"Año del Fortalecimiento de la Soberanía Nacional"

RESOLUCION DE GERENCIA MUNICIPAL N° 44-2022-MDLO/GM

Los Olivos, 10 de Agosto 2022

EL GERENTE MUNICIPAL DE LA MUNICIPALIDAD DISTRITAL DE LOS OLIVOS:

VISTOS:

El Informe N° 054-2022-MDLO/GTIC de la Gerencia de Tecnologías de la Información y Comunicaciones, Informe N° 094-2022-MDLO/GTIC-JSRT de la Jefatura de Soporte, Redes y Telecomunicaciones, Memorando N° 142-2022-MDLO/GTIC de la Gerencia de Tecnologías de la Información y Comunicaciones, el Informe N° 071-2022-SGPMGP-GPP/MDLO, de la Subgerencia de Planeamiento y Modernización de la Gestión Pública, el Informe N° 156-2022-GPP/MDLO de la Gerencia de Planeamiento y Presupuesto, y el Informe N° 133-2022/MDLO/GAJ de la Gerencia de Asesoría Jurídica; y,

CONSIDERANDO:

Que, el artículo 194° de la Constitución Política del Perú, modificado por el artículo 1° de la Ley N° 30305, establece que las municipalidades son órganos de gobierno local, con autonomía política, económica y administrativa en los asuntos de su competencia, lo cual es concordante con los dispuesto en el artículo II del Título Preliminar de la ley Orgánica de Municipalidades, y que dicha autonomía radica en la facultad de ejercer actos de gobiernos administrativos y de administración con sujeción al ordenamiento jurídico; es decir, que la autonomía que los municipios ostentan no es absoluta, sino más bien relativa, por cuanto no está sujeta al ordenamiento jurídico vigente. Dicha restricción también alcanza a los administrados en los procedimientos administrativos que se ejecutan de los gobiernos locales;

Que, el artículo 4° de la Ley marco de Modernización de la Gestión Pública indica que el proceso de modernización de la gestión del Estado tiene como finalidad fundamental la obtención de mayores niveles de eficiencia del aparato estatal de manera que se logre una mejor atención a la ciudadanía, priorizando y optimizando el uso de los recursos públicos;

Que, la Política Nacional de Modernización de la Gestión Pública al 2021 aprobada mediante Decreto Supremo N° 004-2012-PCM, indica, en el numeral 4 del artículo 2.3°, que la Política Nacional de Modernización de la Gestión Pública tiene por objetivo general el implementar la gestión por procesos y promover la simplificación administrativa en todas las entidades públicas a fin de generar resultados positivos en la mejora de los procedimientos y servicios orientados a los ciudadanos y empresas;

Que, a través del Decreto Supremo N° 029-2021-PCM, se aprueba el Reglamento del Decreto Legislativo N° 1412, Ley de Gobierno Digital; asimismo, con el Decreto de Urgencia N° 007-2020, que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento;

Que, con Resolución Ministerial N° 028-2015-PCM, se aprueba los "Lineamientos para la gestión de la continuidad operativa de las entidades públicas en los tres niveles de gobierno";

Que, en el artículo 28.1 del Reglamento de Organización y Funciones aprobado con Ordenanza N° 491-CDLO y su modificatoria, indica que la Gerencia de Planeamiento y Presupuesto es la encargada de dirigir los procesos de planeamiento, planificación, inversiones públicas, gestión presupuestaria, racionalización, estadística y modernización de la gestión pública con la finalidad de asesorar, promover y orientar a las unidades orgánicas de la municipalidad en las materias antes mencionadas;

Que, siendo los documentos normativos formulados y expedidos por los órganos de una entidad precisando políticas y determinando los procedimientos que deben realizarse en la ejecución de funciones, éstas deben ser concordantes con la normatividad vigente;

Que, mediante el Memorando N° 142-2022-MDLO/GTIC de la Gerencia de Tecnologías de la Información y Comunicaciones, valida la opinión de las unidades orgánicas con algún grado de intervención y remite la propuesta de Directiva, **"DIRECTIVA PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE LOS OLIVOS"**, a la Subgerencia de Planeamiento y Modernización de la Gestión Pública, con el objeto de Establecer los criterios y metodología para la Gestión de Riesgos de Seguridad de la Información (SGSI) de la Municipalidad Distrital de Los Olivos, ajustándose a los lineamientos establecidos en la normativa vigente. Asimismo, con el documento en mención, la Gerencia de Tecnologías de la Información y Comunicaciones da conformidad al proceso de revisión, comentarios y/u opinión de las unidades con algún grado de intervención en la propuesta de directiva;

Que, mediante el Informe N° 071-2022-SGPMGP-GPP/MDLO de la Subgerencia de Planeamiento y Modernización de la Gestión Pública da su conformidad, y señala la necesidad y oportunidad de aprobar la propuesta de Directiva denominado: "**DIRECTIVA PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE LOS OLIVOS**";

Que, con Memorándum N° 133-2022/MDLO/GAJ, la Gerencia de Asesoría Jurídica informa que es procedente la aprobación de la propuesta de Directiva, "**DIRECTIVA PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE LOS OLIVOS**";

Que, mediante el Informe N° 156-2022-GPP/MDLO, la Gerencia de Planeamiento Presupuesto informa que se hace necesario aprobar mediante Resolución de Gerencia la propuesta de Directiva, "**DIRECTIVA PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE LOS OLIVOS**";

Que, de conformidad con lo dispuesto en el numeral 20 del artículo 20 de la Ley Orgánica de Municipalidades N° 27972, se indica que el alcalde se encuentra facultado en "Delegar sus atribuciones administrativas en el Gerente Municipal". Asimismo, en uso de las facultades previstas en el inciso f) del ARTÍCULO PRIMERO de la Resolución de Alcaldía N° 471-2017, se delega en el Gerente Municipal las facultades de "Aprobar planes y directivas internas de competencia de la Alcaldía sobre los sistemas administrativos y de gestión pública, así como modificarlas y/o dejarlas sin efecto las mismas";

SE RESUELVE:

ARTÍCULO PRIMERO. - **APROBAR** la Directiva N° 003-2022-MDLO/GM, "**DIRECTIVA PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE LOS OLIVOS**", cuyo objeto es establecer los criterios y metodología para la Gestión de Riesgos de Seguridad de la Información (SGSI) de la Municipalidad Distrital de Los Olivos, ajustándose a los lineamientos establecidos en la normativa vigente.

ARTÍCULO SEGUNDO. - **NOTIFICAR** lo dispuesto en la presente resolución a la Gerencia de Tecnologías de la Información y Comunicaciones y a la Gerencia de Planeamiento y Presupuesto.

ARTÍCULO TERCERO. - **DISPONER** la publicación de la presente Resolución de Gerencia Municipal en el Portal de Transparencia Estándar de la Municipalidad Distrital de Los Olivos www.munilosolivos.gob.pe.

REGÍSTRESE, COMUNÍQUESE Y CÚMPLASE.

