 27001 en su versión vigente.
- Norma ISO/IEC 27005 en su versión vigente.



RESPONSABILIDADES

- 5.1 Los Propietarios de los Activos de Información deben dar cumplimiento a este procedimiento, promover la participación activa del personal en la identificación, análisis y evaluación de riesgos de seguridad de la información. Los propietarios deberán revisar y dar la conformidad a la matriz de riesgos.
- 5.2 El Comité de Gestión de Seguridad de Información
- Aprobar el resultado de la evaluación de riesgos.
- 5.3 El Oficial de Seguridad de la Información verifica el cumplimiento del presente documento, así como las siguientes actividades:
- Liderar los talleres a desarrollarse para la identificación, análisis y evaluación de riesgos de seguridad de la información.
 - Compilar información remitida por los propietarios relacionada a la identificación, análisis y evaluación de riesgos de seguridad de la información.
 - Presentar a los propietarios de procesos el resultado del análisis de riesgos
 - Presentar al Comité de Gestión de Seguridad de Información el resultado del análisis de riesgos para su aprobación.
- 5.4 Los Usuarios del área del alcance del SGSI deben de dar cumplimiento a este procedimiento, así como también rubricar el formato utilizado como hoja de trabajo dando conformidad a la información brindada.





DESCRIPCIÓN DEL PROCEDIMIENTO

El proceso de Análisis de Riesgos está sujeto a métodos de valorización cualitativos y está orientado a los activos de información, que soportan los procesos del negocio.

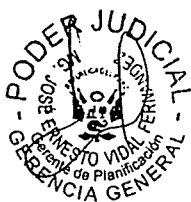
Para el desarrollo del análisis de riesgo nos apoyaremos del P-02-2016-CGSI-GG-CE-PJ Procedimiento de Identificación de Activos de Información, para luego utilizar el formato "Informe de Análisis y Evaluación de Riesgos".

N° de Actividad	UNIDAD ORGÁNICA / RESPONSABLE	ACCIÓN A REALIZAR
1		Identificación de Activos de Información
1.1	Usuarios del área del alcance del SGSI	a. Identifican, clasifican y valorizan los activos de información según lo indicado en el procedimiento P-02-2016-CGSI-GG-CE-PJ Procedimiento de Identificación de Activos de Información y el formato "Procedimiento de Identificación de Activos de Información".
1.2	Usuario del área del alcance del SGSI	a. Realizan el análisis de riesgo a los activos de información cuyo valor sea <u>alto</u> , los mismos que se incluirán en el formato "Informe de Análisis y Evaluación de Riesgos".
2		Desarrollo de talleres para Análisis de Riesgos de Seguridad de la Información
2.1	Oficial de Seguridad de la Información	a. Desarrolla los talleres para brindar información de cómo realizar la identificación de amenazas, vulnerabilidades, valoración de la Confidencialidad, Integridad y Disponibilidad - CID, determinación de impacto, determinación de probabilidad de ocurrencia y determinación del riesgo, tanto a los propietarios de los activos de información de los procesos del alcance del SGSI como a los usuarios que estos designen. Tener en cuenta que el Oficial apoyará tanto a los propietarios de los activos de

N° de Actividad	UNIDAD ORGÁNICA / RESPONSABLE	ACCIÓN A REALIZAR
		información como a los usuarios durante todo el desarrollo de este procedimiento, y toda la información recabada será completada en el formato "Informe de Análisis y Evaluación de Riesgos".
3		Identificación de Amenazas
3.1	Usuario del área del alcance del SGSI	a. Completa las amenazas en base al anexo N° 04 "Tabla de Amenazas", dependiendo del tipo de activo que se esté analizando. Pueden darse una o más amenazas por cada activo.
4		Identificación de Vulnerabilidades
4.1	Usuario del área del alcance del	a. Completa las vulnerabilidades en base al anexo N° 05 "Tabla de Vulnerabilidades", dependiendo del tipo de activo que se esté analizando. Pueden darse una o más vulnerabilidades por cada amenaza identificada.
5		Evaluación del Criterio CID
5.1	Usuario del área del alcance del SGSI	a. Evalúa y completa los valores de Confidencialidad, Integridad y Disponibilidad - CID en base a las siguientes tablas: Anexo N° 06 "Tabla de Valorización de Confidencialidad", Anexo N° 07 "Tabla de Valorización de Integridad", Anexo N° 08 "Tabla de Valorización de Disponibilidad".
6		Determinación del Impacto en la Institución
6.1	Usuario del área del alcance del SGSI	a. Evalúa y determina el impacto en base a los valores del anexo N° 10 "Tabla de Valorización del Impacto". El impacto se obtendrá en forma consecuente con la combinación de los valores del CID indicado en el anexo N° 09 "Tabla de Relación CID e Impacto".



