Oefa Organismo de Evaluación y Fiscalización Ambiental	**FICHA DE PROCEDIMIENTO**	Código: PA0306 Versión: ***01*** Fecha: 22/12/2022

NOMBRE DEL PROCEDIMIENTO	Gestión de riesgos de seguridad de la información

APROBACIÓN		
Nombre y cargo	**Órgano o Unidad Orgánica**	**Firma y sello**
Elaborado por: Magaly Rosa Mendoza Romero Oficial de Seguridad y Confianza Digital	Oficial de Seguridad y Confianza Digital	Oefa Organismo de Evaluación y Fiscalización Ambiental Firmado digitalmente por: MENDOZA ROMERO Magaly Rosa FAU 20521286769 soft Cargo: Oficial de Seguridad y Confianza Digital Lugar: Sede Central - Lima\Lima\Jesus Maria Motivo: Soy el autor del documento
Elaborado por: Zico Alexis Yacila Espinoza Jefe de la Oficina de Tecnologías de la Información	Oficina de Tecnologías de Información	Oefa Organismo de Evaluación y Fiscalización Ambiental Firmado digitalmente por: YACILA ESPINOZA Zico Alexis FAU 20521286769 soft Cargo: Jefe de la Oficina de Tecnologías de la Información Lugar: Sede Central - Lima\Lima\Jesus Maria Motivo: Soy el autor del documento
Revisado por: Elvis Romel Palomino Pérez Jefe de la Oficina de Planeamiento y Presupuesto	Oficina de Planeamiento y Presupuesto	Oefa Organismo de Evaluación y Fiscalización Ambiental Firmado digitalmente por: PALOMINO PEREZ Elvis Romel FAU 20521286769 soft Cargo: Jefe de la Oficina de Planeamiento y Presupuesto Lugar: Sede Central - Lima\Lima\Jesus Maria Motivo: Soy el autor del documento
Revisado por: Gonzalo Pinto Bazurco Mendoza Jefe de la Oficina de Asesoría Jurídica	Oficina de Asesoría Jurídica	Oefa Organismo de Evaluación y Fiscalización Ambiental Firmado digitalmente por: PINTO BAZURCO MENDOZA Gonzalo FAU 20521286769 soft Cargo: Jefe de la Oficina de Asesoría Jurídica Lugar: Sede Central - Lima\Lima\Jesus Maria Motivo: Soy el autor del documento

Oefa Organismo de Evaluación y Fiscalización Ambiental	**FICHA DE PROCEDIMIENTO**	Código: PA0306 Versión: ***01*** Fecha: 22/12/2022

APROBACIÓN		
Nombre y cargo	**Órgano o Unidad Orgánica**	**Firma y sello**
Aprobado por: Miriam Alegría Zevallos Gerenta General	Gerencia General	Oefa Organismo de Evaluación y Fiscalización Ambiental Firmado digitalmente por: ALEGRIA ZEVALLOS Miriam FAU 20521286769 soft Cargo: Gerenta General Lugar: Sede Central - Lima\Lima\Jesus Maria Motivo: Soy el autor del documento

CONTROL DE CAMBIOS		
Versión	**Sección del Procedimiento**	**Descripción del cambio**
00	-	Versión inicial del procedimiento[1]
01	***Base normativa, Consideraciones Generales, Actividades, Documentos que se generan***	- ***Precisiones en la base normativa y las actividades números 15.18, 19 y 20.*** - ***Se adecúa el versionamiento de los formatos a la versión del procedimiento[2].***

OBJETIVO	Establecer las actividades para identificar, evaluar, analizar y tratar los riesgos de seguridad de la información, así como realizar el seguimiento correspondiente, a fin de coadyuvar al cumplimiento de los objetivos estratégicos institucionales.
ALCANCE	El presente procedimiento es de aplicación para las áreas del OEFA que participen en la gestión de riesgos de seguridad de la información. Comprende desde la identificación de los activos de información, hasta el seguimiento a la Matriz de riesgos y la custodia de la información documentada.
RESPONSABLE DEL PROCEDIMIENTO	Jefe/a de la Oficina de Tecnologías de Información.
BASE NORMATIVA	- Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado. - Ley N° 28716, Ley de Control Interno de las entidades del Estado. - Ley N° 29733, Ley de Protección de Datos Personales. - Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital. - Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital - Decreto Supremo N° 004-2013-PCM, que aprueba la Política Nacional de Modernización de la Gestión Pública. - Decreto Supremo N° 013-2017-MINAM, que aprueba el Reglamento de Organización y Funciones del Organismo de Evaluación y Fiscalización Ambiental - OEFA. - Decreto Supremo N° 123-2018-PCM, que aprueba el Reglamento del Sistema Administrativo de Modernización de la Gestión Pública - Decreto Supremo N° 029-2021-PCM que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías

[1] Aprobado por Resolución de Gerencia General N° 0063-2022-OEFA/GEG, del 25 de mayo de 2022.

[2] ***Modificado por Resolución de Gerencia General N° 00114-2022-OEFA/GEG de fecha 22 de diciembre de 2022.***

	- Decreto Supremo N° 157-2021-PCM, Decreto Supremo que aprueba el Reglamento del Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital. - ***Decreto Supremo N° 103-2022-PCM, Decreto Supremo que aprueba la Política Nacional de Modernización de la Gestión Pública al 2030.*** - Resolución de Contraloría N° 146-2019-CG que aprueba la Directiva N° 006-2019-CG/INTEG *"Implementación del Sistema de Control Interno en las Entidades del Estado"*. - Resolución de la Comisión de Normalización y de Fiscalización de Barreras Comerciales No Arancelarias N° 129-2014/CNB-INDECOPI, que aprueba, entre otras Normas Técnicas Peruanas, la 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. Sistemas de gestión de seguridad de la información. Requisitos. 2ª Edición"*, en todas las entidades integrantes del Sistema Nacional de Informática. - Resolución de Secretaría de Gestión Pública N° 006-2018-PCM-SGP, que aprueba la Norma Técnica N° 001-2018-SGP *"Norma Técnica para la implementación de la gestión por procesos en las entidades de la administración pública"*. - Resolución de Presidencia del Consejo Directivo N° 071-2018-OEFA/PCD, que conforma el Comité de Gobierno Digital del Organismo de Evaluación y Fiscalización Ambiental - OEFA. - Resolución de Presidencia del Consejo Directivo N° 062-2019-OEFA/PCD, que designa a la Oficial de Seguridad de la Información del Organismo de Evaluación y Fiscalización Ambiental - OEFA. - Resolución de Presidencia del Consejo Directivo N° 00016-2020-OEFA/PCD, que asigna funciones a la Oficial de Seguridad de la Información del Organismo de Evaluación y Fiscalización Ambiental - OEFA. - Resolución de Presidencia del Consejo Directivo N° 00020-2022-OEFA/PCD, que aprueba la designación y funciones del Oficial de Seguridad y Confianza Digital del OEFA. - Resolución de Gerencia General N° 051-2020-OEFA/GEG, que aprueba las *"Políticas Específicas de Seguridad de la Información del Organismo de Evaluación y Fiscalización Ambiental - OEFA"*, vinculadas a la implementación 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"*. Las referidas normas incluyen sus modificatorias.
CONSIDERACIONES GENERALES	- La identificación y/o actualización de riesgos de seguridad de la información se realiza en el primer trimestre de cada año y está a cargo de los dueños de procesos. Excepcionalmente, y de resultar necesario, dicha identificación y/o actualización puede realizarse en cualquier momento del año. - El Oficial de Seguridad y Confianza Digital **y/o su alterno** realizan el acompañamiento y asesoramiento a los dueños de procesos durante el desarrollo de las actividades del presente procedimiento. - ***Ante la ausencia de el/la Oficial de Seguridad y Confianza Digital; por licencia, vacaciones, u otras razones debidamente justificadas, corresponde a el/la Oficial de Seguridad y Confianza Digital Alterno asumir dicho rol durante el desarrollo de las actividades del presente procedimiento.*** - Las revisiones y/o actualizaciones periódicas del Formato PA0306-F01: *"Matriz de riesgos de seguridad de la información"* están a cargo del Comité de Gobierno y Transformación Digital en coordinación con el/la el/la Oficial de Seguridad y Confianza Digital. - La identificación de aplicabilidad de controles de seguridad de información es realizada por el/la Oficial de Seguridad y Confianza Digital, con el soporte de los dueños de procesos quienes brindan la información para el llenado del mismo y que finalmente se plasman en el Formato PA0306-F02: *"Declaración de aplicabilidad"*. - La gestión de riesgos se realiza tomando en consideración: *(i)* las cuestiones referidas a la comprensión de la organización y su contexto, así como las necesidades y expectativas de las partes interesadas del OEFA, establecidas en el Manual del Sistema de Gestión Integrado; y, *(ii)* lo indicado en el presente procedimiento. - La identificación, análisis y tratamiento de los riesgos de seguridad de la información se realiza por cada proceso, generando como producto final de la ejecución del presente procedimiento matrices de riesgos de seguridad de información para cada caso.

	- Como parte de la creación del Sistema de Gestión de Seguridad de la Información, se realizan las asignaciones y roles pertinentes como la de propietarios de activos.
DEFINICIONES	- **Activo de información:** Conocimientos o datos que tienen valor para la Institución, viene a ser lo que una entidad valora y por lo tanto debe proteger. Estos pueden ser: los datos creados o utilizados por un proceso del OEFA, recursos o documentación (digital, papel u otro medio). - **Amenaza:** Causa potencial no deseada que daña o puede resultar en daño al sistema, a la entidad o a sus activos. Una amenaza puede ser accidental o intencional. - **Análisis de riesgos**: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. - **Áreas del OEFA:** Órganos, unidades orgánicas, coordinaciones y unidades funcionales establecidas por resolución de la Alta Dirección del OEFA. - **Atributos de los activos de información**: Características o propiedades de un activo de información utilizados para documentar o evaluar el activo de información. - **Ciclo de vida del activo de información**: Etapas por las que pasa un activo de información, desde su generación o recopilación, hasta su almacenamiento permanente o destrucción. - **Confidencialidad:** Propiedad que determina que la información no esté disponible, ni sea divulgada a personas o procesos no autorizados. - **Control:** Actividad, procedimiento, documento, política, equipo, entre otros, que permite reducir el riesgo. - **Control correctivo**: Acción que corrige total o parcialmente el impacto de una amenaza. - **Control detectivo**: Acción que detecta la ocurrencia de una amenaza. Supone que la amenaza ya se ha materializado, pero que por sí misma no corrige, detiene o mitiga el efecto. - **Control preventivo**: Acción que se encuentra involucrada dentro de los procesos y tienen como propósito evitar la ocurrencia y frecuencia de una amenaza. - **Custodio del activo de información:** Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de hacer efectiva la seguridad de los activos de información definidos por el propietario. - **Disponibilidad:** Propiedad que asegura que los usuarios autorizados tienen acceso a la información cuando la requieran. - **Dueño del riesgo:** Director/a, Subdirector/a, Jefe/a y Coordinador/a de un área del OEFA con la responsabilidad y autoridad para administrar un riesgo encontrado en los activos de información de su proceso. - **Evaluación de Riesgos**: Proceso de comparar los resultados del análisis de riesgo con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable. - **Evento**: Ocurrencia o cambio de un conjunto particular de circunstancias. Un evento puede ser una o más ocurrencias y puede tener varias causas, también puede consistir en algo que no sucede o puede ser referido como un *"incidente"* o *"accidente"*. - **Evento de seguridad de la información:** Ocurrencia identificada de un sistema o servicio que determine una posible infracción de los compromisos de Seguridad de la Información o falla de los controles, o una situación previamente desconocida que pueda ser relevante para la seguridad de la información. - **Fuente de amenaza:** Elemento o conjunto de elementos que tienen el potencial de aumentar la posibilidad de ocurrencia de una amenaza. - **Gestión integral de riesgos:** Proceso de identificación, medición, control, monitoreo, evaluación, retroalimentación y optimización de todas las situaciones que representan riesgos para la entidad. - **Gobierno digital:** Uso Estratégico de las tecnologías digitales y datos en la Administración Pública para la creación de valor público. Se sustenta en un ecosistema compuesto por actores del sector público, ciudadanos y otros interesados, quienes apoyan en la implementación de iniciativas y acciones de diseño, creación de servicios digitales y contenidos, asegurando el pleno respeto de los derechos de los ciudadanos y personas en general en el entorno digital. - **Impacto:** Resultado o efecto de un evento. El impacto de un evento puede ser positivo o negativo sobre los objetivos del OEFA. - **Incidente de Seguridad de Información:** Uno o una serie de eventos de seguridad de la información no deseados o inesperados que tiene una probabilidad significativa de comprometer las operaciones y amenazar la seguridad de la información. - **Integridad:** Propiedad de salvaguardar que la información no sufra alteraciones conservando su exactitud.

	- **Oficial de Seguridad y Confianza Digital:** Rol asignado a un/a servidor/a civil con la finalidad de supervisar que las acciones de implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información sean conformes a la NTP ISO/IEC 27001:2014. - **Probabilidad:** Posibilidad de que un evento determinado ocurra en un periodo de tiempo dado. - **Propietario de activo de información:** Alta Dirección, Director/a o Jefe/a de un órgano del OEFA que en atención a sus funciones se le ha asignado la responsabilidad de gestionar un activo de información. El término *"propietario"* no comprende el derecho de propiedad sobre el activo de información. - **Responsable de activo de la información**: Servidor/a civil del área que cuente con la responsabilidad asignada por el propietario para controlar todo el ciclo de vida de un activo en su proceso. El responsable identificado no necesariamente tiene derechos de propiedad del activo. - **Riesgo:** Efecto de la incertidumbre, posibilidad de ocurrencia de un evento adverso que afecte negativamente el logro de los objetivos del OEFA. - **Riesgo de seguridad de la información**: Probabilidad de que un incidente o una amenaza logre concretarse aprovechando una vulnerabilidad y generando un impacto en el acceso o disponibilidad de la información de la entidad que impide o retarda el logro de los objetivos. - **Riesgo inherente**: Aquel riesgo propio de la actividad y/o de sus componentes. - **Riesgo residual**: Suceso o circunstancia indeterminada que permanece como proyectado después de que se implementen las acciones de control adicionales y su seguimiento. - **Seguridad digital:** Estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas. - **Seguridad de la Información**: Preservación de la confidencialidad, integridad y disponibilidad de la información. - **Sistema de Gestión de Seguridad de la Información (SGSI):** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua - **Tecnologías digitales**: Aquellas tecnologías de la información y de comunicación, incluidos internet y dispositivos móviles, así como la analítica de datos utilizados para mejorar la generación, recopilación, intercambio, agregación, combinación, análisis, acceso, búsqueda y presentación de contenido digital, incluido el desarrollo de servicios y aplicaciones aplicables a la materia de gobierno digital. - **Tratamiento de riesgo**: Proceso mediante el cual la entidad define qué estrategia va a ejecutar para abordar un riesgo. - **Vulnerabilidad:** Debilidad o ausencia de control que puede ser explotada por una amenaza. Son características de una vulnerabilidad el hecho de que por sí sola no causa daños y, por otro lado, si no es administrada, permitirá que una amenaza genere un daño o perjuicio.
SIGLAS	- CGTD: Comité de Gobierno y Transformación Digital - OSCD: Oficial de Seguridad y Confianza Digital - SGSI: Sistema de Gestión de Seguridad de la Información - GEG: Gerencia General - OTI: Oficina de Tecnologías de la Información

REQUISITOS PARA INICIAR EL PROCEDIMIENTO	
Descripción del requisito	**Fuente**
Mapa de Procesos	Áreas del OEFA