MUNICIPALIDAD DISTRITAL DE LOS OLIVOS
Julian E. Loli Bonilla
Gerente Municipal

DIRECTIVA N° 003-2022-MDLO/ GM

DIRECTIVA PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE LOS OLIVOS

ROL	NOMBRE	CARGO	FECHA	FIRMA y V°B°
Elaborado por:	Ricardo Gustavo Alvarado Bustos	Gerente de Tecnologías de la Información y Comunicaciones		
Revisado por:	Luisa Acero Condori	Gerente de Planeamiento y Presupuesto		
	Johnny Francisco Galván Valdez	Gerente de Asesoría Jurídica		
Aprobado por:	Julián Enrique Loli Bonilla	Gerente Municipal		

CONTROL DE CAMBIOS *

N°	Ítems	Descripción del cambio	Versión	Fecha de vigencia
1	-	Versión Inicial del Documento	01	

Comentarios a las Versiones

* Contemplar sólo las 2 últimas versiones.

INDICE

I. OBJETIVO 5

II. FINALIDAD 5

III. BASE LEGAL 5

IV. ALCANCE 5

V. DEFINICIONES 6

VI. RESPONSABILIDADES 7

VII. DISPOSICIONES GENERALES 8

VIII. DISPOSICIONES ESPECIFICAS 8

IX. DISPOSICIONES COMPLEMENTARIAS 13

X. ANEXOS 14

I. OBJETIVO

Establecer los criterios y metodología para la Gestión de Riesgos de Seguridad de la Información (SGSI) de la Municipalidad Distrital de Los Olivos.

II. FINALIDAD

Identificar, analizar, evaluar y dar tratamiento a los riesgos de seguridad de la información según el alcance del SGSI, en cumplimiento con la normativa vigente para garantizar razonablemente el logro de los objetivos estratégicos y operativos de la entidad municipal.

III. BASE LEGAL

- Constitución Política del Perú
- Ley N° 27658: Ley Marco de Modernización de la Gestión del Estado y modificatorias.
- Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública.
- Ley N° 29733, Ley de Protección de Datos Personales.
- Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital y modificatorias.
- Decreto Supremo N° 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo N° 1412, Ley de Gobierno Digital.
- Decreto de Urgencia N° 007-2020, que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.
- Resolución N°129-2014/CNB-INDECOPI, que aprueba 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".
- 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. Sistema de Gestión de Seguridad de la Información. Requisitos Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución Directoral N° 056-2017-INACAL-DN, que aprueba como Norma Técnica Peruana (NTP), entre otras, la NTP-ISO/IEC 27002:2017 "Tecnología de la Información. Técnicas de Seguridad. Código de prácticas para controles de seguridad de la información", 1° Edición.
- Resolución Directoral N° 047-2018-INACAL-DN, que aprueba como Norma Técnica Peruana (NTP), entre otras, la NTP-ISO/IEC 27005:2018 "Tecnología de la Información. Técnicas de seguridad. Gestión de riesgos de la seguridad de la información", 2° Edición.
- Resolución Directoral N° 029-2019-INACAL-DN, que aprueba como Norma Técnica Peruana (NTP), entre otras, la NTP-ISO/IEC 27035-1:2019 "Tecnología de la Información. Técnicas de seguridad. Gestión de incidentes de seguridad de la información. Parte 1: Principios de la gestión de incidencias", 1° Edición.
- Resolución Directoral N° 014-2018-INACAL-DN, que aprueba como Norma Técnica Peruana (NTP), entre otras, la NTP-ISO 31000:2018 "Gestión de Riesgos – Principios y Directrices", 2° Edición.
- Ordenanza N° 491-CDLO, que aprueba el Reglamento de Organización y Funciones de la Municipalidad Distrital de Los Olivos, y modificatorias.

IV. ALCANCE

Las disposiciones contenidas en el presente documento se aplican en las actividades de gestión y tratamiento de los riesgos de seguridad de la información de la organización en el marco de los procesos contenidos dentro del Alcance del SGSI.

V. DEFINICIONES

Para efectos de la presente directiva, se entenderá por:

a. **Seguridad de la información:** Todas las acciones orientadas a preservar la integridad, confidencialidad y disponibilidad de la información y los activos asociados a su tratamiento independiente de la forma en la que la información se encuentre.
b. **Sistema de Gestión de Seguridad de la Información:** El Sistema de Gestión de Seguridad de la Información (SGSI) permite gestionar de manera adecuada la seguridad de la información institucional, a fin de hacer frente a amenazas de ataque o intromisión, error, actos fortuitos (inundación, incendio, etc.), entre otros.
c. **Confidencialidad:** Evita que personas no autorizadas accedan a la información institucional.
d. **Disponibilidad:** Permite la disposición de la información cuando sea requerido por el personal autorizado.
e. **Integridad:** Mantiene la información en su totalidad y sin alteraciones, a menos que sea modificado por el personal autorizado.
f. **Incidente de seguridad de la información:** Evento no deseado que genera amenaza a la seguridad de la información y que tiene una probabilidad significativa de comprometer a la operatividad de la Entidad
g. **Activo de información:** Cualquier información que tiene valor para la Entidad y para el Sistema de Gestión de Seguridad de la Información. Se consideran también los recursos humanos, tecnológicos que intervienen en el tratamiento directo o indirecto de la información, así como sus procesos y actividades.
h. **Información:** Cualquier forma de registro de contenidos susceptibles a ser procesados, distribuidos y almacenados, pudiendo estar en formato electrónico, óptico, magnéticos u otro medio de almacenamiento.
i. **Amenaza:** Cualquier factor que tiene el potencial para explotar una debilidad y dar lugar a algún tipo de daño a la información o a la institución.
j. **Vulnerabilidad:** Debilidad identificada sobre un activo y que puede ser aprovechado por una amenaza para causar una afectación sobre la confidencialidad, integridad o disponibilidad de dicho activo.
k. **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencia de auditoría y evaluarlas de manera objetiva, para determinar el grado de cumplimiento de criterios pre-establecidos.
l. **Control:** Medio para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la entidad que pueden ser de naturaleza administrativa, técnica, de gestión o legal.
m. **Control de acceso:** Medios o mecanismo para garantizar que el acceso a los activos de manera autorizada y restringida, basado en los requerimientos de negocios y los requisitos de seguridad.

n. **Credencial de acceso:** Corresponde al mecanismo mediante el cual se le asigna una identificación única e irrepetible a una persona, para que tenga acceso a las aplicaciones de la Entidad, con el propósito de desempeñar las tareas encomendadas.

o. **Evento:** Un suceso que puede ser interno o externo a la Entidad, que ocurren en un momento determinado y son originados por una causa especifica.

p. **Propietario de activo:** funcionario o servidor asignado de garantizar que el activo asignado bajo su responsabilidad esté protegido con los controles definidos en el SGSI y que le apliquen a dicho activo; es el responsable por la afectación de la confidencialidad, integridad y disponibilidad del mismo, en cualquiera de los procesos que se encuentre involucrado.

q. **Riesgo:** Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de aquello que se espera, sea positivo, negativo o ambos. Los objetivos pueden tener aspectos diferentes (económicos, de imagen institucional, etc.) y se pueden aplicar a niveles diferentes (operativo, estratégico, organización).

r. **Tratamiento del riesgo:** Proceso de selección e implementaci6n de medidas para modificar el riesgo.

VI. REPONSABILIDADES

6.1. La Gerencia de Tecnologías de la Información y Comunicaciones será responsable del cumplimiento de las disposiciones de la presente directiva, promover la participación activa del personal en la identificación, análisis, y evaluación de riesgos de seguridad de la información.

