RESOLUCIÓN de GERENCIA GENERAL

Nº 023-2019-GG/ZED ILO

Ilo; 2019 Mayo 07.

VISTOS:

El Informe N° 030-2019-DOI/ZED ILO, de la Dirección de Operaciones e Infraestructura de ZED ILO, y;

CONSIDERANDO:

Que, la Zona Especial de Desarrollo Ilo - ZED ILO, es un Organismo Público con autonomía administrativa, técnica, económica, financiera y operativa, en virtud a lo dispuesto en el artículo 2° de la Ley Nº 28569 "Ley que otorga autonomía a los CETICOS", hoy ZED ILO conforme a lo establecido en la Ley N° 30446; adscrita al Gobierno Regional de Moquegua, en virtud a la Ley Nº 29014;

Que, mediante el Informe del Vistos de fecha 06 de Mayo del presente año, la Dirección de Operaciones e Infraestructura de la Entidad remite en veintitrés (23) folios incluidos 14 Anexos la Directiva de controles de seguridad de la Información y Gestión de Riesgos en Tecnología de la Información (TI), indicando que la misma servirá para el desarrollo de las actividades del área de Informática de la institución, así como para los términos de referencia para la contratación del servicio de nube para la Entidad. Por lo cual solicita a la Gerencia General la aprobación de la citada Directiva mediante acto administrativo.

Que el objetivo y finalidad de la Directiva de controles de seguridad de la Información y Gestión de Riesgos en Tecnología de la Información (TI) es establecer lineamientos y directrices respectivamente para efectuar la gestión de controles de seguridad de la información y gestión de riesgos para los procesos de ZED ILO.

Por lo que; de conformidad con lo establecido en el Artículo 8 de la Ley Nº 28569 "Ley que otorga Autonomía a los CETICOS" sus modificatorias Ley Nº 28854, Ley Nº 29479, Ley N° 30446; 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 y sus modificatorias; Resolución N° 031-2018-GG/ZED ILO; y con el visto bueno de la Oficina de Asesoría Legal, Dirección de Operaciones e Infraestructura y Oficina General de Administración de ZED ILO;

ZED ILO Asesoría Legal

SE RESUELVE:

ARTICULO PRIMERO- Aprobar la Directiva N° 06-2019/ZED ILO Directiva de controles de seguridad de la Información y Gestión de Riesgos en Tecnología de la Información (TI) de la Zona Especial de Desarrollo Ilo – ZED ILO, la misma que consta de veintitrés (23) folios incluidos 14 Anexos.

ZED ILO Dirección de Operaciones e Infraestructura

ARTICULO SEGUNDO- Remitir copia de la presente Resolución a la Oficina General de Administración, Oficina de Asesoría Legal, Dirección de Operaciones e Infraestructura, Dirección de Promoción y Desarrollo y Órgano de Control Institucional de ZED ILO.

ZED ILO Oficina General de Administración

REGÍSTRESE, COMUNIQÚESE Y NOTIFIQUESE.

ZED ILO Zona Especial de Desarrollo

Abog. JORGE PACORA FUENTES
Gerente General

DIRECTIVA DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN Y GESTION DE RIESGOS EN TECNOLOGIAS DE LA INFORMACION (TI)

DIRECTIVA N° 06-2019/ZED ILO

I. OBJETIVO

Establecer lineamientos para efectuar la gestión de controles de seguridad de la información y gestión de riesgos para los procesos de ZED ILO.

II. FINALIDAD

Establecer las directrices para efectuar la gestión de controles de seguridad de la información y gestión de riesgos para los procesos de ZED ILO.

III. ALCANCE

La importancia de esta política se orienta a garantizar el uso apropiado de los dispositivos tecnológicos (computadores de escritorio, portátiles, etc.) y de los servicios (Internet, Correo Electrónico, etc.), brindando al personal del de ZED ILO(funcionarios, servidores, CAS, locadores de servicios y otros) y demás personas (naturales, jurídicas, consultores, contratistas, temporales o terceras partes u otros) que brindan servicios a la entidad, las pautas para la utilización apropiada de dichos recursos, permitiendo así minimizar los riesgos de una eventual pérdida de activos de información sensitivos para la ZED ILO.