ACTIVIDADES				**EJECUTOR**	
N°	**ACTIVIDAD**	**DESCRIPCIÓN**	**REGISTROS**	**RESPONSABLE**	**UNIDAD DE ORGANIZACIÓN**
1	Identificar y/o actualizar la información del proceso y los activos de información	Identifica y/o actualiza la información; completando la sección: 1. "*Identificación del Proceso y del Activo"* del Inventario *de activos*" del Formato PA0306-F01: *"Matriz de riesgos de seguridad de la información"*. *Nota:* *Como hoja informativa para valorar los activos de información y su relación por procesos, se usa el Anexo N° 1: "Inventario de activos" del presente procedimiento.*	Formato PA0306-F01: "*Matriz de riesgos de seguridad de la información"* sección 1. *"Identificación del Proceso y del Activo*"	Dueño del proceso	Áreas del OEFA
2	Identificar las características de los activos de información	Identifica las características de los activos de información completando la sección: 2. *"Características del Activo"* del "*Inventario de activos*" del Formato PA0306-F01: *"Matriz de riesgos de seguridad de la información"*. *Nota:* *Como hoja informativa para valorar las características de los activos de información por procesos, se usa el Anexo N° 1: "Inventario de activos" del presente procedimiento*.	Formato PA0306-F01: "*Matriz de riesgos de seguridad de la información"* sección *2. "Características del Activo"*	Dueño del proceso	Áreas del OEFA
3	Determinar la criticidad y tasación de los activos de información	Determina la criticidad y tasación de los activos de información en función de su confidencialidad, disponibilidad e integridad completando la sección 3. "*Criticidad y Tasación del Activo"* del Formato PA0306-F01: *"Matriz de riesgos de seguridad de la información".* *Nota:* *La criticidad y tasación de los activos de información se debe realizar según lo establecido en el Anexo N° 1: "Inventario de activos" del presente procedimiento.*	Formato PA0306-F01: "*Matriz de riesgos de seguridad de la información"* sección 3. *"Criticidad y Tasación del Activo"*	Dueño del proceso	Áreas del OEFA

ACTIVIDADES				**EJECUTOR**	
N°	**ACTIVIDAD**	**DESCRIPCIÓN**	**REGISTROS**	**RESPONSABLE**	**UNIDAD DE ORGANIZACIÓN**
4	Generar el código de riesgo y seleccionar el activo de información	Genera un código de riesgo Los activos de información que obtuvieron una valoración de "*alto"* y "*muy alto"*, se seleccionan y se trasladan de la hoja "*Inventario de activos"* a la hoja *"Análisis y evaluación y riesgos"* del Formato PA0306-F01: *"Matriz de riesgos de seguridad de la información".* Luego selecciona la amenaza que puede afectar al activo de información, así como la frecuencia de ocurrencia. *Nota:* *Para la generación de códigos de riesgos e identificación de amenaza y frecuencia, se usa el Anexo N° 2: "Análisis y evaluación de riesgos" del presente procedimiento.*	Formato PA0306-F01: *"Matriz de riesgos de seguridad de la información" "Análisis y Evaluación de Riesgos"*	Dueño del proceso	Áreas del OEFA
5	Identificar y registrar los controles actuales de protección	Identifica y registra los controles actuales de protección preventivos, detectivos y correctivos y el nivel de capacidad de cada control que protege al activo de información en la hoja *"Análisis y evaluación y riesgos"* del Formato PA0306-F01: *"Matriz de riesgos de seguridad de la información".* *Nota:* *Para la identificación de controles actuales, se usa el Anexo N° 2: "Análisis y evaluación de riesgos" así como la hoja "Inventario de controles" del Formato PA0306-F01"Matriz de riesgos de seguridad de la información".*	Formato PA0306-F01: *"Matriz de riesgos de seguridad de la información" "Análisis y Evaluación de Riesgos*"	Dueño del proceso	Áreas del OEFA
6	Identificar las vulnerabilidades, probabilidad de ocurrencia y descripción del riesgo	Identifica las vulnerabilidades existentes y la probabilidad de ocurrencia. Luego, describe el riesgo al que se encuentra expuesto el activo de información en la hoja *"Análisis y evaluación de riesgos"* del Formato PA0306-F01 *"Matriz de riesgos de seguridad de la*	Formato PA0306-F01: *"Matriz de riesgos de seguridad de la información" "Análisis y Evaluación de Riesgos*"	Dueño del proceso	Áreas del OEFA

ACTIVIDADES				**EJECUTOR**	
N°	**ACTIVIDAD**	**DESCRIPCIÓN**	**REGISTROS**	**RESPONSABLE**	**UNIDAD DE ORGANIZACIÓN**
		información". *Nota:* *La probabilidad de ocurrencia se obtiene de manera automática con los valores y fórmula que se indican en el Anexo N° 2: "Análisis y evaluación de riesgos" del presente procedimiento.*			
7	Evaluar el impacto y determinar el nivel de riesgo efectivo y prioridad	Evalúa el impacto en los ámbitos económico, legal, operacional e imagen que el activo de información puede ocasionar al OEFA y determina el nivel de riesgo efectivo y prioridad de tratamiento. *Nota:* *La evaluación de riesgos se realiza según el Anexo N° 2: "Análisis y evaluación de riesgos" del presente procedimiento.*	Formato PA0306-F01: *"Matriz de riesgos de seguridad de la información" "Análisis y Evaluación de Riesgos"*	Dueño del proceso	Áreas del OEFA
8	Seleccionar el código de riesgo, activo de información, amenaza y frecuencia de ocurrencia	Selecciona los activos de información que obtuvieron un nivel de riesgo de *"alto"* y *"muy alto"* y lo traslada de la hoja "*Análisis y evaluación de riesgos"* a la hoja *"Tratamiento de Riesgos"*, del Formato PA0306-F01: *"Matriz de riesgos de seguridad de la información"*, junto con la información del código de riesgo, amenazas y su frecuencia de ocurrencia.	Formato PA0306-F01: *"Matriz de riesgos de seguridad de la información" "Tratamiento de Riesgos"*	Dueño del proceso	Áreas del OEFA
9	Identificar y seleccionar el tratamiento de riesgo y los mecanismos de protección o control propuestos	Identifica y selecciona el tratamiento de riesgo a ejecutar en el activo de información, así como mecanismos de protección o los controles propuestos a implementar. *Nota 1:* *El tratamiento de riesgos se realiza según el Anexo N° 3: "Tratamiento de riesgos" del presente procedimiento.* *Nota 2:* *Para la identificación de los controles propuestos se toma en consideración los controles de seguridad de información de la hoja "Inventario de controles" de la PA0306-F01"Matriz de riesgos de seguridad de la información"*	Formato PA0306-F01: *"Matriz de riesgos de seguridad de la información" "Tratamiento de Riesgos"*	Dueño del proceso	Áreas del OEFA

ACTIVIDADES				**EJECUTOR**	
N°	**ACTIVIDAD**	**DESCRIPCIÓN**	**REGISTROS**	**RESPONSABLE**	**UNIDAD DE ORGANIZACIÓN**
10	Seleccionar y trasladar el resultado de impacto del activo que requiere tratamiento	Selecciona el resultado de la evaluación de impacto del activo que requiere un tratamiento y se trasladan de la hoja *"Análisis y evaluación de Riesgos"* a la hoja *"Tratamiento de Riesgos"* del Formato PA0306-F01: *"Matriz de riesgos de seguridad de la información".*	Formato PA0306-F01: *"Matriz de riesgos de seguridad de la información" "Tratamiento de Riesgos"*	Dueño del proceso	Áreas del OEFA
11	Identificar el nivel de riesgo residual	Identifica los niveles de riesgo residual y determina los planes de acción. **¿El nivel de riesgo residual es *"alto"* o *"muy alto"*?** **Sí:** Va a la actividad N° 12. **No:** Los niveles de riesgo residual *"bajo"* y *"medio"* se aceptan.	Formato PA0306-F01: *"Matriz de riesgos de seguridad de la información" "Tratamiento de Riesgos"*	Dueño del proceso	Áreas del OEFA
12	Identificar a los/as responsables y definir el plazo de implementación	Identifica a los/as responsables de la implementación de los controles propuestos y define el plazo de implementación, y lo traslada a los responsables de la implementación de los controles propuestos para que establezca el plan de acción.	Formato PA0306-F01: *"Matriz de riesgos de seguridad de la información" "Tratamiento de Riesgos"*	Dueño del proceso	Áreas del OEFA
13	Elaborar los planes de tratamiento y plazos de implementación	Los/as responsables de la implementación de los controles propuestos elaboran el plan de tratamiento y el plazo de implementación de los controles propuestos. Una vez definidos son comunicados a los dueños de proceso.	Formato PA0306-F01: *"Matriz de riesgos de seguridad de la información" "Tratamiento de Riesgos"*	Responsables de implementación	Áreas del OEFA
14	Identificar, analizar, evaluar y tratar la oportunidad	Identifica, analiza la oportunidad y realiza su evaluación, estimando la probabilidad y el impacto. Luego, determina el valor y el nivel de la oportunidad. Establece el tratamiento de la oportunidad cuando esta obtiene niveles **ALTO Y MUY ALTO** y las medidas de control/ acción para su tratamiento, de acuerdo con los criterios para el tratamiento de oportunidades	Formato PA0306-F03: *"Matriz de Oportunidades SGSI"* sección 3. *"Plan de acción"*	Dueño del proceso	Áreas del OEFA

ACTIVIDADES				**EJECUTOR**	
N°	**ACTIVIDAD**	**DESCRIPCIÓN**	**REGISTROS**	**RESPONSABLE**	**UNIDAD DE ORGANIZACIÓN**
		en la sección *"3.Plan de acción"*.			
15	***Remitir*** las matrices de riesgos y oportunidades de seguridad de información	***Remite, mediante correo institucional al OSCD*** la *"Matriz de riesgos de seguridad de la información"* y la *"Matriz de oportunidades SGSI"*	Correo institucional	Dueño del proceso	Áreas del OEFA
16	Elaborar el informe de sustento de la Matriz de riesgos de seguridad de la información y Matriz de oportunidades SGSI	Elaboran el informe que sustenta la Matriz de riesgos de seguridad de la información, la cual se adjunta al Informe y plan de tratamiento dirigido a la Presidencia del CGTD.	Matriz de riesgos de seguridad de la información Matriz de oportunidades SGSI Informe de sustento	OSCD Jefe/a	OTI
17	Revisar y validar la Matriz de Riesgos de seguridad de la información y Matriz de oportunidades SGSI	Revisa la hoja *"Tratamiento de Riesgos"* de la Matriz de riesgos de seguridad de la información, y Matriz de oportunidades SGSI **¿Es conforme?** **Sí:** Valida mediante acuerdo las matrices, para ello elabora el Acta de Sesión del CGTD. Va a la actividad N° 16. **No:** Va a la actividad N° 14.	Acta de sesión	CGTD	-
18	Remitir Matriz de Riesgos de seguridad de la información y Matriz de oportunidades SGSI dirigido a la GEG	Remite la Matriz de Riesgos de seguridad de la información ***que contiene la hoja del Plan de tratamiento*** de riesgos, Matriz de oportunidades SGSI, dirigido a la GEG (con copia a OPP) mediante el ***Sistema de Gestión Electrónica de Documentos***, para su validación, mediante Memorando	Memorando	Secretario/a Técnico/a	CGTD
19	Revisar y validar las Matrices de seguridad de la información	Revisa y valida mediante memorando la Matriz de riesgos y Matriz de oportunidades, y de corresponder, ***el plan de acción para el tratamiento de riesgos***. Lo comunica a la OTI.	Formato PA0306-F01: *"Matriz de riesgos de seguridad de la información"* Formato PA0306-F03: *"Matriz de oportunidades*	Gerente/a General	GEG

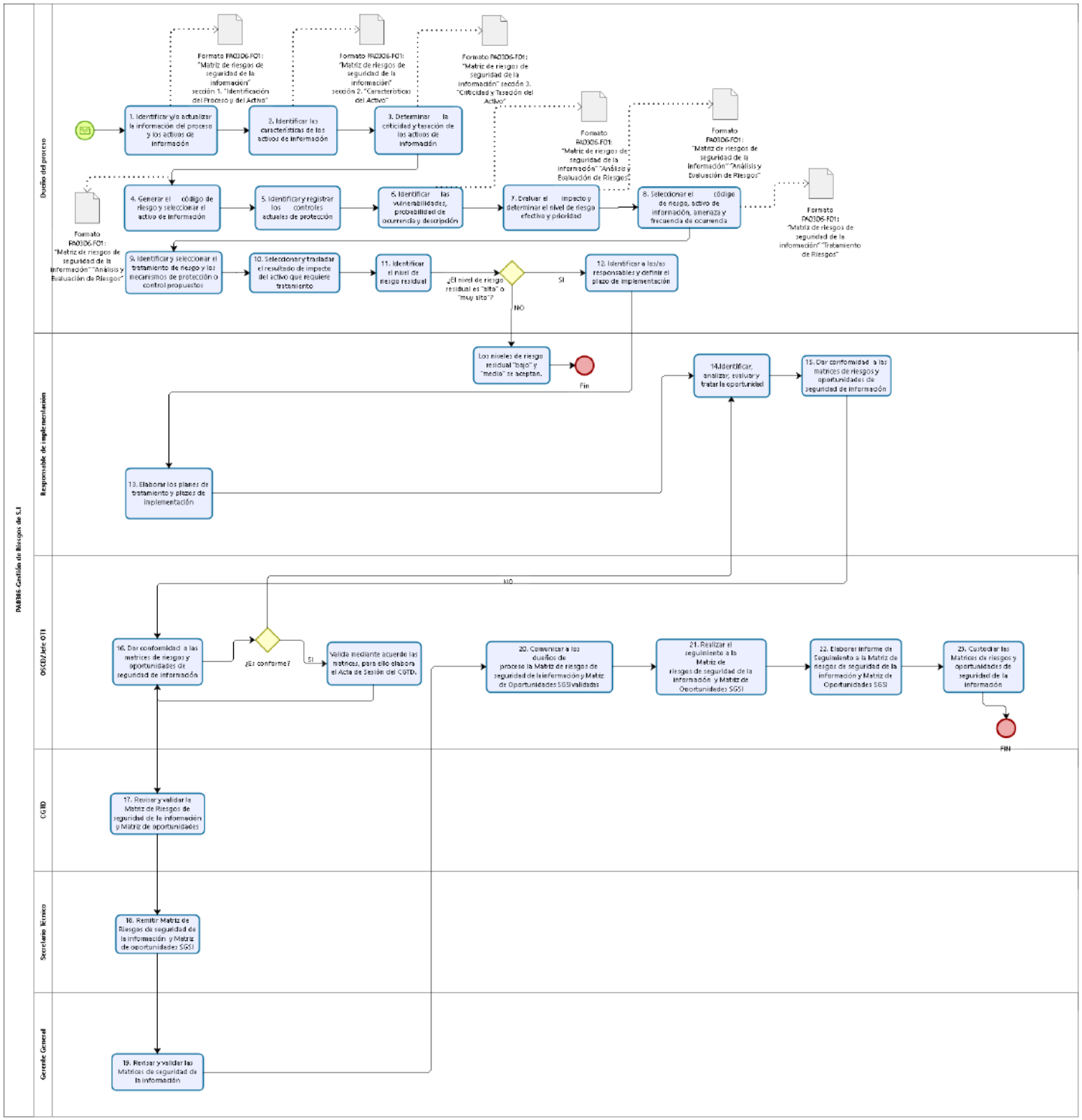
ACTIVIDADES				**EJECUTOR**	
N°	**ACTIVIDAD**	**DESCRIPCIÓN**	**REGISTROS**	**RESPONSABLE**	**UNIDAD DE ORGANIZACIÓN**
			SGSI" Memorando		
20	Comunicar a los dueños de proceso la Matriz de riesgos de seguridad de la información y Matriz de Oportunidades SGSI validadas	Comunica, mediante correo institucional, a los dueños de proceso, la Matriz de riesgos de seguridad de la información y Matriz de Oportunidades SGSI validadas, para su implementación, con copia a el/la ***OSCD*** y a la OPP.	Correo Institucional	Jefe/a	OTI
21	Realizar el seguimiento a la Matriz de riesgos de seguridad de la información y Matriz de Oportunidades SGSI	Realiza el seguimiento trimestral a la Matriz de riesgos de SGSI - hoja de *"Tratamiento de riesgos"* y Matriz de oportunidades SGSI, con respecto a las actividades planificadas y responsables asignados.	Formato PA0306-F01: *"Matriz de riesgos de seguridad de la información" "Tratamiento de Riesgos"* Formato PA0306-F03: *"Matriz de oportunidades SGSI"*	Jefe/a	OTI
22	Elaborar informe de Seguimiento a la Matriz de riesgos de seguridad de la información y Matriz de Oportunidades SGSI	Realiza el seguimiento trimestral a la Matriz de riesgos SGSI y matriz de oportunidades, a través del análisis de los resultados de los indicadores de gestión establecidos, así como el cumplimiento de las metas establecidas, de acuerdo al Anexo N° 4: *"Informe de seguimiento a la Matriz de Riesgos y oportunidades SGSI"*, el cual es remitido a la GEG dentro de los siete (07) días hábiles siguientes de concluido el trimestre.	-	Jefe/a	OTI
23	Custodiar las Matrices de riesgos y oportunidades de seguridad de la información	Custodia la carpeta compartida del SGSI, con la Matriz de riesgos y Matriz de oportunidades de seguridad de la información y sus evidencias. **Fin del procedimiento.**	-	Jefe/a	OTI

Oefa Organismo de Evaluación y Fiscalización Ambiental	**FICHA DE PROCEDIMIENTO**	Código: PA0306
		Versión: ***01***
		Fecha: 22/12/2022

DOCUMENTOS QUE SE GENERAN:
- Formato PA0306-F01: *"Matriz de riesgos de seguridad de la información"*. - Formato PA0306-F02: *"Declaración de aplicabilidad"*. - Formato PA0306-F03: *"Matriz de oportunidades SGSI"*.