6.2. La Gerencia de Tecnologías de la Información y Comunicaciones será responsable de adoptar las acciones pertinentes para implementar los lineamientos dispuesto en la presente directiva en coordinación con el Comité de Gobierno Digital y la Gerencia Municipal.

6.3. El Comité de Gobierno Digital, será el responsable de gestionar, supervisar y velar su cumplimiento de la presente metodología de gestión de riesgos de seguridad de la información, comprometiendo el apoyo de la Alta Gerencia.

6.4. El Oficial de Seguridad y Confianza Digital será el responsable de liderar las reuniones a desarrollarse para el tratamiento de los riesgos de seguridad de la información, verificar, supervisar y coordinar el cumplimiento de la presente directiva Metodologías de Gestión de Seguridad de la Información.

VII. DISPOSICIONES GENERALES

7.1. Para el tratamiento de la Metodología de Gestión de Seguridad de la Información se deberá utilizar los formatos establecidos en los anexos que forma parte de la presente directiva.

7.2. El análisis y evaluación de riesgos de seguridad de la información se realizará utilizando el método cualitativo, de manera a función de juicio de expertos, experiencia y conocimiento de las partes involucradas en cumplimiento al numeral 6.1 Acciones para tratar los riesgos y las oportunidades, 6.1.2 Valoración del riesgo de seguridad de la información y 6.1.3 Tratamiento del riesgo de seguridad de la información de la Norma Técnica Peruana ISO/IEC27001:2014.

7.3. El proceso de la Metodología de Gestión de Seguridad de la Información, comprenderá las principales actividades de acuerdo a la NTP/IEC 31000:2018, la cual señala el proceso de gestión del riesgo.

7.4. El glosario de la terminología utilizada en el proceso de gestión de riesgos la información, estará comprendida en la NTP ISO/IEC 27001:2014, NTP ISO/IEC 31000:2018 e ISO 18788:2015.

VIII. DISPOSICIONES ESPECIFICAS

8.1. COMUNICACIÓN Y CONSULTA

8.1.1. La comunicación y consulta con las partes involucradas tanto internas como externas deberá realizarse durante todas las etapas del proceso para la gestión del riesgo.

8.1.2. La comunicación será importante para garantizar que aquellos responsables de la implementación de las acciones dentro de cada uno de los procesos entiendan las bases sobre las cuales se toman las decisiones y las razones por las cuales se requieren dichas acciones, que permita llevar a cabo con el fin de:

a. Ofrecer garantías de los resultados de la gestión del riesgo de la entidad municipal.
b. Recopilar información sobre los riesgos.
c. Compartir los resultados de la evaluación del riesgo y presentar el plan de tratamiento de riesgos.
d. Evitar o reducir la ocurrencia y la consecuencia de las violaciones de seguridad de la información debido a la falta de comprensión mutua entre la Gerencia de Tecnologías de la Información y Comunicaciones y las demás Gerencias tomadores de decisiones.
e. Obtener información para la toma de decisiones.
f. Obtener nuevos conocimientos en seguridad de la información.
g. Coordinar con las partes involucradas y planificar las respuestas para reducir las consecuencias de cualquier incidente.
h. Proporcionar información a la alta gerencia acerca de la responsabilidad de los riesgos.
i. Enriquecer y mejorar el conocimiento referente a la gestión del riesgo.

8.1.3. El Oficial de Seguridad y Confianza Digital de la Municipalidad Distrital de Los Olivos deberá fomentar y coordinar la participación y las actuaciones de todas las partes involucradas internas como externas en la gestión del riesgo a través de reuniones y talleres planificados.

8.1.4. El Oficial de Seguridad y Confianza Digital deberá comunicar al Comité de Gobierno Digital el inicio de un nuevo ciclo de gestión de riesgos de seguridad de la información.

8.1.5. El Oficial de Seguridad y Confianza Digital deberá comunicar al Comité de Gobierno Digital, el desarrollo de las actividades del proceso de metodología de gestión de riesgos de seguridad de la información.

8.2. ESTABLECIMIENTO DEL CONTEXTO

8.2.1. Gestionar los riesgos a la seguridad de la información del Alcance del SGSI y que soportan las operaciones de la entidad, manteniendo los acuerdos de niveles de servicio (SLA) en los términos de:

a. Confidencialidad (C)
b. Integridad (I)
c. Disponibilidad (D)

8.2.2. El Oficial de Seguridad y Confianza Digital es el responsable de brindar soporte en las actividades de implementación y mantenimiento en la gestión del riesgo de la seguridad de la información dentro del ámbito de su competencia.

8.2.3. La frecuencia para las evaluaciones de riesgos de seguridad de la información será anualmente, siendo los principales criterios los siguientes:

a. **Cambios en la entidad:** Tecnológicos, estratégicos, instalaciones, etc.
b. **Cambios en el entorno:** Aparición de nuevas amenazas, nuevas oportunidades, nuevos requerimientos legales, etc.

8.2.4. Las evaluaciones realizadas serán informadas al Comité De Gobierno Digital.

8.2.5. Al inicio de un nuevo ciclo de gestión de riesgos de seguridad de la información, el Comité de Gobierno Digital deberá evaluar los cambios en el contexto de la entidad, objetivos, estrategias; así como también las disposiciones legales, reglamentarias, necesidades y expectativas que son relevantes para el desarrollo del proceso de gestión de riesgos, asegurando que el Sistema de Gestión de Seguridad de la Información (SGSI) pueda lograr los resultados deseados.

8.3. IDENTIFICACION DEL RIESGO

8.3.1. Inventario de activos de información

8.3.1.1. Los activos de información son los recursos que utiliza un Sistema de Gestión de Seguridad de la Información para que las organizaciones funcionen y consigan los objetivos del negocio.

8.3.1.2. Clasificar los activos de tipo de información, de acuerdo a lo señalado en el **Anexo 01 "Clasificación de la Información".**

8.3.1.3. El registro de los activos de información se hará según lo establecido en el **Anexo 02 "Formato Inventario de Activos de Información".**

8.3.2. Valorización del activo de la información

8.3.2.1. Realizar la valoración de los activos de información, de acuerdo a las escalas establecidas en el **Anexo 03 "Escala para la valoración de activos".**

8.3.3. Identificación de riesgos

8.3.3.1. Identificar los activos con escalas de valoración Alto y Muy Alto, según lo descrito en el **Anexo 04 "Criterios de Valoración y Selección de Activos"**, a fin de asegurar la identificación de riesgos para dichos activos.

8.3.3.2. La identificación del riesgo de seguridad de la información deberá realizarse con los activos que tienen la escala de valoración Alto y Muy Alto, por ello el propietario del activo y el oficial de seguridad y confianza digital, evaluaran teniendo en cuenta las siguientes consideraciones:

a. Identificar las vulnerabilidades de los activos de información es necesario considerar que la vulnerabilidad no causa daños por sí misma, es necesario la existencia de una amenaza presente para explotarla, lo cual significa que una vulnerabilidad que no tiene una amenaza podría no requerir la implementación de un control. El **Anexo 05 "Listado de Vulnerabilidades"**.

b. Las causas y amenazas que puedan determinar la materialización de un evento, su posible consecuencia o afectación, relacionándolos con la identificación de riesgos de seguridad de la información. Algunas amenazas pueden afectar a más de un activo y en tales casos pueden causar diferentes impactos dependiendo de los activos que se vean afectados. En el **Anexo 06 "Listado de Amenazas"**, se describe las amenazas más comunes, asimismo se debe considerar también las Fuentes de Amenazas Humanas descritas en el mismo anexo.

c. Adicionalmente, se detallará para cada activo el proceso donde fue identificado, las vulnerabilidades, amenazas, descripción del riesgo inherente y propietario de riesgo, consideradas en el **Anexo 07 "Formato de Análisis y Evaluación de Riesgos"**.