ZED ILO ANALISTA DE SISTEMAS

ALCANCE DE LA SEGURIDAD DE LA INFORMACIÓN

Para la ZED ILO la seguridad de la información es aplicable a todos los activos de información durante su ciclo de vida. Dicha seguridad está orientada a proteger los activos de información en todos los ambientes en los cuales ésta reside, y para asegurar los activos de información que residen en lugares externos (pe. Dependencias, proveedores de servicios, etc.), estos son sometidos a controles equivalentes para su protección.

ZED ILO Dirección de Operaciones e Infraestructura

ALCANCES DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Estas Políticas aplican a todo el personal dela ZED ILO (funcionarios, servidores, CAS, locadores de servicios y otros) y demás personas (naturales, jurídicas, consultores, contratistas, temporales y terceras partes u otros) que brindan servicios a la entidad, quienes están sujetos a los mismos requerimientos de seguridad, y tienen las mismas responsabilidades de seguridad de información que el personal de la entidad.

La Oficina de Recursos Humanos deberá notificar a los trabajadores actuales y a los nuevos sobre los lineamientos de la presente Directiva y en el caso de los locadores de servicio deberá ser informado a estos a través del responsable de las adquisiciones de la entidad.

IV. BASE LEGAL

- ✓ Ordenanza Regional N° 02-2017-CR/GRN, Reglamento de Organización y Funciones de la Zona Especial de Desarrollo de Ilo – ZED ILO
- ✓ Resolución Ministerial N° 004-2016-PCM que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a Edición". Modificada por el Artículo 3 de la Resolución Ministerial N° 166-2017-PCM, publicada el 21 junio 2017, por el Artículo 2 de la Resolución Ministerial N° 087-2019-PCM, publicada el 22 marzo 2019.
- ✓ Ley 27806, Ley de Transparencia y Acceso a la Información Pública.
- ✓ Resolución N°031-2018-GG/ZED ILO, que Aprueba la Política Institucional de Gestión de Riesgos.

V. DISPOSICIONES GENERALES

1. Este punto lo voy a sacar dado a que no es necesario colocarlo dado que la entidad no tiene el implementado el ISO 27001, pero si podemos tomar referencias de dicha norma para la presente directiva.
2. En ZED Ilo, el planeamiento para la Gestión de Riesgos, en el marco del Sistema de Control Interno, se encuentra a cargo del Comité de Evaluación de Riesgos, (conformado por la Dirección de Promoción y Desarrollo, área de Tesorería y área de Informática), estando supervisado por el Comité de Control Interno. La ejecución del proceso de Gestión de Riesgos, es efectuada por las jefaturas y unidades orgánicas de la entidad, según se establezca en el Plan de Administración de Riesgos correspondiente.
3. Se deberá registrar la información de Gestión de riesgos y Oportunidades en los formatos indicados en los Anexos 3 y 4 de la presente directiva, así como guardar dichos registros tal como lo establecido en la Ley N°28717, "Ley de Control Interno para las entidades del estado"
4. Dichos formatos fueron elaborados por la oficina de informática teniendo como referencias análisis de riesgo aplicados a otras entidades del estado.
5. El análisis y evaluación de los riesgos y oportunidades se efectuará sobre la base de escalas de valoración de tipo cualitativo, es decir, haciendo uso de valores subjetivos de acuerdo al conocimiento y experiencia de las partes involucradas en el proceso a analizar.

VI. DISPOSICIONES ESPECÍFICAS

6.1 COORDINACIONES PARA EL INICIO DE UN CICLO DE GESTIÓN DE RIESGOS Y OPORTUNIDADES

6.1.1 El Comité de Evaluación de Riesgos comunicará el inicio de un ciclo de gestión riesgos y oportunidades a todas las partes interesadas en los procesos dentro alcance del análisis, así como la necesidad de su participación. Dicho comité ha sido aprobado con Resolución N°031-2018-GG/ZED ILO

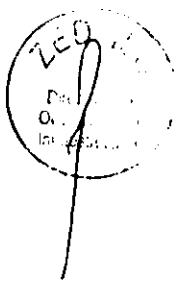
6.1.2 El Comité de Evaluación de Riesgos efectuará una breve inducción al personal a fin de uniformizar los conocimientos sobre la gestión de riesgos y oportunidades, asimismo, explicará las responsabilidades de los participantes en cada actividad y las implicancias de los retrasos.