N° de Actividad	UNIDAD ORGÁNICA / RESPONSABLE	ACCIÓN A REALIZAR
7		Determinación la Probabilidad de Ocurrencia
7.1	Usuario del área del alcance del SGSI	a. Evalúa y determina la probabilidad de ocurrencia en base a los valores del anexo N° 11 "Tabla de Probabilidad de Ocurrencia".
8		Determinación el Riesgo
8.1	Usuario del área del alcance del SGSI	a. Determina el nivel de riesgo en base a los valores indicados en el anexo N° 14 "Mapa de Riesgos", cuyos niveles están definidos en el anexo N° 13 "Nivel de Riesgo".
8.2	Usuario del área del alcance del SGSI	a. Asigna un nombre al riesgo generado, se sugiere combinar el nombre de la vulnerabilidad con el de la amenaza.
8.3	Usuario del área del alcance del SGSI	a. Asigna un código al riesgo generado, se sugiere identificarlo con un acrónimo en base al nombre del proceso y una numeración correlativa (por ejemplo RTI-01, de riesgo de tecnologías de la información).
9		Validación de Información del Recibida
9.1	Propietarios de los Activos de Información	a. Valida la información recibida y colectada en el "Informe de Análisis y Evaluación de Riesgos" con los propietarios de activos de información. Tener en cuenta que las hojas de trabajo deben de ser firmadas por los usuarios quienes brindaron la información.
10		Desarrollo de Informe de Análisis de Riesgos
10.1	Oficial de Seguridad de la Información	a. En base a la información recolectada y validada, genera el Informe de Análisis de Riesgos de Seguridad de la Información, el cual servirá como base para desarrollar el Plan de Tratamiento de Riesgos de Seguridad de la Información.





N° de Actividad	UNIDAD ORGÁNICA / RESPONSABLE	ACCIÓN A REALIZAR
11		Revisión y Aprobación del Informe de Análisis de Riesgos
11.1	Comité de Seguridad de la Información	a. Revisa el Informe de Análisis de Riesgos de Seguridad de la Información, el cual consiste en validar que la información del "Informe de Análisis y Evaluación de Riesgos" firmados se vea reflejada en el Informe Final de Análisis de Riesgos de Seguridad de la Información, en caso el "Informe de Análisis y Evaluación de Riesgos" no esté firmado o el inventario no refleje la información del mismo, el Informe no será aprobado y será devuelto al Oficial de Seguridad de la Información para las correcciones necesarias.
12		Desarrollo de Plan de Tratamiento del Riesgo
12.1	Oficial de Seguridad de la Información	a. Propone controles a cada uno de los riesgos identificados pero a partir del nivel especificado en este procedimiento (por ejemplo solo los riesgos de nivel alto y extremo), esto con el fin de darle un tratamiento adecuado (reducir, evitar, trasladar o convivir con el riesgo).
13		Validación de Controles Propuestos
13.1	Propietarios de los Activos de Información	a. Valida los controles propuestos con los propietarios de los activos, ya que estos últimos tendrán la tarea de implementar dichos controles. En caso que los controles sobrepasen los recursos de cualquiera de los propietarios de los activos, se puede plantear las siguientes alternativas: coordinar la implementación de otro control que reduzca el nivel de riesgo a uno de nivel medio o bajo, o aceptar el riesgo y "convivir" con el mismo para esto adicionalmente se requiere la aprobación del Comité de Seguridad de la



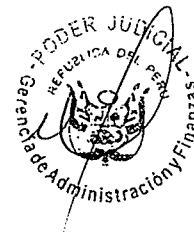
N° de Actividad	UNIDAD ORGÁNICA / RESPONSABLE	ACCIÓN A REALIZAR
		Información. b. Adicionalmente se requiere que los propietarios de los activos de información informen de una fecha tentativa de implementación de cada uno de los controles, así como un responsable de implementación de cada control propuesto, esto con la finalidad de dar seguimiento a dicha implementación.
14		Aprobación del Plan de Tratamiento de Riesgos
14.1	Comité de Seguridad de la Información	a. El Comité de Seguridad de la Información revisará el Plan de Tratamiento de Riesgos de Seguridad de la Información y brindará su aprobación siempre y cuando los propietarios de los activos de información hayan aprobado los controles propuestos por el Oficial de Seguridad así como haber brindado las fechas de implementación tentativa de cada uno de los controles, caso contrario será devuelto al Oficial de Seguridad para completar dicha información.
FIN DEL PROCEDIMIENTO		

7. ANEXOS

- 7.1. Anexo N° 01: Flujograma del Procedimiento de Identificación, Análisis y Evaluación de Riesgos de Seguridad de la Información.
- 7.2. Anexo N° 02: Formulario de Identificación de Activos de Información.
- 7.3. Anexo N° 03: Formulario de Informe de Análisis y Evaluación de Riesgos.
- 7.4. Anexo N° 04: Tabla de Amenazas.
- 7.5. Anexo N° 05: Tabla de Vulnerabilidades.
- 7.6. Anexo N° 06: Tabla de Valorización de Confidencialidad.
- 7.7. Anexo N° 07: Tabla de Valorización de Integridad.
- 7.8. Anexo N° 08: Tabla de Valorización de Disponibilidad.