8.4. ANALISIS DEL RIESGO

8.4.1. El Oficial de Seguridad y Confianza Digital, en coordinación con el propietario del activo, deberá realizar el análisis de riesgo con la finalidad de establecer su valor de acuerdo a los criterios de probabilidad e impacto considerados en el **Anexo 08 "Escala de Probabilidad de Ocurrencias del Riesgo"** y **Anexo 09 "Escala de Impacto del Riesgo"**, respectivamente. Así como también de completar la información indicada en el Anexo 7 "**Formato de Análisis y Evaluación de Riesgos**".

8.4.2. El valor del riesgo o el nivel de exposición (riesgo inherente) se calculará mediante la multiplicación de la relación de probabilidad / impacto según **Anexo 10 "Cálculo del Nivel de Riesgo" y el Anexo 11 "Criterios para el Tratamiento de Riesgos"**.

8.4.3. Posteriormente, se identificará los controles existentes o implementar nuevos controles, considerados según el **Anexo 12 "Tipos de Controles"** y el **Anexo 13 "Evaluación de Controles"**.

8.4.4. Finalmente, se determinará el riesgo residual según el **Anexo 14 "Determinación del Riesgo Residual"**.

8.5. VALORACIÓN DEL RIESGO

8.5.1. La valoración del riesgo es el producto de confrontar los resultados de la evaluación del riesgo con los controles identificados, esto se hace con el objetivo de establecer prioridades para su manejo y para la fijación de políticas.

8.5.2. El Oficial de Seguridad y Confianza Digital, en coordinación con el propietario del activo efectuaran la valoración del riesgo.

8.5.3. Los riesgos serán valorados en 3 valores (Alto, Moderado y Bajo), los valores iguales y por debajo del moderado serán los riesgos aceptables o tolerables debido a que no representa mayor impacto en la entidad municipal, considerada en el **Anexo 10 "Cálculo del Nivel de Riesgo".**

8.5.4. Los riesgos valorados como "Alto", ingresarán al proceso de tratamiento de riesgos de seguridad de la información que debe ser realizado por el propietario del activo y por el Oficial de Seguridad y Confianza Digital, quienes comunicarán los resultados al Comité de Gobierno Digital.

8.5.5. Los riesgos identificados como aceptables serán evaluados por lo menos una vez al año o en el siguiente nuevo ciclo de gestión de riesgos para verificar si continúan con los valores de probabilidad e impacto estimados.

8.5.6. La información será presentada en el **Anexo 07 "Formato de Análisis y Evaluación de Riesgos"**; contando con la conformidad del propietario del activo.

8.5.7. El Oficial de Seguridad y Confianza Digital, es el responsable de consolidar la información una vez haya finalizado el análisis y evaluación de riesgos que deberá informar al Comité de Gestión de Seguridad de la Información.

8.6. TRATAMIENTO DEL RIESGO

8.6.1. Para tratamiento del riesgo, deberá considerar las mejoras a implementar, ya sea mediante la inclusión de controles adicionales, teniendo en cuenta las discreciones establecidas en el **Anexo 11 "Criterios para el Tratamiento de Riesgos"**.

8.6.2. La aceptación del riesgo será formalizada por el Oficial de Seguridad y Confianza Digital, así como también de completar la información indicada en el **Anexo 15 "Formato de Aceptación de Riesgos"**.

8.6.3. El Oficial de Seguridad y Confianza Digital, en coordinación con el propietario del activo, deberá formular y determinar la estrategia de tratamiento a seguir y los controles a implementar (de corresponder) para cada riesgo de seguridad de la información no tolerable según el **Anexo 17 "Tratamientos de Riesgos".**

8.7. SEGUIMIENTO Y REVISION

8.7.1. El seguimiento y la revisión se deberá realizar en todas las etapas del proceso de la gestión del riesgo; considerando planificar, recopilar y analizar información, registrar resultados y proporcionar retroalimentación.

8.7.2. El Oficial de Seguridad y Confianza Digital, deberá realizar el seguimiento periódico al Tratamiento de Riesgo, considerando los estados definidos en el **Anexo 16 "Estados del Tratamiento de Riesgos"**.

8.7.3. El Oficial de Seguridad y Confianza Digital, realizará el seguimiento y revisión de la implementación de los controles del SGSI, cuyo resultado será informado al Comité de Gobierno Digital mediante en reuniones.

8.7.4. El Oficial de Seguridad y Confianza Digital, debe informar al Comité de Gobierno Digital el resultado del análisis, evaluación y tratamiento de los riesgos, anualmente una (01) vez al año.

8.8. REGISTRO INFORME

8.8.1. El Oficial de Seguridad y Confianza Digital, deberá documentar e informar al Comité de Gobierno Digital de las actividades realizadas respecto a la gestión de riesgo.

DISPOSICIONES COMPLEMENTARIAS

PRIMERA. - La presente directiva entrará en vigencia a partir del día siguiente de su aprobación a través del correspondiente acto administrativo.

X. REGISTROS

Producto de la ejecución del presente procedimiento, se deben generar los siguientes registros:

N°	Registro	Responsable de su administración	Requisitos mínimos
1	Registro de Incidencias de Respaldo; Registro de Pruebas de la Información Respalda; Registro de Información Recuperada	Jefatura de Soporte, Redes y Telecomunicaciones	El archivo debe proporcionarse, por la Jefatura de Soporte, Redes y Telecomunicaciones, en formato digital y/o impresa editable con información clara, concordante y precisa. Validad por el responsable.

XI. ANEXOS

- Anexo 01 - Clasificación de la Información
- Anexo 02 - Formato Inventario Activos de Información
- Anexo 03 - Escala Para La Valoración de los Activos
- Anexo 04 - Criterios de Valoración y Selección de Activos
- Anexo 05 - Listado de Vulnerabilidades
- Anexo 06 - Listado de Amenazas
- Anexo 07 - Formato de Análisis y Evaluación de Riesgos
- Anexo 08 - Escala de Probabilidad de Ocurrencias del Riesgo
- Anexo 09 - Escala de Impacto del Riesgo

- Anexo 10 - Cálculo del Nivel de Riesgo
- Anexo 11 - Criterios para el Tratamiento de Riesgos
- Anexo 12 - Tipos de Controles
- Anexo 13 - Evaluación de Controles
- Anexo 14 - Determinación del Riesgo Residual
- Anexo 15 - Formato de Aceptación de Riesgos
- Anexo 16 - Estados del Tratamiento de Riesgos
- Anexo 17 - Tratamiento de Riesgos

ANEXO 01 - CLASIFICACIÓN DE LA INFORMACIÓN

Los criterios de clasificación que vamos aplicar a los activos de información, estará establecido por su nivel de accesibilidad.