ANEXOS DEL PROCEDIMIENTO:
- Anexo N° 1: *"Inventario de activos"*. - Anexo N° 2: *"Análisis y evaluación de riesgos"*. - Anexo N° 3: *"Tratamiento de riesgos"*. - Anexo N° 4: *"Informe de seguimiento a la Matriz de Riesgos y oportunidades SGSI"*.

PROCESO RELACIONADO
PA03 - Tecnologías de la Información


PA03M6 Gestión de Riesgos de S.I
Dueño del proceso
Responsable de implementación
OSCD/Jefe OTI
CGTD
Secretario Técnico
Gerente General
Formato PA03D6-FD1: "Matriz de riesgos de seguridad de la información" sección 1. "Identificación del Proceso y del Activo"
Formato PA03D6-FD1: "Matriz de riesgos de seguridad de la información" sección 2. "Características del Activo"
Formato PA03D6-FD1: "Matriz de riesgos de seguridad de la información" sección 3. "Criticidad y Tasación del Activo"
Formato PA03D6-FD1: "Matriz de riesgos de seguridad de la información" "Análisis y Evaluación de Riesgos"
Formato PA03D6-FD1: "Matriz de riesgos de seguridad de la información" "Análisis y Evaluación de Riesgos"
Formato PA03D6-FD1: "Matriz de riesgos de seguridad de la información" "Tratamiento de Riesgos"
Formato PA03D6-FD1: "Matriz de riesgos de seguridad de la información" "Análisis y Evaluación de Riesgos"
1. Identificar y/o actualizar la información del proceso y los activos de información
2. Identificar las características de los activos de información
3. Determinar la criticidad y tasación de los activos de información
4. Generar el código de riesgo y seleccionar el activo de información
5. Identificar y registrar los controles actuales de protección
6. Identificar las vulnerabilidades, probabilidad de ocurrencia y descripción
7. Evaluar el impacto y determinar el nivel de riesgo efectivo y prioridad
8. Seleccionar el código de riesgo, activo de información, amenaza y frecuencia de ocurrencia
9. Identificar y seleccionar el tratamiento de riesgo y los mecanismos de protección o control propuestos
10. Seleccionar y tratadar el resultado de impacto del activo que requiere tratamiento
11. Identificar el nivel de riesgo residual
¿El nivel de riesgo residual es "alto" o "muy alto"?
SI
NO
12. Identificar a los/as responsables y definir el plazo de implementación
Los niveles de riesgo residual "bajo" y "medio" se aceptan.
Fin
13. Elaborar los planes de tratamiento y plazos de implementación
14.Identificar, analizar, evaluar y tratar la oportunidad
15. Dar conformidad a las matrices de riesgos y oportunidades de seguridad de información
NO
16. Dar conformidad a las matrices de riesgo y oportunidades de seguridad de información
¿Es conforme?
SI
Valida mediante acuerdo las matrices, para ello elabora el Acta de Sesión del CGTD.
20. Comunicar a los dueños de procese la Matriz de riesgos de seguridad de la información y Matriz de Oportunidades SGSI validadas
21. Realizar el seguimiento a la Matriz de riesgos de seguridad de la información y Matriz de Oportunidades SGSI
22. Elaborar informe de Seguimiento a la Matriz de riesgos de seguridad de la información y Matriz de Oportunidades SGSI
23. Custodiar las Matrices de riesgos y oportunidades de seguridad de la información
FIN
17. Revisar y validar la Matriz de Riesgos de seguridad de la información y Matriz de oportunidades
18. Remitir Matriz de Riesgos de seguridad de la información y Matriz de oportunidades SGSI
19. Revisar y validar las Matrices de seguridad de la información

PASO 1. INVENTARIO DE ACTIVOS

1. Identificación del Proceso y del Activo							2. Características del Activo							3. Criticidad y Tasación del Activo				
N°	**Digite**: Código de identificación del activo	Proceso	Nombre del activo	Descripción del activo	Propietario del activo	Custodio del activo	Categoría del activo	Tipo del activo	Clasificación del uso del activo	Frecuencia de uso del activo	Tipo de ubicación del activo	Ubicación del activo	Requisito legal, reglamentario o contractual	Confidencialidad	Disponibilidad	Integridad	Valor del Activo	Nivel de Tasación
1	ACT_TI_001	PA03 TECNOLOGÍAS DE LA INFORMACIÓN	Informe de Supervisión	Documento que detalla las actividades y resultados de la Supervisión	Supervisión	Administrador de Archivo	Físicos	Información escrita	Confidencial	Mensual	Física	Archivo de la Dirección	Si, Legal	4	4	4	4.00	Muy Alto
2	ACT_TI_002	PA03 TECNOLOGÍAS DE LA INFORMACIÓN	Storage	Dispositivo de almacenamiento de datos	Gestor de Infraestructura y Comunicaciones	Administrador de Comunicaciones	Físicos	Medio de almacenamiento	Confidencial	Diario	Física	Data Center		3	2	2	2.33	Alto
3	ACT_TI_003	PA03 TECNOLOGÍAS DE LA INFORMACIÓN	Servicio de custodia de Cintas de Backup	Empresa de custodia de activos	Gestor de Infraestructura y Comunicaciones	Administrador de Comunicaciones	Servicios	Otros servicios	Confidencial	Semanal	Física	Data Center		1	1	1	1.00	Bajo
4	ACT_TI_004	PA03 TECNOLOGÍAS DE LA INFORMACIÓN	Routers Switches	Equipos de comunicaciones de redes LAN	Gestor de Infraestructura y Comunicaciones	Administrador de Comunicaciones	Físicos	Equipo de comunicaciones	Confidencial	Diario	Física	Data Center		2	2	2	2.00	Medio
5																		
6																		
7																		
8																		
9																		
10																		
11																		
12																		
13																		
14																		
15																		
16																		
17																		
18																		
19																		
20																		
21																		
22																		
23																		
24																		
25																		
26																		
27																		
28																		
29																		
30																		
31																		
32																		
33																		
34																		
35																		
36																		
37																		
38																		
39																		
40																		
41																		
42																		
43																		
44																		
45																		
46																		
47																		
48																		
49																		
50																		

PASO 2. ANÁLISIS DE RIESGOS

PASO 3. EVALUACIÓN DE RIESGOS

	ACTIVO	AMENAZA		MECANISMO DE PROTECCIÓN O CONTROL ACTUAL						VULNERABILIDAD		PROBABILIDAD DE OCURRENCIA		RIESGO	EVALUACIÓN DE IMPACTO					RIESGO EFECTIVO		
Código del Riesgo	Activo	Descripción de la Amenaza	Frecuencia de Amenaza	Preventivo	Nivel de Capacidad	Detectivo	Nivel de Capacidad	Correctivo	Nivel de Capacidad	Descripción de la Vulnerabilidad	Nivel de Vulnerabilidad	Probabilidad de Ocurrencia	Nivel de Probabilidad de Ocurrencia	**Descripción del Evento Adverso (Riesgo) *Amenaza +Activo + Vulnerabilidad**	Impacto Económico	Impacto Legal	Impacto Operacional	Impacto a la Imagen	Nivel de Impacto	**Nivel de exposición al riesgo**	**Nivel de Riesgo**	**Prioridad**
PM04 - R - 01	Informe de Supervisión	Incendio	2	Charlas de seguridad	3	Detectores de Humo	4	Sistema de extinción de fuego manual	4	Falta de mantenimiento preventivo	1.3	1.667	Medio	Incencio del informe de supervisión por falta de mantenimiento preventivo	4	1	4	1	2.5	2.083	Medio	no necesita
PM04 - R - 02	Registro de supervisión	Mal funcionamiento del equipo	1	Adquisición previsoria de espacio de disco	1	-				Falta de mantenimiento preventivo	4.7	2.833	Alto	Mal funcionamiento del equipo de registro de supervisión por falta de mantenimiento preventivo	1	2	4	1	2.0	2.417	Medio	no necesita
PM04 - R - 03	Servicio de custodia de Cintas de Backup	Fallas en el servicio	1	Control mediante cargos de entrega de caja de cintas, bitácoras internas.	3	-				Falta de proceso formal de monitoreo y revisión de servicios de terceros	4.0	2.500	Alto		3	3	3	3	3.0	2.750	Alto	2
PM04 - R - 04	Routers Switches	Ataques a la Red LAN	3	Contrato de soporte y mantenimiento.	1	Supervisión mediante el servidor NAGIOS.	1	Alta disponibilidad de equipos de redes	1	Sobrecarga eléctrica	4.0	3.500	Muy Alto		3	3	3	3	3.0	3.250	Alto	2

Formato PA0306-F01
Versión: ***01***
Fecha de aprobación: 22/12/2022

PASO 4. TRATAMIENTO DE RIESGOS

		AMENAZA		TRATAMIENTO	MECANISMO DE PROTECCIÓN O CONTROL PROPUESTO						PROBABILIDAD	IMPACTO					RIESGO RESIDUAL		RESPONSABLE	TIEMPO DE IMPLEMENTACIÓN	
Código del Riesgo	Activo	Descripción de la Amenaza	Frecuencia de Amenaza	OPCIONES DE TRATAMIENTO AL RIESGO	**Preventivo**	Nivel de Capacidad	**Detectivo**	Nivel de Capacidad	**Correctivo**	Nivel de Capacidad	Nivel de Probabilidad de Ocurrencia	Impacto Económico	Impacto Legal	Impacto Operacional	Impacto a la Imagen	Nivel de Impacto	**Nivel de exposición al riesgo**	**Nivel de Tolerancia**	**Responsable de Implementación**	**Fecha Inicio**	**Fecha Fin**
	Informe de Supervisión	Incendio	4	Transferir		1		1		1	Alto	1	1	1	1	1	2.50	Medio			
											0					0	0.00	0			
											0					0	0.00	0			
											0					0	0.00	0			

Formato PA0306-F01
Versión: ***01***
Fecha de aprobación: 22/12/2022

N°	ACTIVO	AMENAZA	CRITERIOS DE EVALUACIÓN						RIESGO EFECTIVO	
			Impacto				Probabilidad de Ocurrencia del Riesgo	Relevancia del Activo (Valor del Activo)	Nivel de Exposición al Riesgo	Nivel de Riesgo
			Impacto Legal	Impacto Económico /Imagen Institucional	Impacto Operacional	Nivel de Impacto				
AMENAZAS A LOS ACTIVOS DE INFORMACIÓN										
AMENAZAS A LOS ACTIVOS DE SOFTWARE										
AMENAZAS A LOS ACTIVOS FÍSICOS										
AMENAZAS A LOS SERVICIOS										
AMENAZAS AL PERSONAL (CLIENTES, EMPLEADOS, PERSONAL EXTERNO)										

Tabla de Vulnerabilidades

CÓDIGO	VULNERABILIDAD	CÓDIGO Y VULNERABILIDAD	CATEGORÍA
VU1	Mantenimiento insuficiente / instalación fallida de medios de almacenamiento	VU1 - Mantenimiento insuficiente / instalación fallida de medios de almacenamiento	Hardware
VU2	Falta de esquemas de reemplazo periódicos	VU2 - Falta de esquemas de reemplazo periódicos	
VU3	Susceptibilidad a la humedad, al polvo y a la suciedad	VU3 - Susceptibilidad a la humedad, al polvo y a la suciedad	
VU4	Sensibilidad a la radiación electromagnética	VU4 - Sensibilidad a la radiación electromagnética	
VU5	Falta de control eficiente del cambio de configuración	VU5 - Falta de control eficiente del cambio de configuración	
VU6	Susceptibilidad a variación de voltaje	VU6 - Susceptibilidad a variación de voltaje	
VU7	Susceptibilidad a variaciones de temperatura	VU7 - Susceptibilidad a variaciones de temperatura	
VU8	Almacenamiento no protegido	VU8 - Almacenamiento no protegido	
VU9	Falta de cuidado al descartarlo	VU9 - Falta de cuidado al descartarlo	
VU10	Equipo desfasado por vigencia tecnológica	VU10 - Equipo desfasado por vigencia tecnológica	
VU11	Pruebas al software inexistentes o insuficientes	VU11 - Pruebas al software inexistentes o insuficientes	Software
VU12	Errores conocidos en el software	VU12 - Errores conocidos en el software	
VU13	No hacer "logout" cuando se sale de la estación de trabajo	VU13 - No hacer "logout" cuando se sale de la estación de trabajo	
VU14	Disposición o reutilización de medios de almacenamiento sin borrar apropiadamente	VU14 - Disposición o reutilización de medios de almacenamiento sin borrar apropiadamente	
VU15	Falta de evidencia de auditoria	VU15 - Falta de evidencia de auditoria	
VU16	Asignación equivocada de derechos de acceso	VU16 - Asignación equivocada de derechos de acceso	
VU17	Software ampliamente distribuido	VU17 - Software ampliamente distribuido	
VU18	Aplicar programas de aplicación a datos incorrectos en términos del tiempo	VU18 - Aplicar programas de aplicación a datos incorrectos en términos del tiempo	
VU19	Interfaz de usuario complicada	VU19 - Interfaz de usuario complicada	
VU20	Falta de documentación	VU20 - Falta de documentación	
VU21	Seteo incorrecto de parámetros	VU21 - Seteo incorrecto de parámetros	
VU22	Fechas incorrectas	VU22 - Fechas incorrectas	
VU23	Falta de mecanismos de identificación y autentificación como la autentificación de usuarios	VU23 - Falta de mecanismos de identificación y autentificación como la autentificación de usuarios	
VU24	Tablas de claves no protegidas	VU24 - Tablas de claves no protegidas	
VU25	Mala administración de claves	VU25 - Mala administración de claves	
VU26	Habilitación de servicios innecesarios	VU26 - Habilitación de servicios innecesarios	
VU27	Software inmaduro o nuevo	VU27 - Software inmaduro o nuevo	
VU28	Especificaciones no claras o incompletas para los desarrolladores	VU28 - Especificaciones no claras o incompletas para los desarrolladores	
VU29	Falta de control de cambios eficaz	VU29 - Falta de control de cambios eficaz	
VU30	Descarga y uso incontrolado de software	VU30 - Descarga y uso incontrolado de software	
VU31	Falta de copias de respaldo	VU31 - Falta de copias de respaldo	
VU32	No producir informes de gestión	VU32 - No producir informes de gestión	
VU33	Falta de pruebas de envió o recepción de mensaje	VU33 - Falta de pruebas de envió o recepción de mensaje	Red
VU34	Líneas de comunicación no protegidas	VU34 - Líneas de comunicación no protegidas	
VU35	Tráfico delicado no protegido	VU35 - Tráfico delicado no protegido	
VU36	Juntas malas en el cableado	VU36 - Juntas malas en el cableado	
VU37	Punto de falla única	VU37 - Punto de falla única	
VU38	Falta de identificación y autentificación del destinatario	VU38 - Falta de identificación y autentificación del destinatario	
VU39	Arquitectura de red insegura	VU39 - Arquitectura de red insegura	
VU40	Transferencia de claves en claro	VU40 - Transferencia de claves en claro	
VU41	Gestión inadecuada de la red	VU41 - Gestión inadecuada de la red	