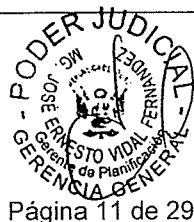
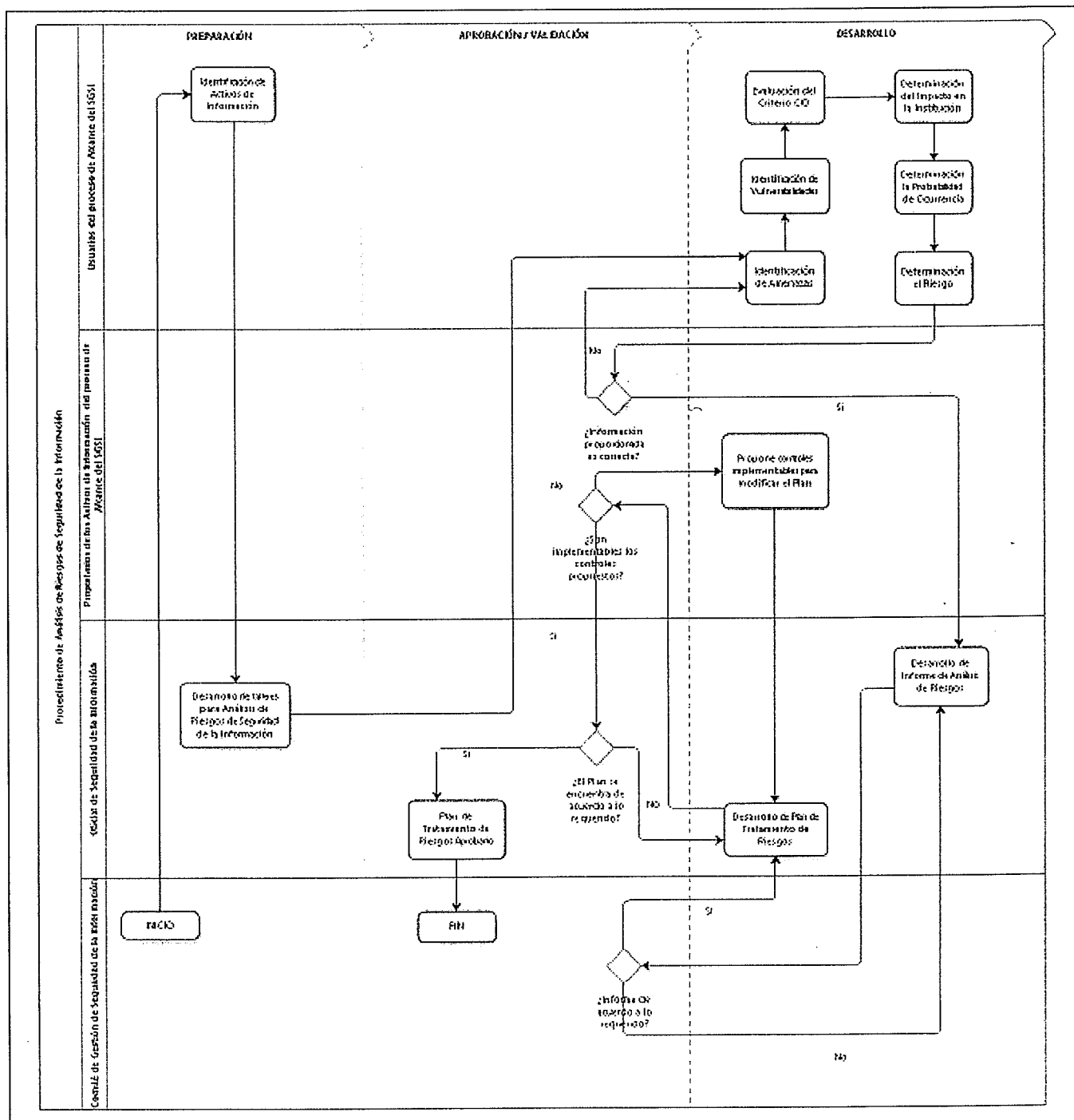


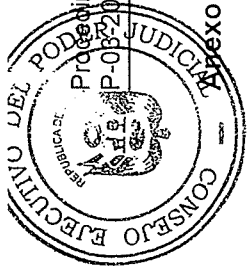
- 7.9. Anexo N° 09: Tabla de Relación CID e Impacto.
- 7.10. Anexo N° 10: Tabla de Valorización del Impacto.
- 7.11. Anexo N° 11: Tabla de Probabilidad de Ocurrencia.
- 7.12. Anexo N° 12: Tabla de Valorización del Riesgo.
- 7.13. Anexo N° 13: Tabla de Nivel de Riesgo.
- 7.14. Anexo N° 14: Mapa de Riesgos.
- 7.15. Anexo N° 15: Información del Tratamiento del Riesgo.



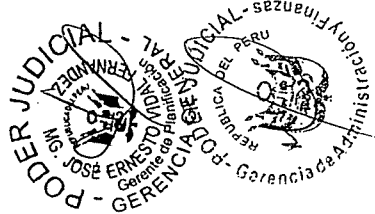
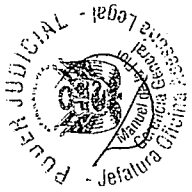



Anexo N° 01: Flujograma del Procedimiento de Identificación, Análisis y Evaluación de Riesgos de Seguridad de la Información.





Apexo N° 02: Formulario de Identificación de Activos de Información.



 Poder Judicial Gerencia General	FORMATO	Código: SGSI-FORM-02
		Revisión: 01
	Identificación de Activos de Información	Aprobado:
		Fecha: 1 de 1

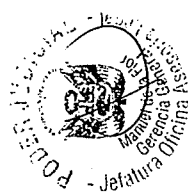
INFORMACIÓN GENERAL DEL ACTIVO						LIBRACIÓN		CLASIFICACIÓN DE INFORMACIÓN	SUBPROCESO	TÍTULO DE USO	VALOR DEL ACTIVO
ITEM	NOMBRE	DETALLE	PROPIETARIO	CUSTODIO	USUARIO	CATEGORÍA	TIPO				

NOMBRE Y FIRMA DEL PROPIETARIO

NOMBRE Y FIRMA PRESIDENTE DEL COMITÉ



Anexo N° 03: Formulario de Informe de Análisis y Evaluación de Riesgos.