Los activos de tipo de información serán clasificados de acuerdo a lo establecido en el siguiente cuadro:

CLASIFICACIÓN DE INFORMACIÓN EN EL MARCO DEL SGSI	
CLASIFICACIÓN	**DESCRIPCIÓN**
PÚBLICA	Son todos aquellos activos que se presumen públicos, y que pueden ser accedidos tanto por miembros de la institución como por personas externas a ella (**público en general**), sin estar sujetos a ningún control. Su divulgación no genera impacto para la Municipalidad Distrital de Los Olivos.
CONFIDENCIAL	Son todos aquellos activos que pertenecen a un **proceso o unidad orgánica** y que por su naturaleza son reservados exclusivamente al personal del área o proceso específico y cuyo acceso excepcional por parte de personal externo (auditores, entidades reguladoras, consultores externos) puede realizarse, sin embargo, se encuentra regulado y sujeto a condiciones específicas de acceso. Su divulgación podría generar un impacto relevante a la Municipalidad Distrital de Los Olivos (pérdida económica, sanción legal o pérdida de imagen).
INTERNA	Son todos aquellos activos que son accedidos exclusivamente por **personal interno de la institución** y cuyo acceso excepcional por parte de personal externo (auditores, entidades reguladoras, consultores externos) puede realizarse, sin embargo, se encuentra regulado y sujeto a condiciones específicas de acceso (acuerdo de confidencialidad).
RESTRINGIDA	Es toda información cuyo contenido es restringido a un **grupo determinado de individuos**, seleccionados a partir de un proyecto específico o que pertenecen a un grupo dentro de la organización.

ANEXO 02 - FORMATO INVENTARIO ACTIVOS DE INFORMACIÓN

Donde se registrarán los siguientes datos:

a. **Área.** - Se registra el nombre del área dueña del proceso a registrar sus activos de información.

b. **Proceso.** - Se registra el nombre del proceso al que pertenecen los activos de información.

c. **Fecha.** - Se registra la fecha de identificación de los activos de información.

d. **Código del Activo.** - Se define con el siguiente formato: AC0001; donde AC= Activo y 0001: número correlativo integral.

e. **Nombre del Activo.** - Nombre corto del activo de información.

f. **Descripción del Activo.** - Se registra un breve descripción detallada del activo de información, como, por ejemplo: Manual del Proceso ABC, Manual del Usuario del Sistema XYZ, Reporte ABC, etc.

g. **Clasificación del Activo.** - Tipo de activo según su clasificación del anexo 01.

h. **Ubicación.** - Ubicación física o electrónica del activo de información.

i. **Propietario del Activo.** - Detalla el nombre del propietario del activo de información identificado; bajo el concepto que este es el responsable de controlar la producción, desarrollo, mantenimiento, uso y seguridad del activo de información, tiene autoridad formal y no significa que tenga derechos de propiedad sobre el activo.

j. **Valor Total.** - Valoración del activo de información según el anexo 03.

k. **Observaciones.** - Observaciones o información adicional sobre el activo de información.

l. **Grupo.** - Agrupación de activo de información, como, por ejemplo: software, hardware, electrónica, etc.

ANEXO 02 - FORMATO INVENTARIO ACTIVOS DE INFORMACIÓN

AREA			
PROCESO			
RESPONSABLE		FECHA	

CÓDIGO DE ACTIVO	NOMBRE DE ACTIVO	DESCRIPCIÓN DEL ACTIVO	CLASIFICACIÓN DEL ACTIVO	UBICACIÓN	PROPIETARIO DEL ACTIVO	VALOR TOTAL	OBSERVACIONES	GRUPO

MUNICIPALIDAD DISTRITAL DE LOS OLIVOS V°B° GERENCIA MUNICIPAL

MUNICIPALIDAD DISTRITAL DE LOS OLIVOS GERENCIA Gerencia de Planeamiento y Presupuesto

MUNICIPALIDAD DISTRITAL DE LOS OLIVOS ASESORÍA JURÍDICA

ANEXO 03 - ESCALA PARA LA VALORACIÓN DE LOS ACTIVOS

El valor del activo de información se estima mediante el promedio de sumar los valores del nivel de relevancia respecto a la confidencialidad, integridad y disponibilidad:

$$Valor\ del\ Activo = \frac{(\ Confidencialidad + Integridad + Disponibilidad\ )}{3}$$

Para determinar el nivel de relevancia de cada aspecto de la confidencialidad, integridad y disponibilidad de la información, se emplea la siguiente escala de valor:

Valor	Confidencialidad	Disponibilidad	Integridad
Muy Alto (5)	La información asociada al activo es solo accedida por el personal de alto rango, pues su divulgación afectaría irreversiblemente a la organización.	Se requiere que el activo nunca se encuentre indisponible (0 horas), pues su carencia afectaría irreversiblemente a la organización o a sus procesos operativos críticos.	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 0%, pues la vulneración de su integridad afectaría irreversiblemente a la organización o a sus procesos operativos críticos.
Alto (4)	La información asociada al activo es restringida y solo personal de un proyecto específico puede acceder a ella, pues su divulgación afectaría gravemente a la organización.	Se considera que como máximo el activo puede estar indisponible por una hora (01), pues su carencia afectaría gravemente a la organización o a sus procesos operativos críticos.	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 25%, pues la vulneración de su integridad afectaría gravemente a la organización o a sus procesos operativos críticos.
Medio (3)	La información asociada al activo es confidencial y solo personal de algunas áreas internas pueden acceder a ella, pues su divulgación afectaría considerablemente a la organización.	Se considera que como máximo el activo puede estar indisponible por un día, pues su carencia afectaría considerablemente a la organización.	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 50%, pues la vulneración de su integridad afectaría considerablemente a la organización.

Bajo (2)	La información asociada al activo es de uso interno y solo personal de la organización puede acceder a ella, pues su divulgación afectaría parcialmente a la organización.	Se considera que como máximo el activo puede estar indisponible por una semana, pues su carencia afectaría parcialmente a la organización.	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 85%, pues la vulneración de su integridad afectaría parcialmente a la organización.
Muy Bajo (1)	La información asociada al activo es pública y cualquiera puede acceder a ella, pues no impacta a la organización.	Se considera que como máximo el activo puede estar indisponible por tiempo indefinido, pues su carencia no impacta a la organización.	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 100%, pues la vulneración de su integridad no impacta a la organización.

En base al promedio obtenido (valor del activo de información en términos de confidencialidad, integridad y disponibilidad) y al rango de tasación establecido por la entidad, se identifican los activos más significativos.

ANEXO 04 - CRITERIOS DE VALORACION Y SELECCIÓN DE ACTIVOS

Los activos a considerar en la etapa de análisis y evaluación de riesgos serán aquellas cuyo valor obtenido en la valoración es mayor o igual a cuatro (4).

A manera de ejemplo tenemos lo siguiente:

Tabla N° 1
Ejemplo de selección de activos

ACTIVOS	VALORACIÓN
<Activo 1>	2
<Activo 2>	5
<Activo 3>	4
<Activo 4>	3

Del ejemplo anterior, tenemos lo siguiente:

Los activos que serán considerados para la etapa de análisis y evaluación de riesgo son el activo 2 y el activo 3, porque presenta valores mayores o iguales a cuatro (4).