6.2 REVISIÓN DEL CONTEXTO Y DEL PROCESO A ANALIZAR

6.2.1 Previo al inicio de un nuevo ciclo de gestión de riesgos y oportunidades, El Comité de Evaluación de Riesgos, deberán revisar la información de contexto como los objetivos y estrategias de la organización, las disposiciones legales y reglamentarias, los requisitos y expectativas de las partes externas e internas que son importantes para el desarrollo del proceso y la información sobre la satisfacción de las necesidades de las partes interesadas.

6.2.2 Asimismo, deberán revisar los subprocesos, actividades, entradas, salidas, flujos de información existentes de los procesos dentro del alcance del análisis de riesgo y oportunidades.

6.3 IDENTIFICACIÓN Y VALORACIÓN DE ACTIVOS (PARA EL CASO DE RIESGOS Y OPORTUNIDADES DE SEGURIDAD DE LA INFORMACIÓN).



6.3.1 El Comité de Evaluación de Riesgos; debe identificar, clasificar y registrar los activos de información, tomando como referencia las categorías indicadas en el Anexo 6 "Categorización de los activos de la información".

6.3.2 Efectúa la tasación de activos de información, de acuerdo a las escalasestablecidas en el Anexo 7 "Escala para la tasación de activos".

6.3.3 Así mismo, en esta etapa se efectuará la clasificación de los activos de tipo información, de acuerdo a lo señalado en el Anexo 08: Clasificación de la Información.

6.3.4 El Comité de Evaluación de Riesgos, deberá asegurarse que los activos con escalas de tasación Alto y Muy Alto ingresen a la siguiente etapa de identificación de riesgos y oportunidades según lo descrito en el Anexo N° 9 – Criterios de selección de activos.

6.4 IDENTIFICACIÓN DE RIESGOS Y OPORTUNIDADES

6.4.1 El Comité de Evaluación de Riesgos, en coordinación con el personal encargado de su ejecución, efectuará el relevamiento de los riesgos u oportunidades asociados a cada proceso dentro del alcance tomando en consideración catalizadores como: cambios en los objetivos o estrategias de negocio, cambios en las normas legales, cambios en los procesos, cambios en el Sistema de Gestión, resultados de las revisiones independientes o revisiones por la Dirección, resultados de las auditorías, eventos o incidentes, resultados de la revisión o seguimiento de indicadores, resultados de la matriz de riesgos anteriores, propuestas de mejora, entre otros.

6.4.2 Adicionalmente, se detallará para cada riesgo u oportunidad el proceso en donde fue identificado y los datos considerados en el Anexo N° 3 - Formato de Análisis y Evaluación de Riesgos y Oportunidades.

6.5 ANÁLISIS DE RIESGOS Y OPORTUNIDADES

6.5.1 El Comité de Evaluación de Riesgos; en coordinación con el personal que ejecuta el proceso, realizarán el análisis de riesgo y oportunidades con la finalidad de establecer su valor de acuerdo a los criterios de probabilidad e impacto considerados en los Anexos 10 y 11 respectivamente.

6.5.2 Asimismo, también se completarán los datos en indicados en el Anexo N' 3 - Formato de Análisis y Evaluación de Riesgos y Oportunidades.

6.5.3 El valor del riesgo o el nivel de exposición (riesgo inherente) se calculará automáticamente de la relación de probabilidad / impacto según el Anexo 12 – Cálculo del nivel de riesgo.

6.6 EVALUACIÓN DE RIESGOS Y OPORTUNIDADES

ZED ILO
ANALISTA DE SISTEMAS

6.6.1 El Comité de Evaluación de Riesgos; en coordinación con el personal que ejecuta el proceso, efectuarán la evaluación de riesgos.

6.6.2 Los riesgos de valor Muy alto y Alto deberán contar con un Plan de Tratamiento de riesgos y oportunidades.

6.6.3 Los riesgos por debajo del valor Alto se consideran tolerables o aceptables para la organización y no se requiere un Plan de Tratamiento de Riesgos, sin embargo, serán evaluados por lo menos una vez al año o en el siguiente ciclo de gestión de riesgos y oportunidades para verificar si continúan con los valores de probabilidad e impacto estimados.