	FORMATO	Código:	SGSI-FORM-03
		Revisión:	01
		Aprobado:	
		Fecha:	
		Página:	1 de 1

Informe de Análisis y Evaluación de Riesgos

NOMBRE DEL ACTIVO	AMENAZA	VULNERABILIDAD	C	H	D	VALOR C/D	IMPACTO	PROBABILIDAD	NIVEL DE RIESGO	NOMBRE DEL RIESGO	CÓDIGO DEL RIESGO

NOMBRE Y FIRMA DEL PROPIETARIO

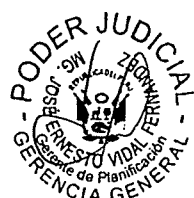
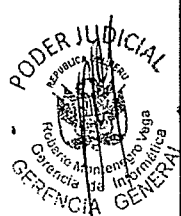
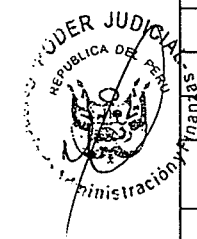
NOMBRE Y FIRMA PRESIDENTE DEL COMITÉ

Anexo N° 04: Tabla de Amenazas.

Código	Amenaza	Tipo
AM1	Incendio	Daño físico
AM2	Daño por agua	
AM3	Contaminación	
AM4	Accidente mayor	
AM5	Destrucción del equipo o los medios	
AM6	Mantenimiento efectuado deficientemente	
AM7	Polvo, corrosión, congelación	
AM8	Fenómeno Climático	Eventos naturales
AM9	Fenómeno sísmico	
AM10	Fenómeno volcánico	
AM11	Fenómeno meteorológico	
AM12	Inundación	
AM13	Fallas del sistema de aire acondicionado o del suministro de agua	Pérdida de servicios esenciales
AM14	Pérdida del suministro de electricidad	
AM15	Falla del equipo de telecomunicaciones	
AM16	Radiación electromagnética	Perturbación debido a radiación
AM17	Radiación térmica	
AM18	Pulsos electromagnéticos	
AM19	Intercepción de señales de interferencia comprometedoras	Compromiso de la información
AM20	Espionaje remoto	
AM21	Interceptación de comunicaciones	
AM22	Vencimiento de contrato	
AM23	Robo de medios o documentos	
AM24	Pérdida de equipo	
AM25	Robo de equipos	
AM26	Hallazgo de medios reciclados o descartados	
AM27	Divulgación	
AM28	Divulgación de claves de software	
AM29	Datos de fuentes no confiables	
AM30	Pérdida de datos	
AM31	Adulteración del Hardware	
AM32	Adulteración del software	
AM33	Uso no autorizado de software	
AM34	Detección de posición	
AM35	Falla de equipo	Fallas técnicas
AM36	Falla en la línea de comunicaciones	

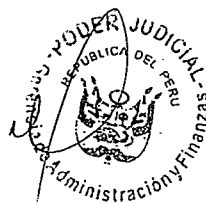
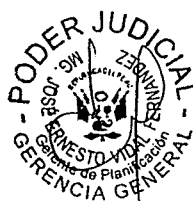


Código	Amenaza	Tipo
AM37	Error en la configuración de software	
AM38	Error en la descarga de archivo	
AM39	Mal funcionamiento del equipo	
AM40	Degradación del servicio	
AM41	Saturación del sistema de información	
AM42	Saturación del sistema de cableado	
AM43	Interrupción de servicios de verificación en línea: Timestamping, OCSP, CRL	
AM44	Desactualización del antivirus	
AM45	Vencimiento de certificado	
AM46	Mal funcionamiento del software	
AM47	Uso no autorizado del equipo	Acciones no autorizadas
AM48	Copia fraudulenta del software	
AM49	Uso de software falsificado o copiado	
AM50	Corrupción de datos	
AM51	Procesamiento ilegal de datos	
AM52	Error en el uso	Compromiso de funciones
AM53	Abuso de derechos	
AM54	Falsificación de derechos	
AM55	Negación de acciones	
AM56	Ruptura en la disponibilidad del personal	
AM57	Hacking	Hacker, cracker
AM58	Ingeniería social	
AM59	Intrusión en el sistema, incursiones	
AM60	Acceso no autorizado al sistema	Criminal informático
AM61	Crimen informático (acoso cibernético)	
AM62	Acto fraudulento (reproducción de archivos, suplantación, interceptación)	
AM63	Soborno informático	
AM64	Falsificación o usurpación de la dirección	Terrorismo
AM65	Intrusión en el sistema	
AM66	Bomba/Terrorismo	
AM67	Equipo de guerra informática	
AM68	Ataque al sistema (ej. DDOS)	
AM69	Penetración en el sistema	Espionaje
AM70	Adulteración del sistema	
AM71	Ventaja de defensa	
AM72	Ventaja política	





Código	Amenaza	Tipo
AM73	Explotación económica	Gente de adentro de la institución (empleados mal capacitados, resentidos, maliciosos, negligentes, deshonestos o despedidos)
AM74	Robo de información	
AM75	Intrusión en la privacidad personal	
AM76	Asalto a un empleado	
AM77	Acceso no autorizado	
AM78	Chantaje	
AM79	Búsqueda de información propietaria	
AM80	Abuso informático	
AM81	Fraude y robo	
AM82	Orientación inadecuada hacia usuarios	
AM83	Acto fraudulento (reproducción o manipulación de documentos)	
AM84	Soborno por información	
AM85	Ingreso de datos falsificados o corruptos	
AM86	Ingreso de información errónea o incompleta	
AM87	Intercepción	
AM88	Códigos maliciosos (ej. Virus, bomba lógica, troyano)	
AM89	Venta de información personal	
AM90	Disfunciones del sistema (bugs)	
AM91	Intrusión en el sistema	
AM92	Sabotaje al sistema	





— Anexo N° 05: Tabla de Vulnerabilidades.