ANEXO 05 - LISTADO DE VULNERABILIDADES

CODIGO	VULNERABILIDAD	CATEGORIA
VU001	Mantenimiento insuficiente	Hardware
VU002	Falta de esquemas de reemplazo periódicos	
VU003	Susceptibilidad a la humedad, al polvo y a la suciedad	
VU004	Falta de control eficiente del cambio de configuración	
VU005	Susceptibilidad a variación de voltaje	
VU006	Susceptibilidad a variaciones de temperatura	
VU007	Almacenamiento no protegido	
VU008	Falta de cuidado al descartarlo	
VU009	Equipo desfasado por vigencia tecnológica	
VU010	Pruebas al software inexistentes o insuficientes	Software
VU011	Software	
VU012	Errores conocidos en el software	
VU013	No hacer "logout" cuando se sale de la estación de trabajo	
VU014	Disposición o reutilización de medios de almacenamiento sin borrar apropiadamente	
VU015	Falta de evidencia de auditoria	
VU016	Asignación equivocada de derechos de acceso	
VU017	Software ampliamente distribuido	
VU018	Interfaz de usuario complicada	
VU019	Falta de documentación	
VU020	Seteo incorrecto de parámetros	
VU021	Fechas incorrectas	
VU022	Falta de mecanismos de identificación y autentificación como la autentificación de usuarios	
VU023	Tablas de claves no protegidas	
VU024	Mala administración de claves	
VU025	Habilitación de servicios innecesarios	
VU026	Software inmaduro o nuevo	
VU027	Especificaciones no claras o incompletas para los desarrolladores	
VU028	Falta de control de cambios eficaz	
VU029	Descarga y uso incontrolado de software	
VU030	Falta de copias de respaldo	
VU031	Falta de pruebas de envió o recepción de mensaje	Red
VU032	Lineas de comunicación no protegidas	
VU033	Tráfico delicado no protegido	
VU034	Mala estructura del cableado	
VU035	Falta de identificación y autentificación del destinatario	
VU036	Arquitectura de red insegura	

VU037	Transferencia de claves en claro	
VU038	Gestión inadecuada de la red (capacidad de recuperación del ruteo)	
VU039	Conexiones no protegidas de la red pública	
VU040	Ausencia del personal	Personal
VU041	Procedimientos inadecuados del reclutamiento	
VU042	Capacitación de seguridad insuficiente	
VU043	Uso incorrecto del software y hardware	
VU044	Falta de conciencia de seguridad	
VU045	Falta de mecanismos de monitoreo	
VU046	Trabajo no supervisado del personal externo o de limpieza	
VU047	Falta de políticas para el uso correcto de medios de telecomunicaciones y mensajería	
VU048	Uso inadecuado o negligente del control de acceso físico a edificios y ambientes	Sitio
VU049	Ubicaciones en un área susceptible a las inundaciones	
VU050	Red inestable de energía eléctrica	
VU051	Falta de protección física del edificio, puertas y ventanas	
VU052	Falta de un procedimiento formal para el registro y baja de usuarios	Institución
VU053	Falta de proceso formal para revisar el derecho de acceso (supervisión)	
VU054	Disposiciones inexistentes o insuficientes (respecto de la seguridad) en contratos con proveedores y/o terceros	
VU055	Falta de auditorias regulares (supervisión)	
VU056	Falta de informes de fallas registradas en los registros del administrador y del operador	
VU057	Respuesta inadecuada del mantenimiento del servicio	
VU058	Inexistencia o insuficiencia de acuerdo sobre el nivel de servicio	
VU059	Falta de procedimiento de control de cambios	
VU060	Falta de procedimiento formal para el control de la documentación de la institución	
VU061	Falta de proceso formal para autorización de información pública disponible	
VU062	Falta de asignación apropiada de responsabilidades de seguridad en la información	
VU063	Falta de planes de continuidad	
VU064	Falta de una política de uso de correos electrónicos	
VU065	Falta de procedimientos para introducir software en sistemas operativos	
VU066	Faltas de registro en los historiales del administrador y del operador	
VU067	Falta de procedimientos para manejo de la información clasificada	
VU068	Falta de responsabilidades sobre la seguridad de la información en las descripciones de puestos	
VU069	Ausencia o insuficiencia de disposiciones (concernientes a la seguridad de la información en contratos con el personal y personal estable)	

VU070	Falta de proceso disciplinario definido en caso de incidentes en la seguridad de la información	Institución
VU071	Falta de política formal sobre el uso de computadoras portátiles	
VU072	Falta de control de activos que se encuentran fuera del local	
VU073	Inexistencia o insuficiencia de la política de "escritorio despejado y pantalla despejada"	
VU074	Falta de autorización al acceso a las instalaciones de procesamiento de la información	
VU075	Falta de mecanismos de monitoreo establecidos para las rupturas de la seguridad	
VU076	Falta de revisiones regulares de la gestión	
VU077	Falta de procedimientos para reportar debilidades en la seguridad	
VU078	Otras vulnerabilidades más que se pudieran presentar (*)	Otros

(*) En caso de presentar una nueva vulnerabilidad no descrita en la lista, podrá continuar actualizando la lista.

ANEXO 06 - LISTADO DE AMENAZAS

CODIGO	AMENAZA	TIPO
AM001	Incendio	Daño físico
AM002	Daño por agua	
AM003	Contaminación	
AM004	Destrucción del equipo o los medios	
AM005	Polvo, corrosión, congelación	
AM006	Fenómeno climático	Eventos naturales
AM007	Fenómeno sísmico	
AM008	Fenómeno volcánico	
AM009	Fenómeno meteorológico	
AM010	Inundación	
AM011	Fallas del sistema de aire acondicionado o del suministro de agua	Pérdida de servicios esenciales
AM012	Pérdida del suministro de electricidad	
AM013	Falla del equipo de telecomunicaciones	
AM014	Radiación electromagnética	Perturbación debido a radiación
AM015	Radiación térmica	
AM016	Interceptación de comunicaciones	Compromiso de la información
AM017	Robo de medios o documentos	
AM018	Robo de equipos	
AM019	Hallazgo de medios reciclados o descartados	
AM020	Divulgación de información	
AM021	Datos de fuentes no confiables	
AM022	Adulteración del hardware	
AM023	Adulteración del software	
AM024	Falla de equipo	Fallas técnicas
AM025	Saturación del sistema de información	
AM026	Mal funcionamiento del software	
AM027	Uso no autorizado del equipo	Acciones no autorizadas
AM028	Copia fraudulenta del software	
AM029	Uso de software falsificado o copiado	
AM030	Procesamiento ilegal de datos	
AM031	Abuso de derechos	Compromiso de funciones
AM032	Falsificación de derechos	
AM033	Negación de acciones	
AM034	Ruptura en la disponibilidad del personal	
AM035	Hacking	Hacker, cracker
AM036	Ingeniería social	
AM037	Acceso no autorizado al sistema	

AM038	Bomba/Terrorismo	Terrorismo
AM039	Ataque al sistema (ej. DDOS)	
AM040	Adulteración del sistema	
AM041	Asalto a un empleado	Gente dentro de la Institución (empleados mal capacitados, resentidos, maliciosos, negligentes, deshonestos o despedidos)
AM042	Chantaje	
AM043	Abuso informático	
AM044	Robo de información	
AM045	Soborno por información	
AM046	Ingreso de datos falsificados o corruptos	
AM047	Códigos maliciosos (ej. Virus, bomba lógica, troyano)	
AM048	Otras amenazas más que se pudieran presentar (*)	Otros

(*) En caso de presentar una nueva amenaza no descrita en la lista, podrá continuar actualizando dicho cuadro de lista.