6.6.4 La formalización de la información proporcionada se efectuará en el Anexo N- 3 Formato de Evaluación de Riesgos y Oportunidades, contando con la conformidad de los participantes y del dueño o propietario del proceso.

6.7 TRATAMIENTO DE RIESGO Y OPORTUNIDADES

6.7.1 El Comité de Evaluación de Riesgos; en coordinación con el personal que ejecuta el proceso, determinará la estrategia de tratamiento a seguir y los controles a implementar (de corresponder) para cada riesgo no tolerable utilizando el anexo N- 4 "Formato de Plan de tratamiento y seguimiento a los riesgos y oportunidades":

Nota: La Estrategia de tratamiento se deberá seleccionar de acuerdo a lo establecido en el Anexo 13 "Estrategias para el tratamiento de riesgos y oportunidades"

6.7.2 Efectuar la evaluación de los controles en el formato indicado en el Anexo 5 – Formato de evaluación de controles tomando en consideración los criterios mencionados en el Anexo 14 – Criterios de Evaluación de Controles.

6.7.3 Calcular del riesgo residual que será igual al riesgo inherente menos el resultado de la evaluación del control.

6.7.4 Para el caso de los riesgos no tolerables que se determinen aceptar se deberá contar con la conformidad expresa del Propietario de Riesgos o el Comité encargado del seguimiento", en el que se indique la justificación de no aplicar otra estrategia de tratamiento. Esta conformidad se puede dar a través de un acta u otro documento.

6.7.5 El propietario del riesgo o el comité que corresponda, deberá aprobar formalmente el plan de tratamiento de riesgo, así como comunicar y difundir su aprobación mediante Oficio a los responsables de la implementación de los controles y enviar copia al Comité de Evaluación de Riesgos.

6.7.6 Para el caso de los riesgos de seguridad de la información, El Comité de Evaluación de Riesgosdeberá generar/actualizar la declaración de aplicabilidad de acuerdo al alcance establecido dentro del Sistema de Gestión de Seguridad de la Información.

6.8 SEGUIMIENTO A LA IMPLEMENTACIÓN

6.8.1 El Comité de Evaluación de Riesgos, efectuará el seguimiento periódico al Plan deTratamiento del Riesgo considerando para ello los siguientes estados:

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

6.8.2 Después de implementadas las acciones de tratamiento de un riesgo u oportunidad, un Auditor Interno de la especialidad, evaluará laeficacia de las acciones tomadas para tratar los riesgos y oportunidades a fin de asegurarse que sean eficaces en su diseño y operación, asignado los siguientes estados según el resultado de su evaluación:

CIERRE NO EFICAZ	Se consignará este estado cuando ya se concluyó la implementación de las acciones de tratamiento del riesgo o controles
	Se considera a aquellas acciones desestimadas. Se deberá justificar esta decisión, actualizar la estrategia de tratamiento y el valor de riesgo residual, de corresponder.

Nota: Esta evaluación podrá efectuarla a través de la medición de indicadores.

6.8.3 El Comité de Evaluación de Riesgos, al término de un ciclo de riesgos o por lo menos dos veces al año informará a la Gerencia General o al Comité correspondiente el resultado de análisis, evaluación y tratamiento de los riesgos, así como el estado de las acciones consideradas en el Plan de tratamiento.

VII. DISPOSICIONES FINALES

7.1 El propietario del riesgo deberá de aprobar el Plan de tratamiento de riesgos y aceptar los riesgos residuales referentes.

7.2 Los titulares de los órganos involucrados, así como el Comité de Evaluación de Riesgos, deberá de velar por preservar la confidencialidad, integridad y disponibilidad de la información dentro del alcance del Sistema de Gestión de Seguridad (SGSI) de la Información de ZED ILO.

VIII. VIGENCIA

La presente Directiva, entrará en vigencia al día siguiente de ser emitida la Resolución que aprueba.

IX. APROBACIÓN

La presente Directiva y sus anexos serán aprobados mediante Resolución de Gerencia General.

ZED ILO
ANALISTA DE SISTEMAS

ANEXO N° 1
DEFINICIÓN DE TÉRMINOS

Activo: Bienes, recursos o derechos que presentan valor para la organización. Activo de la información es cualquier componente (sea humano, tecnológico, software, etc.) que sustenta uno o más procesos de negocios de una unidad o área de negocio.