CÓDIGO	VULNERABILIDAD	CÓDIGO Y VULNERABILIDAD	CATEGORÍA
VU42	Conexiones no protegidas de la red publica	VU42 - Conexiones no protegidas de la red publica	
VU43	Ausencia del personal	VU43 - Ausencia del personal	Personal
VU44	Procedimientos inadecuados del reclutamiento	VU44 - Procedimientos inadecuados del reclutamiento	
VU45	Capacitación de seguridad insuficiente	VU45 - Capacitación de seguridad insuficiente	
VU46	Uso incorrecto del software y hardware	VU46 - Uso incorrecto del software y hardware	
VU47	Falta de conciencia de seguridad	VU47 - Falta de conciencia de seguridad	
VU48	Falta de mecanismos de monitoreo	VU48 - Falta de mecanismos de monitoreo	
VU49	Trabajo no supervisado del personal externo o de limpieza	VU49 - Trabajo no supervisado del personal externo o de limpieza	
VU50	Falta de políticas para el uso correcto de medios de telecomunicaciones y mensajería	VU50 - Falta de políticas para el uso correcto de medios de telecomunicaciones y mensajería	
VU51	Uso inadecuado o negligente del control de acceso físico a edificios y ambientes	VU51 - Uso inadecuado o negligente del control de acceso físico a edificios y ambientes	Sitio
VU52	Ubicaciones en una área susceptible a las inundaciones	VU52 - Ubicaciones en una área susceptible a las inundaciones	
VU53	Red inestable de energía eléctrica	VU53 - Red inestable de energía eléctrica	
VU54	Falta de protección física del edificio, puertas y ventanas	VU54 - Falta de protección física del edificio, puertas y ventanas	
VU55	Falta de un procedimiento formal para el registro y baja de usuarios	VU55 - Falta de un procedimiento formal para el registro y baja de usuarios	Institución
VU56	Falta de proceso formal para revisar el derecho de acceso (supervisión)	VU56 - Falta de proceso formal para revisar el derecho de acceso (supervisión)	
VU57	Disposiciones inexistentes o insuficientes (respecto de la seguridad) en contratos con clientes y/o terceros	VU57 - Disposiciones inexistentes o insuficientes (respecto de la seguridad) en contratos con clientes y/o terceros	
VU58	Falta de procedimientos de monitoreo de instalaciones de procesamiento de la información	VU58 - Falta de procedimientos de monitoreo de instalaciones de procesamiento de la información	
VU59	Falta de auditorías regulares (supervisión)	VU59 - Falta de auditorías regulares (supervisión)	
VU60	Falta de procedimientos de identificación y evaluación del riesgo	VU60 - Falta de procedimientos de identificación y evaluación del riesgo	
VU61	Falta de informes de fallas registradas en los registros del administrador y del operador	VU61 - Falta de informes de fallas registradas en los registros del administrador y del operador	
VU62	Respuesta inadecuada del mantenimiento del servicio	VU62 - Respuesta inadecuada del mantenimiento del servicio	
VU63	Inexistencia o insuficiencia de acuerdo sobre el nivel de servicio	VU63 - Inexistencia o insuficiencia de acuerdo sobre el nivel de servicio	
VU64	Falta de procedimiento de control de cambios	VU64 - Falta de procedimiento de control de cambios	
VU65	Falta de procedimiento formal para el control de la documentación de la institución	VU65 - Falta de procedimiento formal para el control de la documentación de la institución	
VU66	Falta de procedimiento formal para la supervisión del registro de la institución	VU66 - Falta de procedimiento formal para la supervisión del registro de la institución	
VU67	Falta de proceso formal para autorización de información pública disponible	VU67 - Falta de proceso formal para autorización de información pública disponible	
VU68	Falta de asignación apropiada de responsabilidades de seguridad en la información	VU68 - Falta de asignación apropiada de responsabilidades de seguridad en la información	
VU69	Falta de planes de continuidad	VU69 - Falta de planes de continuidad	
VU70	Falta de una política de uso de correos electrónicos	VU70 - Falta de una política de uso de correos electrónicos	
VU71	Falta de procedimientos para introducir software en sistemas operativos	VU71 - Falta de procedimientos para introducir software en sistemas operativos	
VU72	Faltas de registro en los historiales del administrador y del operador	VU72 - Faltas de registro en los historiales del administrador y del operador	
VU73	Falta de procedimientos para manejo de la información clasificada	VU73 - Falta de procedimientos para manejo de la información clasificada	
VU74	Falta de responsabilidades sobre la seguridad de la información en las descripciones de puestos	VU74 - Falta de responsabilidades sobre la seguridad de la información en las descripciones de puestos	
VU75	Ausencia o insuficiencia de disposiciones (concernientes a la seguridad de la información en contratos con empleados)	VU75 - Ausencia o insuficiencia de disposiciones (concernientes a la seguridad de la información en contratos con empleados)	
VU76	Falta de proceso disciplinario definido en caso de incidentes en la seguridad de la información	VU76 - Falta de proceso disciplinario definido en caso de incidentes en la seguridad de la información	
VU77	Falta de política formal sobre el uso de computadoras portátiles	VU77 - Falta de política formal sobre el uso de computadoras portátiles	
VU78	Falta de control de activos que se encuentran fuera del local	VU78 - Falta de control de activos que se encuentran fuera del local	
VU79	Inexistencia o insuficiencia de la política de "escritorio despejado y pantalla despejada"	VU79 - Inexistencia o insuficiencia de la política de "escritorio despejado y pantalla despejada"	
VU80	Falta de autorización al acceso a las instalaciones de procesamiento de la información	VU80 - Falta de autorización al acceso a las instalaciones de procesamiento de la información	
VU81	Falta de mecanismos de monitoreo establecidos para las rupturas de la seguridad	VU81 - Falta de mecanismos de monitoreo establecidos para las rupturas de la seguridad	
VU82	Falta de revisiones regulares de la gestión	VU82 - Falta de revisiones regulares de la gestión	
VU83	Falta de procedimientos para reportar debilidades en la seguridad	VU83 - Falta de procedimientos para reportar debilidades en la seguridad	

CÓDIGO	VULNERABILIDAD	CÓDIGO Y VULNERABILIDAD	CATEGORÍA
VU84	Falta de procedimientos sobre el cumplimiento de disposiciones respecto de derechos intelectuales	VU84 - Falta de procedimientos sobre el cumplimiento de disposiciones respecto de derechos intelectuales	
VU85	Falta de política formal sobre el uso de dispositivos de almacenamiento removibles	VU85 - Falta de política formal sobre el uso de dispositivos de almacenamiento removibles	
VU86	Falta de cuidado en el traslado	VU86 - Falta de cuidado en el traslado	
VU87	Inexistente clasificación y disposiciones sobre el tratamiento de la información	VU87 - Inexistente clasificación y disposiciones sobre el tratamiento de la información	
VU88	Documentos almacenados en mobiliario no protegido	VU88 - Documentos almacenados en mobiliario no protegido	
VU89	Información almacenada en disco duro o USB no protegida	VU89 - Información almacenada en disco duro o USB no protegida	
VU90	Falta de procedimiento formal para el otorgamiento y control de llaves en la organización	VU90 - Falta de procedimiento formal para el otorgamiento y control de llaves en la organización	
VU91	Contratos inadecuados / Inexistencia de contratos	VU91 - Contratos inadecuados / Inexistencia de contratos	
VU92	Insuficientes mecanismos de monitoreo	VU92 - Insuficientes mecanismos de monitoreo	
VU93	Falta de procedimiento formal de rotación o cambio de puesto	VU93 - Falta de procedimiento formal de rotación o cambio de puesto	
VU94	Parche no instalado correctamente	VU94 - Parche no instalado correctamente	
VU95	Problemas del proveedor respecto a los componentes del servicio	VU95 - Problemas del proveedor respecto a los componentes del servicio	
VU96	Falta de proceso formal de monitoreo y revisión de servicios internos y/o de terceros	VU96 - Falta de proceso formal de monitoreo y revisión de servicios internos y/o de terceros	
VU97	Falta de personal capacitado / Personal poco capacitado	VU97 - Falta de personal capacitado / Personal poco capacitado	
VU98	Falta de pruebas periódicas de restauración	VU98 - Falta de pruebas periódicas de restauración	
VU99	Falta de procedimiento de rehuso y eliminación segura de equipos y medios	VU99 - Falta de procedimiento de rehuso y eliminación segura de equipos y medios	
VU100	Inadecuadas condiciones y controles ambientales	VU100 - Inadecuadas condiciones y controles ambientales	
VU101	Falta de procedimiento de organización y funcionamiento de los archivos de la organización	VU101 - Falta de procedimiento de organización y funcionamiento de los archivos de la organización	
VU102	Falta de políticas de uso aceptable de activos de información	VU102 - Falta de políticas de uso aceptable de activos de información	
VU103	Inadecuado ambiente físico	VU103 - Inadecuado ambiente físico	
VU104	Falta de procedimiento formal de Ingreso al Data Center	VU104 - Falta de procedimiento formal de Ingreso al Data Center	
VU105	Personal de tecnología de la información mediante requerimiento formal extrae la información directamente de la base de datos	VU105 - Personal de tecnología de la información mediante requerimiento formal extrae la información directamente de la base de datos	
VU106	Perfiles inadecuados para los cargos	VU106 - Perfiles inadecuados para los cargos	
VU107	Log de trazabilidad limitado	VU107 - Log de trazabilidad limitado	
VU108	Falta de proceso formal para revisar los usuarios y perfiles	VU108 - Falta de proceso formal para revisar los usuarios y perfiles	
VU109	Ingreso / actualización de información por personal que no corresponde	VU109 - Ingreso / actualización de información por personal que no corresponde	
VU110	Documentos almacenados en carpeta sin respaldo	VU110 - Documentos almacenados en carpeta sin respaldo	
VU111	Versión desactualizada del software	VU111 - Versión desactualizada del software	
VU112	No se cuenta con soporte local	VU112 - No se cuenta con soporte local	
VU113	Equipos no cuentan con garantía	VU113 - Equipos no cuentan con garantía	
VU114	Acceso directo, lógico y controlado por parte del proveedor al aplicativo	VU114 - Acceso directo, lógico y controlado por parte del proveedor al aplicativo	
VU115	Documentación del sistema inexistente o desactualizada	VU115 - Documentación del sistema inexistente o desactualizada	
VU116	Falta de una depuración adecuada del buzón de correo	VU116 - Falta de una depuración adecuada del buzón de correo	
VU117	Falta de proceso formal para revisar la adecuada asignación de tamaño del buzón de correo	VU117 - Falta de proceso formal para revisar la adecuada asignación de tamaño del buzón de correo	
VU118	Falta actualización del Sistema Operativo (parche) o firmware	VU118 - Falta actualización del Sistema Operativo (parche) o firmware	
VU119	Recursos insuficientes de hardware	VU119 - Recursos insuficientes de hardware	
VU120	Software obsoleto	VU120 - Software obsoleto	
VU121	Pruebas insuficientes luego de instalado el software	VU121 - Pruebas insuficientes luego de instalado el software	
VU122	Falta de control para el manejo de las licencias	VU122 - Falta de control para el manejo de las licencias	
VU123	Ausencia de procesos y documentación formal de Gestión (Proyectos, Mantenimientos, Incidencias) y/o Ciclo de Vida de Desarrollo de Software y/o Estándares de Programación	VU123 - Ausencia de procesos y documentación formal de Gestión (Proyectos, Mantenimientos, Incidencias) y/o Ciclo de Vida de Desarrollo de Software y/o Estándares de Programación	
VU124	Falta de un formal planeamiento de la capacidad para la proyección y dimensionamiento de los recursos	VU124 - Falta de un formal planeamiento de la capacidad para la proyección y dimensionamiento de los recursos	
VU125	Acceso directo del personal de Sistemas a la base de datos con privilegios de lectura	VU125 - Acceso directo del personal de Sistemas a la base de datos con privilegios de lectura	

CÓDIGO	VULNERABILIDAD	CÓDIGO Y VULNERABILIDAD	CATEGORÍA
VU126	Falta de monitoreo de actividades de las cuentas administradoras	VU126 - Falta de monitoreo de actividades de las cuentas administradoras	
VU127	Falta de eliminación o modificación de información personal o confidencial utilizada para pruebas	VU127 - Falta de eliminación o modificación de información personal o confidencial utilizada para pruebas	
VU128	Ausencia de ambiente para certificación similar al ambiente de producción	VU128 - Ausencia de ambiente para certificación similar al ambiente de producción	
VU129	Inadecuado control del código fuente	VU129 - Inadecuado control del código fuente	
VU130	Disposición o reutilización de equipos sin borrar apropiadamente	VU130 - Disposición o reutilización de equipos sin borrar apropiadamente	
VU131	Inadecuada disponibilidad de la documentación del sistema	VU131 - Inadecuada disponibilidad de la documentación del sistema	
VU132	Falta de solicitud de la adquisición / desarrollo / mantenimiento de software al área responsable (Tecnología de la Información)	VU132 - Falta de solicitud de la adquisición / desarrollo / mantenimiento de software al área responsable (Tecnología de la Información)	
VU133	Falta de comunicación de la adquisición / desarrollo / mantenimiento de software al Responsable de Seguridad de la Información para emitir opinión sobre los riesgos inherentes y/o impacto en la seguridad de la Información de la institución	VU133 - Falta de comunicación de la adquisición / desarrollo / mantenimiento de software al Responsable de Seguridad de la Información para emitir opinión sobre los riesgos inherentes y/o impacto en la seguridad de la Información de la institución	
VU134	Falta de comunicación adecuada de los eventos y debilidades de seguridad de la información	VU134 - Falta de comunicación adecuada de los eventos y debilidades de seguridad de la información	
VU135	Los colaboradores y terceros no están al tanto de sus responsabilidades para reportar los incidentes relativos a la seguridad de la información	VU135 - Los colaboradores y terceros no están al tanto de sus responsabilidades para reportar los incidentes relativos a la seguridad de la información	
VU136	Falta de planes de continuidad (Plan de recuperación de desastres / plan de contingencias) actualizados	VU136 - Falta de planes de continuidad (Plan de recuperación de desastres / plan de contingencias) actualizados	
VU137	Capacitación y entrenamiento en el uso del sistema insuficientes	VU137 - Capacitación y entrenamiento en el uso del sistema insuficientes	
VU138	Bloqueo de procesos	VU138 - Bloqueo de procesos	
VU139	Recursos de hardware insuficientes	VU139 - Recursos de hardware insuficientes	
VU140	Errores en la Migración	VU140 - Errores en la Migración	
VU141	Falta de control sobre la entrada y/o salida de datos	VU141 - Falta de control sobre la entrada y/o salida de datos	
VU142	Insuficientes pruebas de funcionamiento de software	VU142 - Insuficientes pruebas de funcionamiento de software	
VU143	Errores metodológicos en la ejecución de pruebas del software (planificación/procedimientos)	VU143 - Errores metodológicos en la ejecución de pruebas del software (planificación/procedimientos)	
VU144	Sobrecarga transaccional	VU144 - Sobrecarga transaccional	
VU145	Incorrecta configuración	VU145 - Incorrecta configuración	
VU146	Pocos profesionales especializados en la solución	VU146 - Pocos profesionales especializados en la solución	
VU147	Falta de redundancia activa (Fuente A y B)	VU147 - Falta de redundancia activa (Fuente A y B)	
VU148	Información almacenada en medio no protegido (USB Personal, Google Drive personal)	VU148 - Información almacenada en medio no protegido (USB Personal, Google Drive personal)	
VU149	Inadecuada supervisión de servicios de terceros	VU149 - Inadecuada supervisión de servicios de terceros	
VU150	Error humano no intencional	VU150 - Error humano no intencional	
VU151	Inadecuadas condiciones ambientales	VU151 - Inadecuadas condiciones ambientales	
VU152	Incumplimiento de los mecanismos de monitoreo	VU152 - Incumplimiento de los mecanismos de monitoreo	
VU153	Falta de redundancia activa (MAIN y BKP)	VU153 - Falta de redundancia activa (MAIN y BKP)	
VU154	Incumplimiento de disposiciones respecto a la clasificación, etiquetado y tratamiento de los activos de información	VU154 - Incumplimiento de disposiciones respecto a la clasificación, etiquetado y tratamiento de los activos de información	
VU155	Inadecuada revisión del cumplimiento del procedimiento formal de altas, bajas y modificaciones de puesto	VU155 - Inadecuada revisión del cumplimiento del procedimiento formal de altas, bajas y modificaciones de puesto	
VU156	Inadecuado planeamiento de la capacidad para la proyección y dimensionamiento de los recursos	VU156 - Inadecuado planeamiento de la capacidad para la proyección y dimensionamiento de los recursos	
VU157	Climatización de confort	VU157 - Climatización de confort	
VU158	Inadecuado proceso disciplinario definido en caso de incidentes en la seguridad de la información	VU158 - Inadecuado proceso disciplinario definido en caso de incidentes en la seguridad de la información	
VU159	Alta rotación de personal	VU159 - Alta rotación de personal	
VU160	Constantes cambios organizacionales	VU160 - Constantes cambios organizacionales	
VU161	Capacitación de seguridad insuficiente para el SGSI de la organización	VU161 - Capacitación de seguridad insuficiente para el SGSI de la organización	
VU162	Falta de pruebas de restauración periódicas	VU162 - Falta de pruebas de restauración periódicas	
VU163	Electricidad mal proyectada	VU163 - Electricidad mal proyectada	
VU164	Falta de redundancia de fuentes de energía	VU164 - Falta de redundancia de fuentes de energía	
VU165	Inadecuado procedimiento definido para la gestión de incidentes de seguridad de la información	VU165 - Inadecuado procedimiento definido para la gestión de incidentes de seguridad de la información	