Código	Vulnerabilidad	Categoría
VU1	Mantenimiento insuficiente / instalación fallida de medios de almacenamiento	Hardware
VU2	Falta de esquemas de reemplazo periódicos	
VU3	Susceptibilidad a la humedad, al polvo y a la suciedad	
VU4	Sensibilidad a la radiación electromagnética	
VU5	Falta de control eficiente del cambio de configuración	
VU6	Susceptibilidad a variación de voltaje	
VU7	Susceptibilidad a variaciones de temperatura	
VU8	Almacenamiento no protegido	
VU9	Recursos de host insuficientes	
VU10	Desconexión involuntaria del dispositivo	
VU11	Falta de cuidado al descartarlo	
VU12	Copia no controlada	
VU13	Pruebas al software inexistentes o insuficientes	Software
VU14	Pruebas al software de stress inexistentes o insuficientes	
VU15	Falta de análisis de vulnerabilidades de manera regular	
VU16	Errores conocidos en el software	
VU17	Inadecuada distribución	
VU18	No hacer "logout" cuando se sale de la estación de trabajo	
VU19	Disposición o reutilización de medios de almacenamiento sin borrar apropiadamente	
VU20	Falta de evidencia de auditoria	
VU21	Asignación equivocada de derechos de acceso	
VU22	Software ampliamente distribuido	
VU23	Aplicar programas de aplicación a datos incorrectos en términos del tiempo	
VU24	Interfaz de usuario complicada	
VU25	Falta de documentación	
VU26	Insuficientes controles contra el ingreso masivo de datos	
VU27	Seteo incorrecto de parámetros	
VU28	Fechas incorrectas	
VU29	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios	
VU30	Información no protegida con mecanismos de encriptación adecuados	
VU31	Documentación desactualizada	
VU32	Documentación insuficiente o no disponible de las aplicaciones	
VU33	Falta de documentación / checklist para configuración de Sistema Operativo seguro	



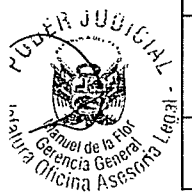
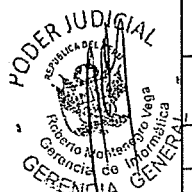
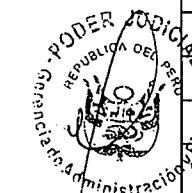


Código	Vulnerabilidad	Categoría
VU34	Falta de procedimientos para el despliegue de aplicaciones web seguras	
VU35	Falta de procedimientos para la revisión y gestión de registros (logs)	
VU36	Falta de un proceso formal para la gestión del cambio y la configuración	
VU37	Falta de cumplimiento del procedimiento formal para la autorización en los sistemas	
VU38	Formato inadecuado no permite seleccionar niveles de autorización por aplicación	
VU39	Complejidad en la administración de los formatos de autorización	
VU40	Procedimientos de operación insuficientes	
VU41	Procedimientos de control de cambios insuficientes	
VU42	Procedimientos de configuración insuficientes	
VU43	Tablas de claves no protegidas	
VU44	Mala administración de claves	
VU45	Habilitación de servicios innecesarios	
VU46	Habilitación de accesos innecesarios	
VU47	Software inmaduro o nuevo	
VU48	Mecanismos de monitoreo insuficientes	
VU49	Falta de procedimiento para el reporte y registro de incidentes	
VU50	Falta de procedimiento formal para la validación de cintas backup	
VU51	Falta de actualización del software	
VU52	Posible envío de datos duplicados	
VU53	Especificaciones no claras o incompletas para los desarrolladores	
VU54	Falta de control de cambios eficaz	
VU55	Descarga y uso incontrolado de software	
VU56	Falta de copias de respaldo	
VU57	Falta de respaldo los logs de la totalidad de los sistemas	
VU58	Falta de procedimientos formales para el control de registros	
VU59	Estaciones con privilegios elevados	
VU60	Ausencia de disgregación de perfiles	
VU61	Insuficiencia en la protección de acceso físico y/o lógico	
VU62	No producir informes de gestión	
VU63	Falta de pruebas de envío o recepción de mensaje	Red
VU64	Falta de políticas de uso de mensajería y difusión	
VU65	Líneas de comunicación no protegidas	
VU66	Insuficiencia de mecanismos de monitoreo	





Código	Vulnerabilidad	Categoría
VU67	Tráfico delicado no protegido	
VU68	Juntas malas en el cableado	
VU69	Punto de falla única	
VU70	Falta de identificación y autenticación de remitente y destinatario	
VU71	Arquitectura de red insegura	
VU72	Inadecuada gestión del enlace (ancho de banda)	
VU73	Planificación inadecuada de puntos de red	
VU74	Transferencia de claves en claro	
VU75	Gestión inadecuada de la red (capacidad de recuperación del ruteo)	
VU76	Conexiones no protegidas de la red pública	
VU77	Ausencia del personal	Personal
VU78	Procedimientos inadecuados del reclutamiento	
VU79	Capacitación de seguridad insuficiente	
VU80	Descuido del personal	
VU81	Uso incorrecto del software y hardware	
VU82	Cuentas administrativas compartidas por más de una persona	
VU83	Falta de conciencia de seguridad	
VU84	Falta de mecanismos de monitoreo	
VU85	Trabajo no supervisado del personal externo o de limpieza	
VU86	Falta de políticas para el uso correcto de medios de telecomunicaciones y mensajería	
VU87	Uso inadecuado o negligente del control de acceso físico a edificios y ambientes	Sitio
VU88	Ubicaciones en una área susceptible a las inundaciones	
VU89	Red inestable de energía eléctrica	
VU90	Falta de protección física del edificio, puertas y ventanas	Institución
VU91	Escenarios de pruebas insuficientes para planes de contingencias	
VU92	Falta de un procedimiento formal para el registro y baja de usuarios	
VU93	Falta de proceso formal para revisar el derecho de acceso (supervisión)	
VU94	Procedimiento poco claro o desactualizado	
VU95	Disposiciones inexistentes o insuficientes (respecto de la seguridad) en contratos con clientes y/o terceros	
VU96	Disposiciones inexistentes o insuficientes (respecto de la seguridad) en contratos con terceros en temas de configuraciones	
VU97	Falta de procedimientos de monitoreo de instalaciones de procesamiento de la información	