Análisis de Riesgo/Oportunidades: Proceso para comprender la naturaleza del riesgo/ oportunidad y que permite determinar el nivel que le corresponde.

Comité de Gestión de Seguridad de la Información (CGSI): Es el comité conformado por el Gerente y los responsables de los órganos de la entidad, con la función de gestionar la seguridad de la información en la institución.

Comité de Evaluación de Riesgos: *Comité* conformado por la Dirección de Promoción y Desarrollo, área de Tesorería y área de Informática

Confidencialidad: Garantizar que la información sea accesible únicamente para quienes tengan acceso autorizado

Consecuencia (Impacto): Resultado de una ocurrencia o cambio, que afecta a la consecución de los objetivos.

Control: Medida que modifica un riesgo

Disponibilidad: Garantizar que los usuarios autorizados tengan acceso a la información y activos asociados cuando sea necesario.

Evaluación de Riesgo/Oportunidades: Proceso de comparación de los resultados del análisis del riesgo con los criterios de riesgo para determinar si el riesgo y/o su magnitud son aceptables o tolerables.

Gestión de Riesgos: Proceso de identificación, análisis, evaluación, tratamiento y comunicación de los riesgos a las partes interesadas.

Gestor de Riesgos: Personal designado por el CGSI para la implementación y mantenimiento del Sistema de Gestión, responsable de coordinar la gestión de riesgos. Para el caso de los riesgos de seguridad de la información, corresponder al encargado de la Oficina de Informática desempeñar el Rol de Gestor de Riesgos.

Integridad:Salvaguardar la exactitud e integridad de la información y activos asociados.
Nivel de Riesgo: Magnitud de un riesgo o combinación de riesgos, expresados en términos de la combinación de las consecuencias y de su probabilidad.

Información Sensitiva: *A nivel seguridad informática la información sensitivo es aquella que se relaciona o que puede llegar a mover fibras sensibles: número de cuenta bancaria, de tarjetas de crédito, contraseñas, apellidos de familiares, domicilio detallado, propiedades, etc.*

Oportunidad: Aquello que nos permite crear o preservar el valor de un proceso, servicio o negocio.

Probabilidad: Posibilidad de que algún hecho ocurra.

Proceso: Conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados.

Propietario del Activo: Es el órgano responsable por la gestión, desarrollo, mantenimiento, uso y seguridad del activo.

Propietario del Riesgo: Area u Oficina de ZED ILO que tiene la responsabilidad y autoridad para gestionar el riesgo.

Responsable de Seguridad: Personal de ZED ILO asignado por el órgano al cual pertenece, con el propósito de gestionar los aspectos referentes a la seguridad de la información de los procesos que son responsables.

Riesgo: Efecto de la incertidumbre sobre el logro de los objetivos. El riesgo se puede expresar también en términos de combinación de las consecuencias de un suceso (incluyendo los cambios en las circunstancias) de su probabilidad de ocurrencia. El riesgo puede ser positivo (oportunidad) o negativo, aquello que permite crear o preservar el valor así como destruir o dejar de generar valor.

ZED ILO ANALISTA DE SISTEMAS

Riesgo Inherente: Es el riesgo en su estado natural, antes de considerar los controles que tenga asociados. Este se obtiene del producto de la probabilidad de que se materialice y el impacto que podría ocasionar.

Riesgo Residual: Riesgo remanente después del tratamiento del Riesgo.

Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información adicionalmente puede involucrarse otras propiedades, tales como autenticidad, responsabilidad, no repudio y confiabilidad.

Sistema de Gestión de Seguridad de la Información: Parte del sistema de gestión global, basada en un enfoque de riesgo del negocio, para establecer, implementar, operar, realizar seguimiento, revisar, mantener y mejorar la seguridad de la información.
Tratamiento del Riesgo: Es un proceso destinado a modificar el riesgo.