CÓDIGO	VULNERABILIDAD	CÓDIGO Y VULNERABILIDAD	CATEGORÍA
VU166	Mantenimiento Insuficiente de Base de Datos	VU166 - Mantenimiento Insuficiente de Base de Datos	
VU167	Inadecuados Planes de Contingencia	VU167 - Inadecuados Planes de Contingencia	
VU168	Cableado Estructurado Desorganizado	VU168 - Cableado Estructurado Desorganizado	
VU169	Inadecuada transferencia de conocimiento al personal que da soporte y mantenimiento	VU169 - Inadecuada transferencia de conocimiento al personal que da soporte y mantenimiento	
VU170	Inadecuado soporte y mantenimiento del software	VU170 - Inadecuado soporte y mantenimiento del software	
VU171	Renovación de licencias extemporáneas	VU171 - Renovación de licencias extemporáneas	
VU172	No contar con un segundo proveedor de enlaces de comunicaciones	VU172 - No contar con un segundo proveedor de enlaces de comunicaciones	
VU173	Obsolescencia Tecnológica	VU173 - Obsolescencia Tecnológica	
VU174	Falta de comunicación de la adquisición / desarrollo / mantenimiento de software al Oficial de Seguridad de la Información para emitir opinión sobre los riesgos	VU174 - Falta de comunicación de la adquisición / desarrollo / mantenimiento de software al Oficial de Seguridad de la Información para emitir opinión sobre los riesgos	
VU175	Inoportuna actualización de los manuales del sistema	VU175 - Inoportuna actualización de los manuales del sistema	
VU176	Falta de comunicación adecuada de los incidentes de seguridad de la información	VU176 - Falta de comunicación adecuada de los incidentes de seguridad de la información	
VU177	Ausencia de programador(es) con conocimiento del Sistema	VU177 - Ausencia de programador(es) con conocimiento del Sistema	
VU178	Falta de procedimiento formal de rotación o cambio de puesto	VU178 - Falta de procedimiento formal de rotación o cambio de puesto	
VU179	Falta o Inadecuada Actualización del Software	VU179 - Falta o Inadecuada Actualización del Software	
VU180	Falta de estándares de desarrollo seguro	VU180 - Falta de estándares de desarrollo seguro	
VU181	Falta de un esquema de balanceo de carga	VU181 - Falta de un esquema de balanceo de carga	
VU182	Falta de un esquema de alta disponibilidad	VU182 - Falta de un esquema de alta disponibilidad	
VU183	Inadecuado soporte a usuarios	VU183 - Inadecuado soporte a usuarios	
VU184	Errores en el software de terceros	VU184 - Errores en el software de terceros	**Propias del negocio**
VU185	Inadecuada limpieza del ambiente físico	VU185 - Inadecuada limpieza del ambiente físico	
VU186	Falta de procedimiento formal de Ingreso al Archivo	VU186 - Falta de procedimiento formal de Ingreso al Archivo	
VU187	Inadecuados controles de acceso físico	VU187 - Inadecuados controles de acceso físico	
VU188	Inadecuado mobiliario archivístico (estantes, archivadores verticales, etc.)	VU188 - Inadecuado mobiliario archivístico (estantes, archivadores verticales, etc.)	
VU189	Falta de adecuado ambiente físico para almacenar documentos	VU189 - Falta de adecuado ambiente físico para almacenar documentos	
VU190	Problemas de comunicación con el servidor de correo institucional	VU190 - Problemas de comunicación con el servidor de correo institucional	
VU191	Falta de proceso formal de monitoreo y revisión de servicios de terceros	VU191 - Falta de proceso formal de monitoreo y revisión de servicios de terceros	
VU192	Incorrecta configuración del equipo físico	VU192 - Incorrecta configuración del equipo físico	
VU193	Corte de energía eléctrica	VU193 - Corte de energía eléctrica	
VU194	Falta de procedimiento definido para la gestión de incidentes de seguridad de la información	VU194 - Falta de procedimiento definido para la gestión de incidentes de seguridad de la información	
VU195	Bancos de batería insuficientes	VU195 - Bancos de batería insuficientes	
VU196	Dependencia de proveedor de servicio público	VU196 - Dependencia de proveedor de servicio público	
VU197	Bajo presupuesto destinado a la adquisición de licencias de software	VU197 - Bajo presupuesto destinado a la adquisición de licencias de software	
VU198	Ausencia de un instructivo de instalación	VU198 - Ausencia de un instructivo de instalación	
VU199	Falta de un sistema de aire acondicionado adecuado	VU199 - Falta de un sistema de aire acondicionado adecuado	
VU200	Ausencia de sistemas automatizados contra incendio	VU200 - Ausencia de sistemas automatizados contra incendio	
VU201	Falta de política formal sobre el uso de telefonía celular	VU201 - Falta de política formal sobre el uso de telefonía celular	
VU202	Correo electrónico institucional configurado en celular particular	VU202 - Correo electrónico institucional configurado en celular particular	
VU203	Inadecuado cumplimiento de disposiciones respecto a la confidencialidad de la información	VU203 - Inadecuado cumplimiento de disposiciones respecto a la confidencialidad de la información	
VU204	Insuficientes mecanismos de supervisión/monitoreo	VU204 - Insuficientes mecanismos de supervisión/monitoreo	
VU205	Almacenamiento inadecuado	VU205 - Almacenamiento inadecuado	
VU206	Inadecuado control de calidad	VU206 - Inadecuado control de calidad	
VU207	Uso de papel reciclado conteniendo información sensible	VU207 - Uso de papel reciclado conteniendo información sensible	

CÓDIGO	VULNERABILIDAD	CÓDIGO Y VULNERABILIDAD	CATEGORÍA
VU208	Documentos con información sensible permanecen desatendidos en impresoras o fotocopiadoras	VU208 - Documentos con información sensible permanecen desatendidos en impresoras o fotocopiadoras	
VU209	Pérdida de línea de vista con el equipo radio enlace remoto	VU209 - Pérdida de línea de vista con el equipo radio enlace remoto	
VU210	Falta de personal backup en posiciones clave	VU210 - Falta de personal backup en posiciones clave	
VU211	Falta de políticas de uso de activos de información	VU211 - Falta de políticas de uso de activos de información	
VU212	Incumplimiento de políticas de uso de activos de información	VU212 - Incumplimiento de políticas de uso de activos de información	
VU213	Falta de implementación de funcionalidad en la aplicación	VU213 - Falta de implementación de funcionalidad en la aplicación	
VU214	Extracción de data directamente de la base de datos	VU214 - Extracción de data directamente de la base de datos	
VU215	Ingreso / actualización de data directamente a la base de datos	VU215 - Ingreso / actualización de data directamente a la base de datos	
VU216	Volúmenes altos de documentos	VU216 - Volúmenes altos de documentos	
VU217	Eliminación no segura del documento	VU217 - Eliminación no segura del documento	
VU218	Intermitencia de datos	VU218 - Intermitencia de datos	
VU219	Software almacenado en equipo	VU219 - Software almacenado en equipo	
VU220	Falta de tratamiento de archivos e información de clientes inactivos	VU220 - Falta de tratamiento de archivos e información de clientes inactivos	
VU221	Falta de personal con conocimientos similares (alta especialización)	VU221 - Falta de personal con conocimientos similares (alta especialización)	
VU222	Errores en el respaldo y/o restauración de información	VU222 - Errores en el respaldo y/o restauración de información	
VU223	Falta de implementación de mecanismos de seguridad	VU223 - Falta de implementación de mecanismos de seguridad	
VU224	Inadecuada difusión y comunicación de la política de "escritorio despejado y pantalla despejada"	VU224 - Inadecuada difusión y comunicación de la política de "escritorio despejado y pantalla despejada"	
VU225	Procedimiento incompleto de baja de usuario o cambio de cuenta	VU225 - Procedimiento incompleto de baja de usuario o cambio de cuenta	
VU226	Planes de contingencia no formalizados	VU226 - Planes de contingencia no formalizados	
VU227	Falta de control de logs de acceso	VU227 - Falta de control de logs de acceso	
VU228	Falta de mecanismos de seguridad eléctrica	VU228 - Falta de mecanismos de seguridad eléctrica	
VU229	Falta de organización de carpetas compartidas	VU229 - Falta de organización de carpetas compartidas	
VU230	Falta de mecanismos de seguridad	VU230 - Falta de mecanismos de seguridad	
VU231	Falta de devolución de todos los activos de la organización en su poder al término de su empleo, contrato o acuerdo	VU231 - Falta de devolución de todos los activos de la organización en su poder al término de su empleo, contrato o acuerdo	
VU232	Falta de eliminación o ajuste de los derechos de acceso luego de cambios en la relación laboral	VU232 - Falta de eliminación o ajuste de los derechos de acceso luego de cambios en la relación laboral	
VU233	Falta de equipamiento o soluciones de Prevención de Pérdida de Información	VU233 - Falta de equipamiento o soluciones de Prevención de Pérdida de Información	
VU234	Insuficientes mecanismos de seguridad perimetral e interna	VU234 - Insuficientes mecanismos de seguridad perimetral e interna	
VU235	Falta de control de licenciamiento de software	VU235 - Falta de control de licenciamiento de software	
VU236	Inadecuada instalación	VU236 - Inadecuada instalación	
VU237	Limpieza inadecuada	VU237 - Limpieza inadecuada	
VU238	Incumplimiento de requisitos establecidos en las normas eléctricas	VU238 - Incumplimiento de requisitos establecidos en las normas eléctricas	
VU239	Pérdida de las llaves de cifrado	VU239 - Pérdida de las llaves de cifrado	
VU240	Inadecuado almacenamiento de documentos de clientes (servidor publicado en internet)	VU240 - Inadecuado almacenamiento de documentos de clientes (servidor publicado en internet)	
VU241	Inadecuado control de versiones del archivo en excel	VU241 - Inadecuado control de versiones del archivo en excel	
VU242	Uso de instrucciones no compatibles con software (Microsoft excel)	VU242 - Uso de instrucciones no compatibles con software (Microsoft excel)	
VU243	Archivo contiene información en texto claro de las conexiones a la base de datos	VU243 - Archivo contiene información en texto claro de las conexiones a la base de datos	
VU244	Falta de equipo de contingencia	VU244 - Falta de equipo de contingencia	
VU245	Falta de destrucción segura de documentos	VU245 - Falta de destrucción segura de documentos	
VU246	Desorden en la ubicación de la documentación	VU246 - Desorden en la ubicación de la documentación	
VU247	Falta de foliatura	VU247 - Falta de foliatura	
VU248	Errores en la impresión del formato con datos relevantes	VU248 - Errores en la impresión del formato con datos relevantes	
VU249	Falta de definición en los documentos normativos la aplicabilidad del formato	VU249 - Falta de definición en los documentos normativos la aplicabilidad del formato	

CÓDIGO	VULNERABILIDAD	CÓDIGO Y VULNERABILIDAD	CATEGORÍA
VU250	Incumplimiento de documentos normativos	VU250 - Incumplimiento de documentos normativos	
VU251	Falta de stock (formato / contrato)	VU251 - Falta de stock (formato / contrato)	
VU252	Falta de definición en los documentos normativos las firmas que corrrespondan, en caso de que el crédito tenga fiadores o avales	VU252 - Falta de definición en los documentos normativos las firmas que corrrespondan, en caso de que el crédito tenga fiadores o avales	
VU253	Inadecuada gestión de parches	VU253 - Inadecuada gestión de parches	
VU254	Falta de stock de equipos / impresoras	VU254 - Falta de stock de equipos / impresoras	
VU255	Formato inadecuado	VU255 - Formato inadecuado	
VU256	Capacitación insuficiente para el desempeño del cargo	VU256 - Capacitación insuficiente para el desempeño del cargo	
VU257	Recursos insuficientes de personal	VU257 - Recursos insuficientes de personal	
VU258	Falta de definición de los tiempos de atención internos	VU258 - Falta de definición de los tiempos de atención internos	
VU259	No contar con el sistema Hiperfirma	VU259 - No contar con el sistema Hiperfirma	
VU260	Contar con información incompleta para relacionar la garantía al crédito solicitado	VU260 - Contar con información incompleta para relacionar la garantía al crédito solicitado	
VU261	Información registrada de forma manual	VU261 - Información registrada de forma manual	
VU262	Falta de codificación del documento	VU262 - Falta de codificación del documento	
VU263	Dependencia de conexión a internet	VU263 - Dependencia de conexión a internet	
VU264	Falta de mobiliario para almacenamiento de documentos	VU264 - Falta de mobiliario para almacenamiento de documentos	
VU265	Problemas con las herramientas corporativas	VU265 - Problemas con las herramientas corporativas	
VU266	No contar con perfiles de acceso a internet	VU266 - No contar con perfiles de acceso a internet	
VU267	Inadecuada gestión de licenciamiento de software	VU267 - Inadecuada gestión de licenciamiento de software	
VU268	Falta de información actualizada	VU268 - Falta de información actualizada	
VU269	Falta de segmentación de la red	VU269 - Falta de segmentación de la red	
VU270	Falta de cumplimiento de políticas de gestión de registros de auditoría	VU270 - Falta de cumplimiento de políticas de gestión de registros de auditoría	
VU271	Inadecuados mecanismos de búsqueda de eventos en los registros de auditoría debido a arquitectura y cantidad de información	VU271 - Inadecuados mecanismos de búsqueda de eventos en los registros de auditoría debido a arquitectura y cantidad de información	
VU272	Inadecuado procedimiento para el control de accesos de usuarios	VU272 - Inadecuado procedimiento para el control de accesos de usuarios	
VU273	Falta de mantenimiento formal de la base de datos	VU273 - Falta de mantenimiento formal de la base de datos	
VU274	Falta de controles en la estructura de los datos	VU274 - Falta de controles en la estructura de los datos	
VU275	No contar con equipos redundantes	VU275 - No contar con equipos redundantes	
VU276	Falta de revisión periódica de la información documentada	VU276 - Falta de revisión periódica de la información documentada	
VU277	Insuficientes recursos de hardware	VU277 - Insuficientes recursos de hardware	
VU278	Falta de protección de datos de prueba	VU278 - Falta de protección de datos de prueba	
VU279	Filtro incorrecto sobre cobertura de la garantía	VU279 - Filtro incorrecto sobre cobertura de la garantía	
VU280	Personal de Agencia no cuenta con salida a correo público	VU280 - Personal de Agencia no cuenta con salida a correo público	
VU281	Falta de políticas y controles de teletrabajo	VU281 - Falta de políticas y controles de teletrabajo	
VU282	Falta de capacitación, orientación y soporte a usuarios que trabajan de manera remota	VU282 - Falta de capacitación, orientación y soporte a usuarios que trabajan de manera remota	
VU283	Falta de políticas y controles de uso de activos de información	VU283 - Falta de políticas y controles de uso de activos de información	
VU284	Falta de protección y control de la información cuando se realiza teletrabajo	VU284 - Falta de protección y control de la información cuando se realiza teletrabajo	
VU285	Falta de concientización en seguridad de la información	VU285 - Falta de concientización en seguridad de la información	

1. CAPACIDAD DE LOS CONTROLES

Nivel	Descripción
4	Los controles necesarios se encuentran implementados y permiten mitigar la amenaza.
3	Existen controles y mitigan parcialmente la amenaza y/o reducen el impacto generado.
2	Existen controles pero no son los suficientes para mitigar la amenaza.
1	No existen controles de seguridad de la información que permitan mitigar la amenaza.

2. FRECUENCIA DE LA AMENAZA

Valor	Descripción
4	El evento podría ocurrir de manera semanal o diaria.
3	El evento podría ocurrir de manera quincenal o mensual.
2	El evento podría ocurrir entre 3 o 4 veces al año.
1	El evento podría presentarse al menos 1 vez en el año.