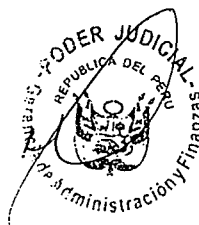
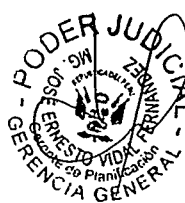
Código	Vulnerabilidad	Categoría
VU98	Falta de auditorías regulares (supervisión)	
VU99	Demora en los procesos de selección de proveedores	
VU100	Falta de procedimientos de identificación y evaluación del riesgo	
VU101	Falta de informes de fallas registradas en los registros del administrador y del operador	
VU102	Respuesta inadecuada del mantenimiento del servicio	
VU103	Inexistencia o insuficiencia de acuerdo sobre el nivel de servicio	
VU104	Falta de procedimiento de control de cambios	
VU105	Falta de procedimientos para el manejo de información clasificada	
VU106	Falta de procedimiento formal para el control de la documentación del Poder Judicial	
VU107	Falta de procedimiento formal para la supervisión del registro del Poder Judicial	
VU108	Falta de proceso formal para autorización de información pública disponible	
VU109	Falta de asignación apropiada de responsabilidades de seguridad en la información	
VU110	Falta de planes de continuidad	
VU111	Falta de una política de uso de correos electrónicos	
VU112	Falta de procedimientos para introducir software en sistemas operativos	
VU113	Faltas de registro en los historiales del administrador y del operador	
VU114	Falta de procedimientos para manejo de la información clasificada	
VU115	Capacitación insuficiente respecto a sus labores	
VU116	Falta de responsabilidades sobre la seguridad de la información en las descripciones de puestos	
VU117	Ausencia o insuficiencia de disposiciones (concernientes a la seguridad de la información en contratos con empleados)	
VU118	Incumplimiento de disposiciones (concernientes a la seguridad de la información por los empleados)	
VU119	Falta de proceso disciplinario definido en caso de incidentes en la seguridad de la información	
VU120	Falta de política formal sobre el uso de computadoras portátiles	
VU121	Falta de control de activos que se encuentran fuera del local	
VU122	Inexistencia o insuficiencia de la política de "escritorio despejado y pantalla despejada"	
VU123	Falta de autorización al acceso a las instalaciones de procesamiento de la información	
VU124	Falta de mecanismos de monitoreo establecidos para las rupturas de la seguridad	



Código	Vulnerabilidad	Categoría
VU125	Falta de revisiones regulares de la gestión	
VU126	Falta de procedimientos para reportar debilidades en la seguridad	
VU127	Falta de procedimientos sobre el cumplimiento de disposiciones respecto de derechos intelectuales	

Anexo N° 06: Tabla de Valorización de Confidencialidad

Valor	Clasificación	Definición	Consecuencia
3	Alta	Es la información o recurso que debe ser divulgada sólo a fuentes autorizadas, controladas y debidamente identificadas. Debe ser modificada y leída por un grupo reducido de personas autorizadas y claramente identificadas.	La divulgación no autorizada produce: - Pérdida de la ventaja competitiva. - Uso malicioso en contra de la Institución. - Pérdidas financieras que no pueden ser absorbidas por la Institución. - Demandas legales que dañan la imagen y confianza pública de la Institución.
2	Media	Es la información que debe ser divulgada sólo al personal de las áreas que la manejan y modificada sólo por personas autorizadas e individualizadas	La divulgación no autorizada produce: - Uso malicioso en contra de la imagen o situaciones puntuales. - Pérdidas financieras que pueden ser absorbidas por la institución - No se producen demandas legales.
1	Baja	Es la información que puede ser divulgada a público general, pero que sólo puede ser modificada por personas autorizadas.	La divulgación no autorizada no representa perjuicio para la Institución.



Anexo N° 07: Tabla de Valorización de Integridad

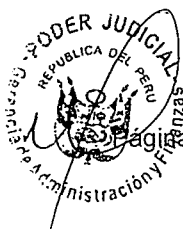
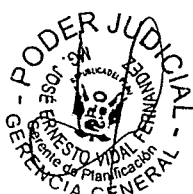
Valor	Clasificación	Criterio	Consecuencia
3	Alta	Es la información o recurso que al ser modificado, intencional o casualmente, por personas o procesos autorizados o no autorizados provoca daños de gran magnitud.	La falta de integridad produce daños de gran magnitud los que se pueden expresar como: <ul style="list-style-type: none"> - Pérdidas económicas (pérdida, incumplimiento de metas). - Falla de los procesos informáticos (incapacidad de ejecutarlos por un período de tiempo más allá de lo estimado como manejable). - Daño de la imagen de la Institución (daño a nivel nacional e internacional que no se puede reparar en el corto plazo). - Pérdida de la confianza de los usuarios.
2	Media	Es la información o recurso que al ser modificado, intencional o casualmente, por personas o procesos autorizados o no autorizados provoca daños de mediana magnitud.	La falta de integridad produce daños de mediana magnitud los que se pueden expresar como: <ul style="list-style-type: none"> - Pérdidas económicas (menor ganancia, incumplimiento de metas en menor escala). - Falla de los procesos informáticos (incapacidad de ejecutarlos por un período de tiempo que está en el límite superior de lo estimado como manejable). - Daño de la imagen de la Institución (daño a nivel nacional, se puede reparar en el corto plazo). - Pérdida de la confianza de los usuarios.
1	Baja	Es la información o recurso que al ser modificado, intencional o casualmente, por personas o procesos autorizados o no autorizados provoca daños de pequeña magnitud.	La falta de integridad produce daños de pequeña magnitud los que se pueden expresar como: <ul style="list-style-type: none"> - Pérdidas económicas (no impacta las ganancias, se cumplen las metas). - Falla de los procesos informáticos (incapacidad de ejecutarlos por un período de tiempo pero este es manejable). - Daño de la imagen de la Institución (daño a nivel nacional que puede no ser percibido y se puede reparar prontamente).