ANEXO N° 2

FORMATO DE GESTION DE ACTIVOS DE LA INFORMACION

ZED ILO	VERSION		FORMATO
			GESTION DE ACTIVOS DE LA INFORMACION
FECHA	N° DE PAGINA		

ITEM	CODIGO DE ACTIVO	DESCRIPCION	FUNCION	UBICACIÓN	PROPIETARIO	CLASIFICACION INTERNO/PUBLICO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	TASACION

Elaborado por: Oficina de Informática de ZED ILO

ZED ILO
ANALISTA DE SISTEMAS

ANEXO N° 3

ANALISIS Y EVALUACION DE RIESGOS

ZED ILO	VERSION	FORMATO
FECHA	N° DE PAGINA	ANALISIS Y EVALUACION DE RIESGOS Y OPORTUNIDADES

ITEM	RIESGO IDENTIFICADO	UBICACIÓN DEL RIESGO	PROPIETARIO	CAUSA	NIVEL DE IMPACTO		
	(Descripción)	(Indicar el proceso donde se genera el riesgo)	(Área u Oficina responsable de dar respuesta o tratamiento al riesgo	(Describir el origen de la generación del riesgo)	ALTO	MEDIO	BAJO

Elaborado por: Oficina de Informática de ZED ILO

ZED ILO
ANALISTA DE SISTEMAS

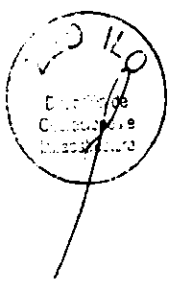
ANEXO N° 4

PLAN DE TRATAMIENTO Y SEGUIMIENTO DE RIESGOS

ZED ILO	VERSION	FORMATO
		PLAN DE TRATAMIENTO Y SEGUIMIENTO DE RIESGOS
FECHA	N° DE PAGINA	

ITEM	PROYECTO	CODIGO DEL RIEGO	ESTRATEGIAS	ACCIONES A IMPLEMENTAR	INDICADOR		
	(Descripción)	(De acuerdo al código del anexo 3)		(Describir el origen de la generación del riesgo)	ALTO	MEDIO	BAJO

Elaborado por: Oficina de Informática de ZED ILO



ANEXO N° 5

EVALUACION DE CONTROLES

ZED ILO	VERSION	FORMATO
		EVALUACION DE CONTROLES
FECHA	N° DE PAGINA	

ITEM	PROYECTO	FECHA DE EVALUACION	TIPO (Preventivo, correctivo, detectivo)	NIVEL DE AUTOMATIZACION	FRECUENCIA	INDICADORES	DOCUMENTACION DE CONTROL

Elaborado por: Oficina de Informática de ZED ILO

ZED ILO
ANALISTA DE SISTEMAS

ANEXO N° 6
CATEGORIZACIÓN DE LOS ACTIVOS DE LA INFORMACIÓN

ACTIVOS PRIMARIOS

Los activos primarios son los procesos e información central de la actividad de la institución. Se clasifican en:

a. Procesos y actividades del negocio

Son considerados los procesos centrales, los cuales giran sobre el core del negocio de la institución. Si estos procesos se interrumpieran sería imposible llevar a cabo la misión de la institución.

- ✓ Procesos que, si se modifican, pueden afectar a gran escala el logro de la misión de la organización.
- ✓ Procesos que son necesarios para que la institución cumpla con los requisitos contractuales, legales o regulatorios.

b. Información

La información primaria comprende:

- ✓ Información vital para el ejercicio de la misión en los negocios de la institución.
- ✓ Información estratégica necesaria para lograr los objetivos definidos de la institución.
- ✓ Información de alto costo cuya recolección, almacenamiento, procesamiento y transmisión requieren tiempo largo y/o involucran un alto costo de adquisición.

Nota: La información puede estar contenida en formato impreso (Políticas, procedimientos, manuales, resoluciones, etc.) o en formato electrónico.

ZED ILO ANALISTA DE SISTEMAS

ACTIVOS DE APOYO

Son aquellos activos que dan soporte a los activos primarios. De verse afectados por algún riesgo, éstos repercuten en dichos activos. Se clasifican en:

a. **Hardware:** Integrado por todos los elementos físicos que apoyan a los procesos. Entre ellos se tienen: equipo portátil, equipo fijo, periféricos (impresora, disco removible), medios para almacenamiento de datos (CD ROM, memoria USB, disco duro removible, cinta).

b. **Software:** Consiste de todos los programas que contribuyen con la operación de un conjunto de procesamiento de datos. Entre ellos se tienen:

i. **Sistema operativo:** Incluye todos los programas de una computadora que constituye la base operativa desde la cual se corren todos los demás programas (servicios o aplicaciones).