3. TASACION DE PROBABILIDAD

Valor	Tasación
3.01 – 4.00	Muy Alto
2.01 – 3.00	Alto
1.01 – 2.00	Medio
1.00 – 1.00	Bajo

4. IMPACTOS

Valor		Impacto Económico	Impacto Legal	Impacto Operacional	Impacto a la Imagen
4	Muy Alto(4)	Pérdidas en millones de soles	Multa o sancion por falta muy grave	No se pueden recuperar las operaciones	Deterioro de la imagen de toda la organización
3	Alto (3)	Pérdidas en cientos de miles de soles	El incumplimiento afecta la permanencia de un Directivo Multa o sanción por falta grave	Las operaciones tardan meses en reanudarse	Deterioro de la imagen de algunas áreas de la organización
2	Medio (2)	Pérdidas en miles de soles	El incumplimiento puede generar una sanción económica leve	Las operaciones tardan días en reanudarse	Deterioro de la imagen de un área de la organización
1	Bajo (1)	Pérdidas mínimas que no afeca a la Institución	El incumplimiento no afecta a la Organización	Se opera parcialmente	Afectación mínima de la imagen de la Organización

5. NIVEL DE RIESGO

Valor	Tasación
3.50 – 4.00	Muy Alto
2.51 – 3.49	Alto
1.51 – 2.50	Medio
1.00 – 1.50	Bajo

		PROBABILIDAD			
		1	2	3	4
IMPACTO	4	2.50	3.00	3.50	4.00
	3	2.00	2.50	3.00	3.50
	2	1.50	2.50	2.50	3.00
	1	1.00	1.50	2.00	2.50

PROBABILIDAD

6. TRATAMIENTO DE RIESGO

Tipo de tratamiento de Riesgo	Descripción
Evitar	Dejar de realizar la actividad que genera el riesgo debido a que el nivel de riesgo es inaceptable.
Reducir (mitigar)	Establecer controles para disminuir la probabilidad de ocurrencia del riesgo.
Transferir	Transferir a un tercero con la capacidad financiera o especialización necesaria para administrar adecuadamente el riesgo, o enfrentar las pérdidas originadas ante la ocurrencia de la adversidad. Los seguros transfieren el riesgo de pérdida financiera del asegurado al asegurador. Las transferencias parciales consisten en compartir los riesgos, dando la responsabilidad a un tercero.
Retener (aceptar)	Aceptar el riesgo en su presente nivel realizando una adecuada administración y monitoreo. Para lo cual se debe verificar que cumpla con los criterios de aceptación de riesgos definidos.

Oefa

1. PROCESO DE NIVEL 0

Proceso Nivel 0	Código
PE01	PE01 PLANEAMIENTO INSTITUCIONAL
PE02	PE02 INNOVACIÓN Y GESTIÓN POR PROCESOS
PE03	PE03 COMUNICACIONES
PE04	PE04 SOCIO AMBIENTAL
PM01	PM01 POLÍTICAS Y ESTRATEGIAS EN FISCALIZACIÓN AMBIENTAL
PM02	PM02 SUPERVISIÓN A ENTIDADES DE FISCALIZACIÓN AMBIENTAL
PM03	PM03 EVALUACIÓN AMBIENTAL
PM04	PM04 SUPERVISIÓN AMBIENTAL
PM05	PM05 FISCALIZACIÓN E INCENTIVOS
PA01	PA01 RECURSOS HUMANOS
PA02	PA02 ADMINISTRACIÓN Y FINANZAS
PA03	PA03 TECNOLOGÍAS DE LA INFORMACIÓN
PA04	PA04 ASESORÍA JURÍDICA

2. CATEGORIA DE ACTIVOS

Categoría
Información
Software
Físicos
Servicios
Personal

3. TIPO DE ACTIVO SEGUN CATEGORIA

Categoría	Tipo de activo
Información	Información electrónica
	Información escrita
	Información hablada
	Otro tipo de información
Software	Software comercial o herramientas, utilitarios
	Software desarrollado por terceros
	Software desarrollado internamente
	Software de administración de base de datos
	Otro software
Físicos	Equipo de procesamiento
	Equipo de comunicaciones
	Medio de almacenamiento
	Mobiliario y equipamiento
	Otros equipos
Servicios	Procesamiento y comunicaciones
	Servicios generales
	Otros servicios
Personal	Clientes
	Empleados
	Accionistas
	Personal Externo

4. CLASIFICACION DE USO DE ACTIVO

Clasificación de uso	Descripción de Clasificación de uso
Pública	Son todos aquellos activos que se presumen públicos, y que pueden ser accedidos tanto por miembros de la organización como por personas externas a ella (público en general), sin estar sujetos a ningún control.
Uso Interno	Son todos aquellos activos que son accedidos exclusivamente por personal interno y cuyo acceso excepcional por parte de personal externo (auditores, entidades reguladoras, consultores externos) puede darse pero se encuentra regulado y sujeto a condiciones específicas de acceso.
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 darse pero se encuentra regulado y sujeto a condiciones específicas de acceso.
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 o nivel específico de poder dentro de la organización

5. FRECUENCIA DE USO DEL ACTIVO

Frecuencia de uso
Diario
Semanal
Quincenal
Mensual
Anual
Eventual

6. UBICACIÓN DEL ACTIVO

Tipo de ubicación
Física
Lógica

7. VALORACION DEL ACTIVO

Rango de valor	Tasación
1.00 - 1.00	Bajo
1.01 - 2.00	Medio
2.01 - 3.00	Alto
3.01 - 4.00	Muy Alto

8. CRITICIDAD DEL ACTIVO

Nivel	Valor	Confidencialidad	Integridad	Disponibilidad
Muy Alto	4	La información asociada al activo sólo es accedida por la Alta Dirección, su divulgación sería catastrófica para la organización.	El activo no puede tolerar pérdida o alteración de todos sus componentes, la alteración de su integridad comprometería varios procesos de la organización.	El activo siempre debe estar disponible, pues su carencia afectaría el flujo de producción de varios procesos de la organización.
Alto	3	La información asociada al activo es restringida y sólo personal de un proyecto específico puede acceder a ella, divulgación comprometería la reputación e imagen de la organización.	El activo no puede tolerar una alteración de sus componentes, la alteración de su integridad afectaría parte de la información del proceso.	El activo no puede estar no disponible por más de un día, su carencia afectaría en la operación del proceso.
Medio	2	La información asociada al activo es confidencial o interna y sólo personal de algunas áreas internas pueden acceder a ella, su divulgación afectaría los procesos de las áreas involucradas.	El activo puede tolerar una alteración media de sus componentes, la alteración de su integridad afectaría una o más actividades importantes del proceso.	El activo puede estar no disponible por más de dos días, su carencia afectaría una o más actividades del proceso.
Bajo	1	La información asociada al activo es de uso general y cualquiera puede acceder a ella, pues no impacta a la organización.	El activo puede tolerar una alteración menor de sus componentes, la alteración de integridad afectaría una actividad menor del proceso.	El activo puede estar no disponible por mas de tres días, su carencia afectaría una actividad menor del proceso.

Control NTP ISO/IEC 27001:2014	Nombre	Descripción
A.5 Políticas de seguridad de la información		
A.5.1 Dirección de la gerencia para la seguridad de la información		
Objetivo: Proporcionar dirección y apoyo de la gerencia para la seguridad de la información en concordancia con los requisitos del negocio y las leyes y regulaciones relevantes.		
A.5.1.1	Políticas para la seguridad de la información	Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la gerencia, publicado y comunicado a los empleados y a las partes externas relevantes.
A.5.1.2	Revisión de las políticas para la seguridad de la información	Las políticas para la seguridad de la información deben ser revisadas a intervalos planificados o si ocurren cambios significativos para asegurar su conveniencia, adecuación y efectividad continua.
A.6 Organización de la seguridad de la información		
A.6.1 Organización interna		
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.		
A.6.1.1	Roles y responsabilidades para la seguridad de la información	Todas las responsabilidades de seguridad de la información deben ser definidas y asignadas.
A.6.1.2	Segregación de funciones	Las funciones y áreas de responsabilidad en conflicto deben ser segregadas para reducir oportunidades de modificación no autorizada o no intencional o mal uso de los activos de la organización.
A.6.1.3	Contacto con autoridades	Contactos apropiados con autoridades relevantes deben ser mantenidos.
A.6.1.4	Contacto con grupos especiales de interés	Contactos apropiados con grupos especiales de interés u otros foros de especialistas en seguridad y asociaciones profesionales deben ser mantenidos.
A.6.1.5	Seguridad de la información en la gestión de proyectos	La seguridad de la información debe ser tratada en la gestión de proyectos, sin importar el tipo de proyecto.
A.6.2 Dispositivos móviles y teletrabajo		
Objetivo: Asegurar la seguridad del teletrabajo y el uso de los dispositivos móviles.		
A.6.2.1	Política de dispositivos móviles	Una política y medidas de seguridad de soporte deben ser adoptadas para gestionar los riesgos introducidos por el uso de dispositivos móviles.
A.6.2.2	Teletrabajo	Una política y medidas de seguridad de apoyo deben ser implementadas para proteger información a la que se accede, se procesa o almacena en sitios de teletrabajo.
A.7 Seguridad de los recursos humanos		
A.7.1 Antes del empleo		
Objetivo: Asegurar que los empleados y contratistas entienden sus responsabilidades y son convenientes para los roles para los que se les considera.		
A.7.1.1	Investigación de antecedentes	Las verificaciones de los antecedentes de todos los candidatos a ser empleados deben ser llevadas a cabo en concordancia con las leyes, regulaciones y ética relevantes, y debe ser proporcional a los requisitos del negocio, la clasificación de la información a la que se tendrá acceso y los riesgos percibidos.
A.7.1.2	Términos y condiciones del empleo	Los acuerdos contractuales con los empleados y contratistas deben estipular responsabilidades de estos y de la organización respecto de la seguridad de la información.
A.7.2 Durante el empleo		
Objetivo: Asegurar que los empleados y contratistas sean conscientes y cumplan con sus responsabilidades de seguridad de la información.		
A.7.2.1	Responsabilidades de gestión	La gerencia debe requerir a todos los empleados y contratistas aplicar la seguridad de la información en concordancia con las políticas y procedimientos establecidos por la organización.
A.7.2.2	Conciencia, educación y capacitación sobre la seguridad de la información	Todos los empleados de la organización y, cuando fuera relevante, los contratistas deben recibir educación y capacitación sobre la conciencia de la seguridad de la información, así como actualizaciones regulares sobre políticas y procedimientos de la organización, según sea relevante para la función del trabajo que cumplen.
A.7.2.3	Proceso disciplinario	Debe haber un proceso disciplinario formal y comunicado para tomar acción contra empleados que hayan cometido una infracción a la seguridad de la información.
A.7.3 Terminación y cambio de empleo		
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.		
A.7.3.1	Terminación o cambio de responsabilidades del empleo.	Las responsabilidades y deberes de seguridad de la información que siguen siendo válidos luego de la terminación o cambio de empleo deben ser definidos, comunicados al empleado o contratista y forzar su cumplimiento.
A.8 Gestión de activos		
A.8.1 Responsabilidad por los activos		
Objetivo: Identificar los activos de la organización y definir responsabilidades de protección apropiadas.		
A.8.1.1	Inventario de activos	Información, Otros activos asociados con información e instalaciones de procesamiento de información deben ser identificados y un inventario de estos activos debe ser elaborado y mantenido.

A.8.1.2	Propiedad de los activos	Los activos mantenidos en el inventario deben ser propios.
A.8.1.3	Uso aceptable de los activos	Las reglas para el uso aceptable de la información y activos asociados con la información y con las instalaciones de procesamiento de la información deben ser identificadas, documentadas e implementadas.
A.8.1.4	Retorno de activos	Todos los empleados y usuarios de partes externas deben retornar todos los activos de la organización en su posesión a la conclusión de su empleo, contrato o acuerdo.
A.8.2 Clasificación de la información		
Objetivo: Asegurar que la información recibe un nivel apropiado de protección en concordancia con su importancia para la organización.		
A.8.2.1	Clasificación de la información	La información debe ser clasificada en términos de los requisitos legales, valor, criticidad y sensibilidad respecto a una divulgación o modificación no autorizada.
A.8.2.2	Etiquetado de la información	Un conjunto apropiado de procedimientos para el etiquetado de la información debe ser desarrollado e implementado en concordancia con el esquema de clasificación de la información adoptado por la organización.
A.8.2.3	Manejo de activos	Los procedimientos para el manejo de activos deben ser desarrollados e implementados en concordancia con el esquema de clasificación de la información adoptado por la organización.
A.8.3 Manejo de los medios		
Objetivo: Prevenir la divulgación, modificación, remoción o destrucción no autorizada de información almacenada en medios.		
A.8.3.1	Gestión de medios removibles	Se debe implementar procedimientos para la gestión de medios removibles en concordancia con el esquema de clasificación adoptado por la organización.
A.8.3.2	Disposición de medios	Se debe poner a disposición los medios de manera segura cuando ya no se requieran, utilizando procedimientos formales.
A.8.3.3	Transferencia de medios físicos	Los medios que contienen información deben ser protegidos contra el acceso no autorizado, el mal uso o la corrupción durante el transporte.
A.9 Control de acceso		
A.9.1 Requisitos de la empresa para el control de acceso		
Objetivo: Limitar el acceso a la información y a las instalaciones de procesamiento de la información.		
A.9.1.1	Política de control de acceso	Una política de control de acceso debe ser establecida, documentada y revisada basada en requisitos del negocio y de seguridad de la información.
A.9.1.2	Acceso a redes y servicios de red	Los usuarios deben tener acceso solamente a la red y a servicios de red que hayan sido específicamente autorizados a usar.
A.9.2 Gestión de acceso de usuario		
Objetivo: Asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas y servicios.		
A.9.2.1	Registro y baja de usuarios	Un proceso formal de registro y baja de usuarios debe ser implementado para permitir la asignación de derechos de acceso.
A.9.2.2	Aprovisionamiento de acceso a usuario	Un proceso formal de aprovisionamiento de acceso a usuarios debe ser implementado para asignar o revocar los derechos de acceso para todos los tipos de usuarios a todos los sistemas y servicios.
A.9.2.3	Gestión de derechos de acceso privilegiados	La asignación y uso de derechos de acceso privilegiado debe ser restringida y controlada.
A.9.2.4	Gestión de información de autentificación secreta de usuarios	La asignación de información de autentificación secreta debe ser controlada a través de un proceso de gestión formal.
A.9.2.5	Revisión de derechos de acceso de usuarios	Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares.
A.9.2.6	Remoción o ajuste de derechos de acceso	Los derechos de acceso a información e instalaciones de procesamientos de información de todos los empleados y de los usuarios de partes externas deben removerse al término de su empleo, contrato o acuerdo, o ajustarse según el cambio.
A.9.3 Responsabilidades de los usuarios		
Objetivo: Hacer que los usuarios respondan por la salvaguarda de su información de autentificación.		
A.9.3.1	Uso de información autentificación secreta	Los usuarios deben ser exigidos a que sigan las prácticas de la organización en el uso de información de autentificación secreta.
A.9.4 Control de acceso a sistema y aplicación		
Objetivo: Prevenir el acceso no autorizado a los sistemas y aplicaciones.		
A.9.4.1	Restricción de acceso a la información	El acceso a la información y a las funciones del sistema de aplicación debe ser restringido en concordancia con la política de control de acceso.
A.9.4.2	Procedimientos de ingreso seguro	Donde la política de control de acceso lo requiera, el acceso a los sistemas y a las aplicaciones debe ser controlado por un procedimiento de ingreso seguro.
A.9.4.3	Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.
A.9.4.4	Uso de programas utilitarios privilegiados	El uso de programas utilitarios que podrían ser capaces de pasar por alto los controles del sistema y de las aplicaciones debe ser restringido y controlarse estrictamente.