Valor	Clasificación	Criterio	Consecuencia
			- Pérdida de la confianza de los usuarios.

Anexo N° 08: Tabla de Valorización de Disponibilidad

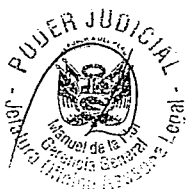
Valor	Clasificación	Definición	Consecuencia
3	Alta	Es información o activo indispensable para la continuidad de la Institución. El recurso principal y el alternativo no pueden faltar por un período prolongado de tiempo en horarios críticos.	La falta de disponibilidad por períodos prolongados produce: - Incumplimiento a los acuerdos de nivel de servicio. La transición entre el recurso principal y el alternativo no debe impactar el acuerdo de servicio. - Perjuicios legales que afectan la imagen de la Institución. - Perjuicios económicos que no pueden ser absorbidos por la Institución. - Problemas sindicales.
2	Media	La disponibilidad de la información es necesaria para la continuidad de la Institución, pero existen canales alternativos para contrarrestar una pérdida de disponibilidad en un tiempo razonable. El recurso principal y el alternativo pueden quedar fuera de servicio por un periodo mínimo de tiempo en horarios críticos.	La falta de disponibilidad produce: - Que los niveles de servicio acordados se puedan ver afectados en la transición entre el medio principal y el alternativo. - Perjuicios legales que no comprometen la imagen de la Institución. - Perjuicios económicos que pueden ser absorbidos por la Institución. - No hay problemas sindicales.
1	Baja	Es información o activos de apoyo o secundarios para el negocio. La información se encuentra duplicada en varias fuentes. Si no está disponible no compromete procesos operativos importantes	La falta de disponibilidad produce: - Que los niveles de servicio acordados para los procesos operativos importantes, no se ven afectados. - Problemas administrativos y operativos no significativos. - Perjuicios económicos que no son significativos. - No hay perjuicios legales. - No hay problemas sindicales.





Anexo N° 09: Tabla de Relación CID e Impacto

Aspecto de Seguridad afectado por el riesgo			IMPACTO
C	I	D	
1	1	1	No Significativo
1	1	2	Menor
1	1	3	Significativo
1	2	1	Menor
1	2	2	Moderado
1	2	3	Significativo
1	3	1	Significativo
1	3	2	Significativo
1	3	3	Significativo
2	1	1	Menor
2	1	2	Moderado
2	1	3	Significativo
2	2	1	Moderado
2	2	2	Moderado
2	2	3	Significativo
2	3	1	Significativo
2	3	2	Significativo
2	3	3	Significativo
	1	1	Significativo
	1	2	Significativo
	1	3	Significativo
	2	1	Significativo
	2	2	Significativo
	2	3	Significativo
	3	1	Significativo
	3	2	Significativo
	3	3	Significativo



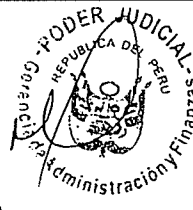


Anexo N° 10: Tabla de Valorización del Impacto

Nivel	Descripción	Impacto en la Institución
5	Catastrófico	Impacta en forma severa en el Poder Judicial punto de comprometer la confidencialidad o integridad de información crítica de la Institución o la continuidad de las operaciones por paralización de los servicios críticos más allá de los tiempos tolerables por el negocio. El impacto es a toda la Institución y su efecto se siente en todo el personal involucrado.
4	Significativo	Impacta en forma grave a un área o servicio específico del Poder Judicial, se puede llegar a comprometer documentos internos clasificados como confidenciales, paralizar o retrasar procesos claves del Poder Judicial por un tiempo considerable. Su efecto está limitado dentro del Poder Judicial.
3	Moderado	El impacto sobre la confidencialidad, integridad y disponibilidad de la información es limitado en tiempo y alcance. Su efecto es para un proceso de soporte o actividad específica que puede subsanarse en corto plazo.
2	Menor	El impacto es leve y se puede prescindir del mismo en un tiempo limitado.
1	No Significativo	No representa un impacto importante para el Poder Judicial.

Anexo N° 11: Tabla de Probabilidad de Ocurrencia

Valor	Clasificación	Definición
1	Muy Baja	El evento no ocurre nunca o casi nunca. Ha ocurrido al menos 1 vez al año.
2	Baja	Si bien el evento puede ocurrir el periodo entre uno y otro evento puede ser muy grande. Al menos 2 veces al año.
3	Moderada	Es posible que ocurra el evento con una frecuencia baja. 3 o 4 veces al año.
4	Alta	Existen antecedentes de que el evento ocurrirá, dentro de un plazo de tiempo que implique una acción para enfrentarlo pero la frecuencia no es alta. 1 vez al mes.
5	Muy Alta	El evento se sabe que ocurre con cierto grado de certeza y que la frecuencia es alta. 1 vez a la semana o más.