ii. **Software de servicio, mantenimiento o administración:** Software caracterizado por el hecho que complementa los servicios del sistema operativo y no está directamente al servicio de los usuarios o aplicaciones.

iii. **Software en paquetes o software estándar:** Son productos completos que proporcionan servicios a los usuarios y aplicaciones, pero no están personalizados o no son específicos como sí lo son las aplicaciones de negocios. Ejemplos: software de administración de base de datos, software de mensajería electrónica, software de directorios, software para servidores de web, entre otros.

iv. **Aplicación empresarial:** Software comercial diseñado para brindar a los usuarios acceso directo a los servicios y funciones que requieren de su sistema de información en su contexto profesional. Ejemplos: software de cuentas, software de atención al cliente, entre otros.

c. **Red y comunicaciones:** Consiste de todos los dispositivos de red y telecomunicaciones que se usan para interconectar varias computadoras físicamente remotas o elementos de un sistema de operación. Ejemplos: router, swicht, enlace de comunicaciones VPN, cableado de red y estructurado.

d. **Servicios tecnológicos:** Son aquellos servicios a nivel de tecnología de la información que buscan responder a las necesidades de los clientes internos de la institución. Ejemplos: Servicio de correo electrónico, Servicio web, Servicio de base de datos entro otros.

e. **Medio de soporte:** Consiste en todo aquellos medios donde soporte información física y electrónica Ejemplos: Dispositivo de USB, disco óptico (CD, DVD), disco duro o externo, cinta magnética, etc. así como gaveta, armario, etc.

f. **Personal:** Consiste de todos los grupos de personas involucradas en el sistema informático.

g. **Sitio:** Comprende todos los lugares que contienen el alcance o parte del alcance y los medios físicos requeridos para que opere. Ejemplos: establecimientos, edificios, oficinas, zona de acceso reservado, zona segura, entre otros.

h. **Servicios públicos:** Servicios y medios (fuentes y cableado) requeridos para proveer energía al equipo de la información y periféricos. Ejemplos: suministro de energía eléctrica, suministro de agua, entre otros.

i. **Organización:** El tipo referente a organización describe el marco organizativo, consistente de todas las estructuras de personal asignadas a una tarea y los procedimientos que controlan estas estructuras. Ejemplos: órgano administrativo, gerencias, entre otros.

ZED ILO
ANALISTA DE SISTEMAS

ANEXO N° 7

ESCALA PARA LA TASACIÓN DE ACTIVOS

Para la tasación de activos utilizaremos la siguiente escala:

Tabla N°1

MUY BAJO	1
BAJO	2
MEDIO	3
ALTO	4

Elaborado por: Oficina de Informática de ZED ILO

La descripción se definirá por cada proceso

CONSIDERACIONES PARA LA TASACIÓN DE ACTIVOS

Teniendo en cuenta la escala anterior y la descripción de cada una, se valora cada uno de los activos, identificando los impactos que generarían la pérdida de la Confidencialidad (C), Integridad (I) y Disponibilidad (D) de la información dentro del alcance del Sistema de Gestión de Seguridad de la Información; para ello se utilizará las siguientes preguntas:

a. **PARA CONFIDENCIALIDAD:**
   ¿Qué implicancia tendría para el desarrollo del proceso que el activo fuera conocido por personas no autorizadas?

b. **PARA INTEGRIDAD:**
   ¿Qué implicancia tendría para el desarrollo del proceso que el activo fuera modificado por personas no autorizadas?

c. **PARA DISPONIBILIDAD:**
   ¿Qué implicancia tendría para el desarrollo del proceso que el activo no estuviera disponible cuando se requiera?

ZED ILO ANALISTA DE SISTEMAS

Nota: Adicionalmente, para la tasación de activos se deberá tener en cuenta lo siguiente:

- ✓ Los activos son tazados sin tener en consideración la existencia de controles (políticas, mecanismos respaldos de los activos, planes de contingencia y otros).
- ✓ Para la valoración de un activo, se considera la dependencia que puede tener en relación con otros activos, ya que esto puede influenciar en los valores de dicho activo.
- ✓ La valoración puede ser realizada durante entrevistas o talleres con el personal involucrado dentro del alcance establecido dentro del SGSI.