ANEXO 07 - FORMATO DE ANÁLISIS Y EVALUACIÓN DE RIESGOS

GRUPO / CAT. DE ACTIVOS	CODIGO DE VULNERABILIDAD	CODIGO DE AMENAZA	CODIGO DE RIESGO	DESCRIPCION DE RIESGO	PROPIETARIO DE RIESGO	RIESGO INHERENTE				SUMA DEL CID	IMPACTO	VALOR DEL RIESGO	NIVEL DEL RIESGO
						PROBABILIDAD	CONFIDENCIALIDAD	INTEGRIDADA	DISPONIBILIDAD				

Para considerar la etapa de Análisis y Evaluación de Riesgos tener en cuenta la descripción de la cabecera del formato:

a. **GRUPO / CAT. DE ACTIVOS.** – Agrupación de activos.
b. **CODIGO DE VULNERABILIDAD.** – código definido en el anexo 5
c. **CODIGO DE AMENAZA.** – código definido en el anexo 6
d. **CODIGO DE RIESGO.** – se define con el siguiente formato: R001; donde R= Riesgo y 001 es el número correlativo incremental.
e. **DESCRIPCION DE RIESGO.** – Breve descripción del riesgo.
f. **PROPIETARIO DE RIESGO.** – Cargo funcional del propietario según definición en el numeral 5.
g. **PROBABILIDAD** – Se calcula considerando el Anexo 8
h. **CONFIDENCIALIDAD** – Los valores son: 0=No afectado, 1=Bajo, 2=Medio, 3=Alto
i. **INTEGRIDAD** - Los valores son: 0=No afectado, 1=Bajo, 2=Medio, 3=Alto
j. **DISPONIBILIDAD** - Los valores son: 0=No afectado, 1=Bajo, 2=Medio, 3=Alto
k. **SUMA DEL CID.** – Se calcula la suma de: CONFIDENCIALIDAD + INTEGRIDAD + DISPONIBILIDAD
l. **IMPACTO.** – Se calcula con la suma del CID, si el valor es: 0 = 1; entre 1 y 2 = 2; entre 3 y 5 = 3 y mayor que 6 = 4
m. **VALOR DEL RIESGO.** – Se obtiene multiplicación de: PROBABILIDAD x IMPACTO
n. **NIVEL DEL RIESGO.** – Se calcula considerando el Anexo 10.

ANEXO 08 - ESCALA DE PROBABILIDAD DE OCURRENCIAS DEL RIESGO

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

PROBABILIDAD	VALOR	DESCRIPCIÓN	FRECUENCIA
Muy Baja	1	El evento puede ocurrir solo en circunstancias excepcionales.	Nunca o no se ha presentado en los últimos 5 años o más.
Baja	2	El evento podría ocurrir en algún momento.	Se puede presentar al menos una vez en los últimos 5 años.
Media	3	El evento probablemente ocurrirá en la mayoría.	Se puede presentar al menos en los dos últimos años.
Alta	4	Se espera que el evento ocurra en la mayoría de las circunstancias.	Se puede presentar al menos una vez al año.

ANEXO 09 - ESCALA DE IMPACTO DEL RIESGO

La valoración del impacto que puede ocasionar a la entidad municipal, la materialización del Riesgo de Seguridad de la información, se representa con la descripción de la siguiente tabla:

IMPACTO	VALOR	DESCRIPCIÓN	SEGURIDAD DE LA INFORMACIÓN
Insignificante	1	Si el hecho llegara a presentarse tendría consecuencias o efectos mínimos sobre la entidad municipal.	Afecta a una actividad del proceso.
Menor	2	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad municipal.	Afecta a un grupo de trabajo, a una persona, grupo de personas o algunas actividades del proceso.
Moderado	3	Si el hecho llegara a presentarse tendría medianas consecuencias o efectos sobre la entidad municipal.	Afecta un conjunto de datos personales o el proceso.
Mayor	4	Si el hecho llegara a presentarse tendría altas consecuencias o efectos sobre la entidad municipal.	Afecta varios conjuntos de datos personales o procesos de la entidad municipal o toda la entidad municipal. Multas por incumplimiento de la Legislación. Suspensión de las actividades misionales de la entidad municipal.

ANEXO 10 - CÁLCULO DEL NIVEL DE RIESGO

Con base en la determinación de la probabilidad y la valoración del impacto, se establecen los niveles de riesgos teniendo una clasificación propia para la entidad municipal:

DIMENSIÓN DEL RIESGO DE SEGURIDAD DE INFORMACIÓN	VALOR	ACCIÓN REQUERIDA
Riesgo Alto	Mayor a 6	Evitar el riesgo, empleando controles que busquen reducir el nivel probabilidad. Reducir el riesgo empleando controles orientados a minimizar el impacto si el riesgo se materializa. Compartir o transferir el riesgo mediante la ejecución de pólizas.
Riesgo Moderado	Menor a 7 y Mayor a 2	Evitar o mitigar el riesgo mediante medidas adecuadas y aprobadas, que permiten llevarlo a la zona de riesgo moderado. Compartir o transferir el riesgo.
Riesgo Bajo	Menor a 3 y Mayor a 0	Asumir el riesgo. Mitigar el riesgo con actividades propias del proceso y por medio de acciones preventivas.

En función a los factores mencionados, se define al nivel de riesgo como la multiplicación del impacto y su probabilidad de ocurrencia.

Nivel de riesgo $_{(Ri)}$ = **Impacto** $_{(Ri)}$ x **Probabilidad** $_{(Ri)}$

Valoración del Riesgo

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

Probabilidad \ Impacto	Mayor (4)	Moderado (3)	Menor (2)	Insignificante (1)
Alta (4)	Alto(16)	Alto (12)	Alto (8)	Medio (4)
Media (3)	Alto (12)	Alto (9)	Medio (6)	Medio (3)
Baja (2)	Alto (8)	Medio (6)	Medio (4)	Bajo (2)
Muy Baja (1)	Medio (4)	Medio (3)	Bajo (2)	Bajo (1)

En concordancia y alineación con los Niveles de Riesgos, las acciones requeridas se contemplan en la siguiente tabla:

DIMENSIÓN DEL RIESGO	ACCIÓN REQUERIDA
Zona de Riesgo Bajo	**Aceptar el Riesgo:** Riesgos para los cuales se determinan que el nivel de exposición es adecuado y por lo tanto es aceptable.
Zona de Riesgo Moderado	**Mitigar o Evitar el Riesgo:** Riesgos para los cuales se requiere fortalecer los controles existentes y/o agregar nuevos controles.
Zona de Riesgo Alto	**Evitar el Riesgo:** Se requiere de acciones inmediatas que permitan reducir la probabilidad y el impacto de materialización.