A.9.4.5	Control de acceso al código fuente de los programas	El acceso al código fuente de los programas debe ser restringido.
A.10 Criptografía		
A.10.1 Controles criptográficos		
Objetivo: Asegurar el uso apropiado y efectivo de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.		
A.10.1.1	Política sobre el uso controles criptográficos	Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada.
A.10.1.2	Gestión de claves	Una política sobre el uso, protección y tiempo de vida de las claves criptográficas debe ser desarrollada e implementada a través de todo su ciclo de vida.
A.11 Seguridad física y ambiental		
A.11.1 Áreas seguras		
Objetivo: Impedir acceso físico no autorizado, daño e interferencia a la información y a las instalaciones de procesamiento de la información de la organización.		
A.11.1.1	Perímetro de seguridad física	Perímetros de seguridad deben ser definidos y utilizados para proteger áreas que contienen información sensible o crítica e instalaciones de procesamiento de la información.
A.11.1.2	Controles de ingreso físico	Las áreas seguras deben ser protegidas por medio de controles apropiados de ingreso para asegurar que se le permite el acceso sólo al personal autorizado.
A.11.1.3	Asegurar oficinas, áreas e instalaciones	Seguridad física para oficinas, áreas e instalaciones debe ser diseñada e implementada.
A.11.1.4	Protección contra amenazas externas y ambientales	Protección física contra desastres naturales, ataque malicioso o accidentes debe ser diseñada y aplicada.
A.11.1.5	Trabajo en áreas seguras	Procedimientos para el trabajo en áreas seguras debe ser diseñado y aplicado.
A.11.1.6	Áreas de despacho y carga	Los puntos de acceso, como las áreas de despacho, carga y otros puntos en donde personas no autorizadas pueden ingresar al local deben ser controlados, y si fuera posible, aislarlos de las instalaciones de procesamiento de la información para evitar el acceso no autorizado.
A.11.2 Equipos		
Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos e interrupción de las operaciones de la organización.		
A.11.2.1	Emplazamiento y protección de los equipos	Los equipos deben ser ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado.
A.11.2.2	Servicios de suministro	Los equipos deben ser protegidos contra fallas de electricidad y otras alteraciones causadas por fallas en los servicios de suministro.
A.11.2.3	Seguridad del cableado	El cableado de energía y telecomunicaciones que llevan datos o servicios de información de soporte debe ser protegido de la interceptación, interferencia o daño.
A.11.2.4	Mantenimiento de equipos	Los equipos deben mantenerse de manera correcta para asegurar su continua disponibilidad e integridad.
A.11.2.5	Remoción de activos	Los equipos, la información o el software no deben ser retirados de su lugar sin autorización previa.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	La seguridad debe ser aplicada a los activos que están fuera de su lugar tomando en cuenta los distintos riesgos de trabajar fuera de las instalaciones de la organización.
A.11.2.7	Disposición o reutilización segura de equipos	Todos los elementos del equipo que contengan medios de almacenamiento deben ser verificados para asegurar que cualquier dato sensible y software con licencia se haya eliminado o se haya sobre escrito de manera segura antes de su disposición o reutilización.
A.11.2.8	Equipos de usuario desatendidos	Los usuarios deben asegurarse de que el equipo desatendido tenga la protección apropiada.
A.11.2.9	Política de escritorio limpio y pantalla limpia	Una política de escritorio limpio de papeles y de medios de almacenamiento removibles, así como una política de pantalla limpia para las instalaciones de procesamientos de la información debe ser adoptada.
A.12 Seguridad de las operaciones		
A.12.1 Procedimientos y responsabilidades operativas		
Objetivo: Asegurar que las operaciones de instalaciones de procesamiento de la información sean correctas y seguras.		
A.12.1.1	Procedimientos operativos documentados	Los procedimientos operativos deben ser documentados y puestos a disposición de todos los usuarios que los necesitan.
A.12.1.2	Gestión del cambio	Los cambios en la organización, procesos de negocio, instalaciones de procesamiento de la información y sistemas que afecten la seguridad de la información deben ser controlados.

A.12.1.3	Gestión de la capacidad	El uso de recursos debe ser monitoreado, afinado y se debe hacer proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido del sistema.
A.12.1.4	Separación de los entornos de desarrollo, pruebas y operaciones	Los entornos de desarrollo, pruebas y operaciones deben ser separados para reducir los riesgos de acceso no autorizado o cambios al entorno operativo.
A.12.2 Protección contra códigos maliciosos		
Objetivo: Asegurar que la información y las instalaciones de procesamiento de la información estén protegidas contra códigos maliciosos.		
A.12.2.1	Controles contra códigos maliciosos	Controles de detección, prevención y recuperación para proteger contra códigos maliciosos deben ser implementados, en combinación con una concientización apropiada de los usuarios.
A.12.3 Respaldo		
Objetivo: Proteger contra la pérdida de datos.		
A.12.3.1	Respaldo de la información	Copias de respaldo de la información, del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada.
A.12.4 Registros y monitoreo		
Objetivo: Registrar eventos y generar evidencia		
A.12.4.1	Registro de eventos	Registros (logs) de eventos de actividades de usuarios, excepciones, fallas y eventos de seguridad de la información deben ser producidos, mantenidos y regularmente revisados.
A.12.4.2	Protección de información de registros	Las instalaciones para registros (logs) y la información de los registros (logs) deben ser protegidas contra la adulteración y el acceso no autorizado.
A.12.4.3	Registros del administrador y del operador	Las actividades del administrador del sistema y del operador del sistema deben ser registradas y los registros (logs) deben ser protegidos y revisados regularmente.
A.12.4.4	Sincronización de reloj	Los relojes de todos los sistemas de procesamiento de la información relevantes dentro de una organización o dominio de seguridad deben estar sincronizados a una fuente de tiempo de referencia única.
A.12.5 Control del software operacional		
Objetivo: Asegurar la integridad de los sistemas operacionales.		
A.12.5.1	Instalación de software en sistemas operacionales	Procedimientos deben ser implementados para controlar la instalación de software en sistemas operacionales.
A.12.6 Gestión de vulnerabilidad técnica		
Objetivo: Prevenir la explotación de vulnerabilidades técnicas.		
A.12.6.1	Gestión de vulnerabilidades técnicas	Información sobre vulnerabilidades técnicas de los sistemas de información utilizados debe ser obtenida de manera oportuna, la exposición de la organización a dichas vulnerabilidades debe ser evaluada y las medidas apropiadas deben ser tomadas para resolver el riesgo asociado.
A.12.6.2	Restricciones sobre la instalación de software	Reglas que gobiernen la instalación de software por parte de los usuarios deben ser establecidas e implementadas.
A.12.7 Consideraciones para la auditoría de los sistemas de información		
Objetivo: Minimizar el impacto de las actividades de auditoría en los sistemas operacionales.		
A.12.7.1	Controles de auditoría de sistemas de información	Requisitos de las auditorías y las actividades que involucran la verificación de sistemas operacionales deben ser cuidadosamente planificados y acordados para minimizar la interrupción a los procesos del negocio.
A.13 Seguridad de las comunicaciones		
A.13.1 Gestión de seguridad de la red		
Objetivo: Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de la información de apoyo.		
A.13.1.1	Controles de la red	Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y las aplicaciones.
A.13.1.2	Seguridad de servicios de red	Mecanismos de seguridad, niveles de servicio y requisitos de gestión de todos los servicios de red deben ser identificados e incluidos en acuerdos de servicios de red, ya sea que estos servicios se provean internamente o sean tercerizados.
A.13.1.3	Segregación en redes	Grupos de servicios de información, usuarios y sistemas de información deben ser segregados en redes.
A.13.2 Transferencia de información		
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.		
A.13.2.1	Políticas y procedimientos de transferencia de la información	Políticas, procedimientos y controles de transferencia formales deben aplicarse para proteger la transferencia de información a través del uso de todo tipo de instalaciones de comunicación.

A.13.2.2	Acuerdo sobre transferencia de información	Los acuerdos deben dirigir la transferencia segura de información del negocio entre la organización y partes externas.
A.13.2.3	Mensajes electrónicos	La información involucrada en mensajería electrónica debe ser protegida apropiadamente.
A.13.2.4	Acuerdos de confidencialidad o no divulgación	Requisitos para los acuerdos de confidencialidad o no divulgación que reflejan las necesidades de la organización para la protección de la información deben ser identificados, revisados regularmente y documentados.
A.14 Adquisición, desarrollo y mantenimiento de sistemas		
A.14.1 Requisitos de seguridad de los sistemas de información		
Objetivo: Garantizar que la seguridad de la información es una parte integral de los sistemas de información a través del ciclo de vida completo. Esto también incluye los requisitos para sistemas de información que proporcionen servicios sobre redes públicas.		
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Requisitos relacionados a la seguridad de la información deben ser incluidos dentro de los requisitos para nuevos sistemas de información o mejoras a los sistemas de información existentes.
A.14.1.2	Aseguramiento de servicios de aplicaciones sobre redes públicas	La información involucrada en servicios de aplicaciones que pasa sobre redes públicas debe ser protegida de actividad fraudulenta, disputa de contratos o divulgación no autorizada y modificación.
A.14.1.3	Protección de transacciones en servicios de aplicación	La información involucrada en las transacciones de servicios de aplicación debe ser protegida para prevenir transmisión incompleta, ruteo incorrecto, alteración no autorizada de mensajes, divulgación no autorizada, duplicación o respuesta no autorizada de mensajes.
A.14.2 Seguridad en los procesos de desarrollo y soporte		
Objetivo: Garantizar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.		
A.14.2.1	Política de desarrollo seguro	Reglas para el desarrollo de software y sistemas deben ser establecidas y aplicadas a desarrollos dentro de la organización.
A.14.2.2	Procedimientos de control de cambio del sistema	Cambios a los sistemas dentro del ciclo de vida del desarrollo deben ser controlados por medio del uso de procedimientos formales de control de cambios.
A.14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa	Cuando se cambian las plataformas operativas, las aplicaciones críticas para el negocio deben ser revisadas y probadas para asegurar que no haya impacto adverso en las operaciones o en la seguridad de la organización.
A.14.2.4	Restricciones sobre cambios a los paquetes de software	Modificaciones a los paquetes de software deben ser disuadidas, limitadas a los cambios necesarios y todos los cambios deben ser estrictamente controlados.
A.14.2.5	Principios de ingeniería de sistemas seguros	Principios para la ingeniería de sistemas seguros deben ser establecidos, documentados, mantenidos y aplicados a cualquier esfuerzo de implementación de sistemas de información.
A.14.2.6	Ambiente de desarrollo seguro	Las organizaciones deben establecer y proteger apropiadamente los ambientes de desarrollo seguros para los esfuerzos de desarrollo e integración de sistemas que cubren todo el ciclo de vida del desarrollo del sistema.
A.14.2.7	Desarrollo contratado externamente	La organización debe supervisar y monitorear la actividad de desarrollo de sistemas contratado externamente.
A.14.2.8	Pruebas de seguridad del sistema	Pruebas de funcionalidad de la seguridad deben ser llevadas a cabo durante el desarrollo.
A.14.2.9	Pruebas de aceptación del sistema	Programas de pruebas de aceptación y criterios relacionados deben ser establecidos para nuevos sistemas de información, actualizaciones y nuevas versiones.
A.14.3 Datos de prueba		
Objetivo: Asegurar la protección de datos utilizados para las pruebas		
A.14.3.1	Protección de datos de prueba	Los datos de prueba deben ser seleccionados cuidadosamente, protegidos y controlados.
A.15 Relaciones con los proveedores		
A.15.1 Seguridad de la información en las relaciones con los proveedores		
Objetivo: Asegurar protección a los activos de la organización que son accesibles por los proveedores		
A.15.1.1	Política de seguridad de la información para las relaciones con los proveedores	Requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso por parte del proveedor a los activos de la organización deben ser acordados con el proveedor y documentados.
A.15.1.2	Abordar la seguridad dentro de los acuerdos con proveedores	Todos los requisitos relevantes de seguridad de la información deben ser establecidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar, o proveer componentes de infraestructura de TI para la información de la organización.

A.15.1.3	Cadena de suministro de tecnología de información y comunicación	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.
A.15.2 Gestión de entrega de servicios del proveedor		
Objetivo: Mantener un nivel de seguridad de la información y entrega de servicios acordado en línea con los acuerdos con proveedores.		
A.15.2.1	Monitoreo y revisión de servicios de los proveedores	Las organizaciones deben monitorear, revisar y auditar regularmente la entrega de servicios por parte de los proveedores.
A.15.2.2	Gestión de cambios a los servicios de proveedores	Los cambios a la provisión de servicios por parte de proveedores, incluyendo el mantenimiento y mejoramiento de políticas, procedimientos y controles existentes de seguridad de la información deben ser gestionados tomando en cuenta la criticidad de la información del negocio, sistemas y procesos involucrados y una reevaluación de riesgos.
A.16 Gestión de incidentes de seguridad de la información		
A.16.1 Gestión de incidentes de seguridad de la información y mejoras		
Objetivo: Asegurar un enfoque consistente y efectivo a la gestión de incidentes de seguridad de la información, incluyendo la comunicación sobre eventos de seguridad y debilidades.		
A.16.1.1	Responsabilidades y procedimientos	Las responsabilidades de gestión y los procedimientos deben ser establecidos para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.
A.16.1.2	Reporte de eventos de seguridad de la información	Los eventos de seguridad de la información deben ser reportados a través de canales de gestión apropiados tan rápido como sea posible.
A.16.1.3	Reporte de debilidades de seguridad de la información	Empleados y contratistas que usan los sistemas y servicios de información de la organización deben ser exigidos a advertir y reportar cualquier debilidad observada o de la que se sospecha en cuanto a seguridad de la información en los sistemas o servicios.
A.16.1.4	Evaluación y decisión sobre eventos de seguridad de la información	Los eventos de seguridad de la información deben ser evaluados y debe decidirse si son clasificados como incidentes de seguridad de la información.
A.16.1.5	Respuesta a incidentes de seguridad de la información	Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	El conocimiento adquirido a partir de analizar y resolver los incidentes de seguridad de la información debe ser utilizado para reducir la probabilidad o el impacto de incidentes futuros.
A.16.1.7	Recolección de evidencia	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
A.17 Aspectos de seguridad de la información en la gestión de continuidad del negocio		
A.17.1 Continuidad de seguridad de la información		
Objetivo: La continuidad de seguridad de la información debe estar embebida en los sistemas de gestión de continuidad del negocio de la organización		
A.17.1.1	Planificación de continuidad de seguridad de la información	La organización debe determinar sus requisitos de seguridad de la información y continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
A.17.1.2	Implementación de continuidad de seguridad de la información	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de seguridad de la información durante una situación adversa.
A.17.1.3	Verificación, revisión y evaluación de continuidad de seguridad de la información	La organización debe verificar los controles de continuidad de seguridad de la información que han establecido e implementado a intervalos regulares para asegurarse que son válidos y efectivos durante situaciones adversas.
A.17.2 Redundancias		
Objetivo: Asegurar la disponibilidad de las instalaciones y procesamiento de la información		
A.17.2.1	Instalaciones de procesamiento de la información	Las instalaciones de procesamiento de la información deben ser implementadas con redundancia suficiente para cumplir con los requisitos de disponibilidad.
A.18 Cumplimiento		
A.18.1 Cumplimiento con requisitos legales y contractuales		
Objetivo: Evitar infracciones de las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas a la seguridad de la información y a cualquier requisito de seguridad.		
A.18.1.1	Identificación de requisitos contractuales y de legislación aplicables	Todos los requisitos legislativos, estatutarios, regulatorios y contractuales relevantes, así como el enfoque de la organización para cumplir con estos requisitos deben ser explícitamente identificados, documentados y mantenidos al día para cada sistema de información y para la organización.
A.18.1.2	Derechos de propiedad intelectual	Procedimientos apropiados deben ser implementados para asegurar el cumplimiento de requisitos legislativos, regulatorios y contractuales relacionados a los derechos de propiedad intelectual y uso de productos de software propietario.

A.18.1.3	Protección de registros	Los registros deben ser protegidos de cualquier pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, de acuerdo con los requisitos legislativos, regulatorios, contractuales y del negocio.
A.18.1.4	Privacidad y protección de datos personales	La privacidad y la protección de datos personales deben ser aseguradas tal como se requiere en la legislación y regulación relevantes donde sea aplicable.
A.18.1.5	Regulación de controles criptográficos	Controles criptográficos deben ser utilizados en cumplimiento con todos los acuerdos, legislación y regulación relevantes.
A.18.2 Revisiones de seguridad de la información		
Objetivo: Asegurar que la seguridad de la información está implementada y es operada de acuerdo con las políticas y procedimientos organizativos.		
A.18.2.1	Revisión independiente de la seguridad de la información	El enfoque de la organización para manejar la seguridad de la información y su implementación (por ejemplo, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) debe ser revisado independientemente a intervalos planeados o cuando ocurran cambios significativos.
A.18.2.2	Cumplimiento de políticas y normas de seguridad	Los gerentes deben revisar regularmente el cumplimiento del procesamiento de la información y de los procedimientos dentro de su área de responsabilidad con las políticas, normas y otros requisitos de seguridad apropiados.
A.18.2.3	Revisión del cumplimiento técnico	Los sistemas de información deben ser revisados regularmente respecto al cumplimiento de las políticas y normas de seguridad de la información de la organización.