El cálculo del valor de tasación de los activos será efectuado considerando el mayor valor obtenido en cuanto a la pérdida de su Confidencialidad (C), Integridad (I) y Disponibilidad (D) (Tabla N° 4).

ANEXO N° 8

CLASIFICACION DE LA INFORMACION

Los activos primarios de tipo información serán clasificados de acuerdo a lo establecido en la Ley de Transparencia y Acceso a la Información Pública.

Tabla N° 2: Clasificación de la Información

Secreta	Es información relacionada a la seguridad nacional, Planes de defensa militar contra posibles agresiones y de otros estados de fuerzas irregulares militarizadas internas y/o externas, planes de inteligencia y contrainteligencia, planes de desarrollo técnico y tecnológico militar y cuya revelación originaria riesgo a la integridad territorial y de las personas, así como a la subsistencia del sistema democrático.
Reservada	Es información relacionada para prevenir y reprimir la criminalidad en el país las cuales pudieran comprender planes de operaciones policiales y de inteligencia, información diplomática y consular cuya revelación no autorizada originaría un riesgo a la seguridad e integridad territorial del estado y la defensa nacional en el ámbito interno y externo y/o la subsistencia del sistema democrático.
Confidencial	Es información relacionada a la institución; del tipo secreto bancario, industrial, tecnológico, bursátil datos personales cuyo acceso y divulgación no autorizado originaria riesgos asociados a incumplimientos legales, operativos y reputaciones contra la institución.
Pública	Es información relacionada a la institución que dejo de ser secreta y/o reservada o que siempre fue publica, de acuerdo a lo estipulado en la Ley de Transparencia y Acceso a la Información Pública. Esta información debe ser publicada y/o entregada por la institución a los interesados.

Elaborado: Tomado de la Ley de Transparencia y Acceso a la Información pública

Adicionalmente, la información relacionada a Datos Personales, deberá clasificar según lo siguiente:

Tabla N° 3: Clasificación de la Datos Personales

CLASIFICACIÓN DE LA INFORMACIÓN	
DATO PERSONAL	Toda información sobre una persona natural que la identifica o la haceidentificable a través de medios que pueden ser razonablemente utilizados
DATO SENSIBLE	Datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual.

Elaborado: Tomado de la Ley de Protección de Datos Personales

ZED ILO
ANALISTA DE SISTEMAS

ANEXO N° 9
CRITERIOS DE SELECCIÓN DE ACTIVOS

Los activos a considerar en la etapa de análisis y evaluación de riesgos u oportunidades serán aquellos cuyo valor obtenido en la tasación es mayor o igual a cuatro (4) o de acuerdo a lo establecido en cada proceso.

Tabla N° 4: Selección de Activos				
ACTIVOS	**CONFIDENCIALIDAD**	**INTEGRIDAD**	**DISPONIBILIDAD**	**TASACION**
Activo 1				
Activo 2				
...				

Elaborado por: Oficina de Informática de ZED ILO

ZED ILO
ANALISTA DE SISTEMAS

ANEXO N° 10

ESCALAS DE PROBABILIDAD DE OCURRENCIA DEL RIESGO U OPORTUNIDAD

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

Tabla N° 5: Escala para el cálculo de la probabilidad de ocurrencia

Valor	Probabilidad de ocurrencia del riesgo	Descripción
1	Muy Baja	• Que no haya ocurrido. • Es poco probable que ocurra en los próximos 5 años. • No existen condiciones para su materialización.
2	Baja	• Que haya ocurrido al menos una vez en los últimos dos años. • Es probable que ocurra en los próximos dos años. • Existen controles pero pueden fallar.
3	Media	• Ha ocurrido por lo menos una vez al año • Es probable que ocurra en el siguiente año • Existen condiciones que pueden favorecen su materialización • Se cuenta con controles pero pueden ser mejorados.
4	Alta	• Ha ocurrido por lo menos una vez al mes • Existen condiciones que favorecen medianamente su materialización • No existen controles suficientes y adecuados que traten el riesgo u oportunidad.
5	Muy Alta	• Ha ocurrido por lo menos una vez a la semana • Existen condiciones que favorecen altamente su materialización • No existen controles para el tratamiento del riesgo u oportunidad.

ZED ILO
ANALISTA DE SISTEMAS