ANEXO 11 - CRITERIOS PARA EL TRATAMIENTO DE RIESGOS

	MEDIDA FRENTE AL RIESGO
EVITAR	Esta estrategia consiste en no iniciar o no continuar con la actividad, eliminar la amenaza o proteger el proceso del impacto que puede generar el riesgo; por ejemplo: • La cancelación de una actividad o conjunto de actividades que generan el riesgo. • Modificaciones de las condiciones en la que funciona el negocio.
MITIGAR	Esta estrategia consiste en implementar medidas o controles para disminuir la posibilidad de ocurrencia o el impacto del riesgo, teniendo en cuenta lo siguiente: • Eliminar la fuente del riesgo. • Cambiar la probabilidad. • Cambiar la consecuencia.
ACEPTAR	Esta estrategia consiste en reconocer el riesgo y sus consecuencias. y no tomar ninguna medida a menos que el riesgo se materialice. La estrategia de aceptar el riesgo implica que periódicamente se deberá revisar la amenaza para asegurarse que no cambie significativamente. La aceptación del riesgo debe ser realizada formalmente por la entidad municipal, ya que su elección implica que la entidad municipal es consciente de las posibles amenazas a las que se encuentra expuesta y que está optando por no tomar medidas frente a estas. Para ello deberá completar el **Formato de Aceptación de Riesgos** (Anexo 15).
TRANSFERIR	Esta estrategia consiste en trasladar el impacto de una amenaza a un tercero (empresas aseguradoras o proveedores de servicio), junto con la responsabilidad de la respuesta. Se utiliza cuando no se puede mitigar la probabilidad de ocurrencia de un riesgo, pero el impacto es inminente. El trasladar o compartir el riesgo no implica que deje de ser propietario de riesgo ni eliminar el riesgo. Entre las actividades que se pueden implementar tenemos el uso de seguros o garantías de cumplimiento.

ANEXO 12 - TIPOS DE CONTROLES

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

ANEXO 13 - EVALUACIÓN DE CONTROLES

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

Se refiere, si el control se encuentra bien definido a nivel teórico, es decir, si con certeza ha sido planteado y documentado, para lograr mitigar la parte del riesgo para lo cual fue concebido.

VALORIZACIÓN DE LA EFECTIVIDAD DEL CONTROL	
NIVEL	**DESCRIPCIÓN**
FUERTE	• El control es totalmente automatizado. • La responsabilidad del control está asignada individualmente y formalizada, y se ha asumido claramente dicha responsabilidad. • Procedimiento del control está documentado y actualizado.
MODERADO	• Control combinado (manual-Automatizado). • La responsabilidad del control esta oficialmente asignada. Procedimiento del control no muy complejo. • Procedimiento del control documentado y no actualizado.
DEBIL	• Control totalmente manual. • La responsabilidad del control no está asignada. Procedimiento del control muy complejo. • Procedimiento del control no documentado.

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

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

VALORIZACIÓN DEL IMPACTO DEL CONTROL	
NIVEL	**DESCRIPCIÓN**
FUERTE	• Históricamente no se han detectado desviaciones del control. • El control es autoevaluado regularmente. • El Control es de aplicación continua y de frecuencia continua.
MODERADO	• Históricamente se presentan muy pocas desviaciones del control. • Ha sido auto-evaluado con alguna frecuencia. • El Control es discreto y periódico.
DEBIL	• Históricamente se presentan continuas desviaciones del control. • Nunca ha sido autoevaluado. • El Control es discreto (Muestreo) y esporádico.

c. **Evaluación del Control**

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

EVALUACIÓN DEL CONTROL		
EFECTIVIDAD	**IMPACTO**	**CALIFICACIÓN DE EVALUACIÓN DEL CONTROL**
Débil	Fuerte, Moderado o Débil	Débil
Fuerte, Moderado o Débil	Débil	Débil
Moderado	Fuerte	Fuerte
Fuerte	Moderado	Moderado

ANEXO 14 - DETERMINACIÓN DEL RIESGO RESIDUAL

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

CALIFICACIÓN DE EVALUACIÓN DEL CONTROL	PROBABILIDAD	IMPACTO
Fuerte	2 niveles hacia abajo	2 niveles hacia abajo
Moderado	1 niveles hacia abajo	1 niveles hacia abajo
Débil	0 niveles hacia abajo	0 niveles hacia abajo

ANEXO 15 - FORMATO DE ACEPTACIÓN DE RIESGOS

Área : .....

Proceso: .....

Fecha : .....

El propietario de Riesgos, de la Municipalidad Distrital de Los Olivos, declara:

- Que la aceptación de los riesgos es una decisión tomada con entera responsabilidad, en forma totalmente voluntaria y sin presiones.
- Un riesgo aceptado podría provocar daños graves a futuro en la entidad municipal, sin embargo, asumimos la responsabilidad personal de aceptar el (los) riesgo(s) aquí descritos y el impacto que estos puedan tener en la Municipalidad Distrital de Los Olivos.
- La responsabilidad personal no significa que somos financieramente responsables de las pérdidas que pueden ocurrir como resultado de la aceptación de riesgos. La responsabilidad personal significa que la aceptación de estos riesgos puede comprometer los recursos, los sistemas, infraestructura.
- También entendemos que la aceptación de estos riesgos y sus responsabilidades expirará en un año a partir de la fecha de firma de este documento.
- La aceptación actual de este riesgo no significa que con un cambio de las condiciones actuales en que se encuentre estos riesgos pueden ser mitigados en un futuro con las condiciones financieras técnicas y administrativas adecuadas.
- He leído la declaración y estoy de acuerdo en aceptar los siguientes riesgos:

N°	CODIGO DEL RIESGO	NOMBRE DEL RIESGO	NIVEL DEL RIESGO
1			
2			
3			
4			

NOMBRE DEL PROPIETARIO DEL RIESGO
CARGO DEL PROPIETARIO DEL RIESGO

ANEXO 16 - ESTADOS DEL TRATAMIENTO DE RIESGOS

Para efectuar el seguimiento periódico al Tratamiento de Riesgos, deberá considerar los siguientes estados:

ESTADO	DESCRIPCIÓN
PENDIENTE	Se establecerá este estado una vez establecido los plazos qua tomará la implementación del control.
EN PROCESO	Se establecerá este estado cuando ya se empezó con la implementación de acciones o controles establecidos.
IMPLEMENTADO	Se consignará este estado cuando ya se concluyó la implementación de las acciones de tratamiento del riesgo o controles.
SUSPENDIDO	Se considera a aquellas acciones desestimadas. Se deberé justificar esta decisión, actualizar la estrategia de tratamiento y el valor de riesgo residual, de corresponder.

ANEXO 17 - TRATAMIENTO DE RIESGOS

PLAN DE TRATAMIENTO DE RIESGOS

RESPONSABLE		FECHA	

CÓDIGO DE ACTIVO	CÓDIGO DE RIESGO	ACCIONES A REALIZAR (CONTROLES)	RESPONSABLE	FECHA DE IMPLEMENTACIÓN	ESTADO

a. **Código de Activo.** - Es el código del activo determinado en el Anexo 02.
b. **Código de Riesgo.** - Es el código del riesgo determinado en el Anexo 07.
c. **Acciones a Realizar.** - Actividades definidas para minimizar riesgos.
d. **Responsable.** - Cargo funcional del responsable del Plan de Acción.
e. **Fecha de Implementación.** - Fecha máxima para el desarrollo o implementación de las acciones a realizar.
f. **Estado.** - Estado de implementación según en el Anexo 16.