Anexo N° 12: Tabla de Valorización del Riesgo

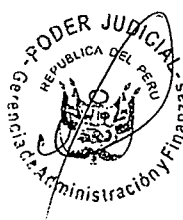
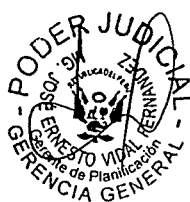
Tabla de Valorización de Riesgos					
Impacto		Probabilidad		Riesgo	
Catastrófico	5	Muy Alta	5		25
Significativo	4	Muy Alta	5		20
Moderado	3	Muy Alta	5		15
Menor	2	Muy Alta	5	Alto	10
No Significativo	1	Muy Alta	5	Mediano	5
Catastrófico	5	Alta	4		20
Significativo	4	Alta	4		16
Moderado	3	Alta	4	Alto	12
Menor	2	Alta	4	Mediano	8
No Significativo	1	Alta	4	Bajo	4
Catastrófico	5	Moderada	3		15
Significativo	4	Moderada	3	Alto	12
Moderado	3	Moderada	3	Alto	9
Menor	2	Moderada	3	Mediano	6
No Significativo	1	Moderada	3	Bajo	3
Catastrófico	5	Baja	2	Alto	10
Significativo	4	Baja	2	Mediano	8
Moderado	3	Baja	2	Mediano	6
Menor	2	Baja	2	Bajo	4
No Significativo	1	Baja	2	No Significativo	2
Catastrófico	5	Muy Baja	1	Mediano	5
Significativo	4	Muy Baja	1	Bajo	4
Moderado	3	Muy Baja	1	Bajo	3
Menor	2	Muy Baja	1	No significativo	2
No Significativo	1	Muy Baja	1	No significativo	1

Nivel de Riesgo:

Del 1 a 2 → No Significativo
 Del 3 a 4 → Bajo
 Del 5 a 8 → Mediano
 Del 9 a 12 → Alto
 Del 15 a 25 → Extremo

Anexo N° 13: Tabla de Nivel de Riesgo

Nivel de Riesgo	Descripción de las Consecuencias
Extremo	Puede afectar seriamente al Poder Judicial, en términos de paralización de las operaciones a la imagen del Poder Judicial. Requiere acción correctiva inmediata más allá del tiempo tolerable, pérdidas considerables o demandas legales y daño considerable.
Alto	Puede afectar los niveles de operación y servicio del Poder Judicial, incumplimiento de metas, y divulgación no autorizada de información fuera del Poder Judicial. Requiere una acción correctiva sujeta a la discreción del Comité de Gestión de Seguridad de la Información en términos de plazos y compromisos.
Mediano	Afecta a los activos de información de soporte a los activos principales, puede afectar la disponibilidad en áreas específicas del Poder Judicial. La divulgación no autorizada no representa perjuicio importante para el Poder Judicial. Su aceptación está sujeta a la revisión del Comité de Gestión de Seguridad de la Información.
Bajo	No causa un efecto considerable en el Poder Judicial. Usualmente son aceptados sin revisión.
No Significativo	El efecto para el Poder Judiciales insignificante. Usualmente no se les considera para la gestión de riesgos.



Anexo N° 14: Mapa de Riesgos

IMPACTO	Catastrófico	5	MEDIANO	ALTO	EXTREMO	EXTREMO	EXTREMO
	Significativo	4	BAJO	MEDIANO	ALTO	EXTREMO	EXTREMO
	Moderado	3	BAJO	MEDIANO	ALTO	ALTO	EXTREMO
	Menor	2	NO SIGNIFICATIVO	BAJO	MEDIANO	MEDIANO	ALTO
	NO Significativo	1	NO SIGNIFICATIVO	NO SIGNIFICATIVO	BAJO	BAJO	MEDIANO
			1	2	3	4	5
			Muy Baja	Baja	Moderada	Alta	Muy Alta
			PROBABILIDAD				

PODER JUDICIAL
REPUBLICA DEL PERU
Gerencia de Informática
Administración y Finanzas

Anexo N° 15 - Información del Tratamiento del Riesgo

El Poder Judicial reconoce los siguientes niveles de riesgos: “Extremo” y “Alto”, “Mediano”, “Bajo y No Significativo”

Para la etapa de tratamiento del riesgo, se han considerado como aceptables los riesgos definidos como: “Mediano”, “Bajo” y “No Significativo”.

Para los riesgos de nivel “Extremo” y “Alto” se procederán a evaluar las siguientes opciones de tratamiento de riesgo:

Reducir el riesgo, Evitar el riesgo o Transferir el riesgo.

Cabe mencionar que durante la etapa de tratamiento de riesgos, cuando el costo de reducir el riesgo sea mayor, al costo del riesgo y/o al activo que lo produce, entonces también el riesgo se considera aceptable.

La decisión sobre el tratamiento de un riesgo se realiza en cada ciclo de evaluación, la cual se realizará una vez al año o cuando ocurran cambios en los procesos del SGSI. Los

PODER JUDICIAL
REPUBLICA DEL PERU
Gerencia de Informática
GERENCIA GENERAL

PODER JUDICIAL
REPUBLICA DEL PERU
Gerencia de Informática
Gerencia General
Oficina Asesora

PODER JUDICIAL
REPUBLICA DEL PERU
Gerencia de Informática
Gerencia General
Oficina Asesora



planes de tratamiento de riesgo, son revisados con periodicidad no mayor a un año por parte del Comité de Gestión de Seguridad de la Información, los nuevos riesgos efectivos son medidos y comparados con los riesgos residuales estimados.