Oefa Organismo de Evaluación y Fiscalización Ambiental	**DECLARACIÓN DE APLICABILIDAD**

FECHA DE ACTUALIZACIÓN:	

Control NTP ISO/IEC 27001:2014				Justificación de la inclusión o exclusión	Evidencia	Status
Código	**Nombre**	**Descripción**	**Aplicabilidad**			
A.5 Políticas de seguridad de la información						
A.5.1 Dirección de la gerencia para la seguridad de la información						
Objetivo: Proporcionar dirección y apoyo de la gerencia para la seguridad de la información en concordancia con los requisitos del negocio y las leyes y regulaciones relevantes.						
A.5.1.1	Políticas para la seguridad de la información	Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la gerencia, publicado y comunicado a los empleados y a las partes externas relevantes.	SÍ			
A.5.1.2	Revisión de las políticas para la seguridad de la información	Las políticas para la seguridad de la información deben ser revisadas a intervalos planificados o si ocurren cambios significativos para asegurar su conveniencia, adecuación y efectividad continua.	SÍ			
A.6 Organización de la seguridad de la información						
A.6.1 Organización interna						
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.						
A.6.1.1	Roles y responsabilidades para la seguridad de la información	Todas las responsabilidades de seguridad de la información deben ser definidas y asignadas.	SÍ			
A.6.1.2	Segregación de funciones	Las funciones y áreas de responsabilidad en conflicto deben ser segregadas para reducir oportunidades de modificación no autorizada o no intencional o mal uso de los activos de la organización.	SÍ			
A.6.1.3	Contacto con autoridades	Contactos apropiados con autoridades relevantes deben ser mantenidos.	SÍ			
A.6.1.4	Contacto con grupos especiales de interés	Contactos apropiados con grupos especiales de interés u otros foros de especialistas en seguridad y asociaciones profesionales deben ser mantenidos.	SÍ			
A.6.1.5	Seguridad de la información en la gestión de proyectos	La seguridad de la información debe ser tratada en la gestión de proyectos, sin importar el tipo de proyecto.	SÍ			
A.6.2 Dispositivos móviles y teletrabajo						
Objetivo: Asegurar la seguridad del teletrabajo y el uso de los dispositivos móviles.						
A.6.2.1	Política de dispositivos móviles	Una política y medidas de seguridad de soporte deben ser adoptadas para gestionar los riesgos introducidos por el uso de dispositivos móviles.	SÍ			
A.6.2.2	Teletrabajo	Una política y medidas de seguridad de apoyo deben ser implementadas para proteger información a la que se accede, se procesa o almacena en sitios de teletrabajo.	SÍ			
A.7 Seguridad de los recursos humanos						
A.7.1 Antes del empleo						
Objetivo: Asegurar que los empleados y contratistas entienden sus responsabilidades y son convenientes para los roles para los que se les considera.						
A.7.1.1	Investigación de antecedentes	Las verificaciones de los antecedentes de todos los candidatos a ser empleados deben ser llevadas a cabo en concordancia con las leyes, regulaciones y ética relevantes, y debe ser proporcional a los requisitos del negocio, la clasificación de la información a la que se tendrá acceso y los riesgos percibidos.	SÍ			
A.7.1.2	Términos y condiciones del empleo	Los acuerdos contractuales con los empleados y contratistas deben estipular responsabilidades de estos y de la organización respecto de la seguridad de la información.	SÍ			
A.7.2 Durante el empleo						
Objetivo: Asegurar que los empleados y contratistas sean conscientes y cumplan con sus responsabilidades de seguridad de la información.						
A.7.2.1	Responsabilidades de gestión	La gerencia debe requerir a todos los empleados y contratistas aplicar la seguridad de la información en concordancia con las políticas y procedimientos establecidos por la organización.	SÍ			
A.7.2.2	Conciencia, educación y capacitación sobre la seguridad de la información	Todos los empleados de la organización y, cuando fuera relevante, los contratistas deben recibir educación y capacitación sobre la conciencia de la seguridad de la información, así como actualizaciones regulares sobre políticas y procedimientos de la organización, según sea relevante para la función del trabajo que cumplen.	SÍ			
A.7.2.3	Proceso disciplinario	Debe haber un proceso disciplinario formal y comunicado para tomar acción contra empleados que hayan cometido una infracción a la seguridad de la información.	SÍ			

A.7.3 Terminación y cambio de empleo						
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.						
A.7.3.1	Terminación o cambio de responsabilidades del empleo.	Las responsabilidades y deberes de seguridad de la información que siguen siendo válidos luego de la terminación o cambio de empleo deben ser definidos, comunicados al empleado o contratista y forzar su cumplimiento.	SÍ			
A.8 Gestión de activos						
A.8.1 Responsabilidad por los activos						
Objetivo: Identificar los activos de la organización y definir responsabilidades de protección apropiadas.						
A.8.1.1	Inventario de activos	Información, Otros activos asociados con información e instalaciones de procesamiento de información deben ser identificados y un inventario de estos activos debe ser elaborado y mantenido.	SÍ			
A.8.1.2	Propiedad de los activos	Los activos mantenidos en el inventario deben ser propios.	SÍ			
A.8.1.3	Uso aceptable de los activos	Las reglas para el uso aceptable de la información y activos asociados con la información y con las instalaciones de procesamiento de la información deben ser identificadas, documentadas e implementadas.	SÍ			
A.8.1.4	Retorno de activos	Todos los empleados y usuarios de partes externas deben retornar todos los activos de la organización en su posesión a la conclusión de su empleo, contrato o acuerdo.	SÍ			
A.8.2 Clasificación de la información						
Objetivo: Asegurar que la información recibe un nivel apropiado de protección en concordancia con su importancia para la organización.						
A.8.2.1	Clasificación de la información	La información debe ser clasificada en términos de los requisitos legales, valor, criticidad y sensibilidad respecto a una divulgación o modificación no autorizada.	SÍ			
A.8.2.2	Etiquetado de la información	Un conjunto apropiado de procedimientos para el etiquetado de la información debe ser desarrollado e implementado en concordancia con el esquema de clasificación de la información adoptado por la organización.	SÍ			
A.8.2.3	Manejo de activos	Los procedimientos para el manejo de activos deben ser desarrollados e implementados en concordancia con el esquema de clasificación de la información adoptado por la organización.	SÍ			
A.8.3 Manejo de los medios						
Objetivo: Prevenir la divulgación, modificación, remoción o destrucción no autorizada de información almacenada en medios.						
A.8.3.1	Gestión de medios removibles	Se debe implementar procedimientos para la gestión de medios removibles en concordancia con el esquema de clasificación adoptado por la organización.	SÍ			
A.8.3.2	Disposición de medios	Se debe poner a disposición los medios de manera segura cuando ya no se requieran, utilizando procedimientos formales.	SÍ			
A.8.3.3	Transferencia de medios físicos	Los medios que contienen información deben ser protegidos contra el acceso no autorizado, el mal uso o la corrupción durante el transporte.	SÍ			
A.9 Control de acceso						
A.9.1 Requisitos de la empresa para el control de acceso						
Objetivo: Limitar el acceso a la información y a las instalaciones de procesamiento de la información.						
A.9.1.1	Política de control de acceso	Una política de control de acceso debe ser establecida, documentada y revisada basada en requisitos del negocio y de seguridad de la información.	SÍ			
A.9.1.2	Acceso a redes y servicios de red	Los usuarios deben tener acceso solamente a la red y a servicios de red que hayan sido específicamente autorizados a usar.	SÍ			
A.9.2 Gestión de acceso de usuario						
Objetivo: Asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas y servicios.						
A.9.2.1	Registro y baja de usuarios	Un proceso formal de registro y baja de usuarios debe ser implementado para permitir la asignación de derechos de acceso.	SÍ			
A.9.2.2	Aprovisionamiento de acceso a usuario	Un proceso formal de aprovisionamiento de acceso a usuarios debe ser implementado para asignar o revocar los derechos de acceso para todos los tipos de usuarios a todos los sistemas y servicios.	SÍ			
A.9.2.3	Gestión de derechos de acceso privilegiados	La asignación y uso de derechos de acceso privilegiado debe ser restringida y controlada.	SÍ			
A.9.2.4	Gestión de información de autentificación secreta de usuarios	La asignación de información de autentificación secreta debe ser controlada a través de un proceso de gestión formal.	SÍ			
A.9.2.5	Revisión de derechos de acceso de usuarios	Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares.	SÍ			.
A.9.2.6	Remoción o ajuste de derechos de acceso	Los derechos de acceso a información e instalaciones de procesamientos de información de todos los empleados y de los usuarios de partes externas deben removerse al término de su empleo, contrato o acuerdo, o ajustarse según el cambio.	SÍ			.
A.9.3 Responsabilidades de los usuarios						

Objetivo: Hacer que los usuarios respondan por la salvaguarda de su información de autentificación.						
A.9.3.1	Uso de información autentificación secreta	Los usuarios deben ser exigidos a que sigan las prácticas de la organización en el uso de información de autentificación secreta.	SÍ			.
A.9.4 Control de acceso a sistema y aplicación						
Objetivo: Prevenir el acceso no autorizado a los sistemas y aplicaciones.						
A.9.4.1	Restricción de acceso a la información	El acceso a la información y a las funciones del sistema de aplicación debe ser restringido en concordancia con la política de control de acceso.	SÍ			.
A.9.4.2	Procedimientos de ingreso seguro	Donde la política de control de acceso lo requiera, el acceso a los sistemas y a las aplicaciones debe ser controlado por un procedimiento de ingreso seguro.	SÍ			.
A.9.4.3	Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.	SÍ			.
A.9.4.4	Uso de programas utilitarios privilegiados	El uso de programas utilitarios que podrían ser capaces de pasar por alto los controles del sistema y de las aplicaciones debe ser restringido y controlarse estrictamente.	SÍ			.
A.9.4.5	Control de acceso al código fuente de los programas	El acceso al código fuente de los programas debe ser restringido.	SÍ			.
A.10 Criptografía						
A.10.1 Controles criptográficos						
Objetivo: Asegurar el uso apropiado y efectivo de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.						
A.10.1.1	Política sobre el uso controles criptográficos	Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada.	SÍ			.
A.10.1.2	Gestión de claves	Una política sobre el uso, protección y tiempo de vida de las claves criptográficas debe ser desarrollada e implementada a través de todo su ciclo de vida.	SÍ			.
A.11 Seguridad física y ambiental						
A.11.1 Áreas seguras						
Objetivo: Impedir acceso físico no autorizado, daño e interferencia a la información y a las instalaciones de procesamiento de la información de la organización.						
A.11.1.1	Perímetro de seguridad física	Perímetros de seguridad deben ser definidos y utilizados para proteger áreas que contienen información sensible o crítica e instalaciones de procesamiento de la información.	SÍ			.
A.11.1.2	Controles de ingreso físico	Las áreas seguras deben ser protegidas por medio de controles apropiados de ingreso para asegurar que se le permite el acceso sólo al personal autorizado.	SÍ			.
A.11.1.3	Asegurar oficinas, áreas e instalaciones	Seguridad física para oficinas, áreas e instalaciones debe ser diseñada e implementada.	SÍ			.
A.11.1.4	Protección contra amenazas externas y ambientales	Protección física contra desastres naturales, ataque malicioso o accidentes debe ser diseñada y aplicada.	SÍ			.
A.11.1.5	Trabajo en áreas seguras	Procedimientos para el trabajo en áreas seguras debe ser diseñado y aplicado.	SÍ			.
A.11.1.6	Áreas de despacho y carga	Los puntos de acceso, como las áreas de despacho, carga y otros puntos en donde personas no autorizadas pueden ingresar al local deben ser controlados, y si fuera posible, aislarlos de las instalaciones de procesamiento de la información para evitar el acceso no autorizado.	SÍ			.
A.11.2 Equipos						
Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos e interrupción de las operaciones de la organización.						
A.11.2.1	Emplazamiento y protección de los equipos	Los equipos deben ser ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado.	SÍ			.
A.11.2.2	Servicios de suministro	Los equipos deben ser protegidos contra fallas de electricidad y otras alteraciones causadas por fallas en los servicios de suministro.	SÍ			.
A.11.2.3	Seguridad del cableado	El cableado de energía y telecomunicaciones que llevan datos o servicios de información de soporte debe ser protegido de la interceptación, interferencia o daño.	SÍ			.
A.11.2.4	Mantenimiento de equipos	Los equipos deben mantenerse de manera correcta para asegurar su continua disponibilidad e integridad.	SÍ			.
A.11.2.5	Remoción de activos	Los equipos, la información o el software no deben ser retirados de su lugar sin autorización previa.	SÍ			.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	La seguridad debe ser aplicada a los activos que están fuera de su lugar tomando en cuenta los distintos riesgos de trabajar fuera de las instalaciones de la organización.	SÍ			.
A.11.2.7	Disposición o reutilización segura de equipos	Todos los elementos del equipo que contengan medios de almacenamiento deben ser verificados para asegurar que cualquier dato sensible y software con licencia se haya eliminado o se haya sobre escrito de manera segura antes de su disposición o reutilización.	SÍ			.
A.11.2.8	Equipos de usuario desatendidos	Los usuarios deben asegurarse de que el equipo desatendido tenga la protección apropiada.	SÍ			.
A.11.2.9	Política de escritorio limpio y pantalla limpia	Una política de escritorio limpio de papeles y de medios de almacenamiento removibles, así como una política de pantalla limpia para las instalaciones de procesamientos de la información debe ser adoptada.	SÍ			.

A.12 Seguridad de las operaciones						
A.12.1 Procedimientos y responsabilidades operativas						
Objetivo: Asegurar que las operaciones de instalaciones de procesamiento de la información sean correctas y seguras.						
A.12.1.1	Procedimientos operativos documentados	Los procedimientos operativos deben ser documentados y puestos a disposición de todos los usuarios que los necesitan.	SÍ			.
A.12.1.2	Gestión del cambio	Los cambios en la organización, procesos de negocio, instalaciones de procesamiento de la información y sistemas que afecten la seguridad de la información deben ser controlados.	SÍ			.
A.12.1.3	Gestión de la capacidad	El uso de recursos debe ser monitoreado, afinado y se debe hacer proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido del sistema.	SÍ			.
A.12.1.4	Separación de los entornos de desarrollo, pruebas y operaciones	Los entornos de desarrollo, pruebas y operaciones deben ser separados para reducir los riesgos de acceso no autorizado o cambios al entorno operativo.	SÍ			.
A.12.2 Protección contra códigos maliciosos						
Objetivo: Asegurar que la información y las instalaciones de procesamiento de la información estén protegidas contra códigos maliciosos.						
A.12.2.1	Controles contra códigos maliciosos	Controles de detección, prevención y recuperación para proteger contra códigos maliciosos deben ser implementados, en combinación con una concientización apropiada de los usuarios.	SÍ			.
A.12.3 Respaldo						
Objetivo: Proteger contra la pérdida de datos.						
A.12.3.1	Respaldo de la información	Copias de respaldo de la información, del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada.	SÍ			.
A.12.4 Registros y monitoreo						
Objetivo: Registrar eventos y generar evidencia						
A.12.4.1	Registro de eventos	Registros (logs) de eventos de actividades de usuarios, excepciones, fallas y eventos de seguridad de la información deben ser producidos, mantenidos y regularmente revisados.	SÍ			.
A.12.4.2	Protección de información de registros	Las instalaciones para registros (logs) y la información de los registros (logs) deben ser protegidas contra la adulteración y el acceso no autorizado.	SÍ			.
A.12.4.3	Registros del administrador y del operador	Las actividades del administrador del sistema y del operador del sistema deben ser registradas y los registros (logs) deben ser protegidos y revisados regularmente.	SÍ			.
A.12.4.4	Sincronización de reloj	Los relojes de todos los sistemas de procesamiento de la información relevantes dentro de una organización o dominio de seguridad deben estar sincronizados a una fuente de tiempo de referencia única.	SÍ			.
A.12.5 Control del software operacional						
Objetivo: Asegurar la integridad de los sistemas operacionales.						
A.12.5.1	Instalación de software en sistemas operacionales	Procedimientos deben ser implementados para controlar la instalación de software en sistemas operacionales.	SÍ			.
A.12.6 Gestión de vulnerabilidad técnica						
Objetivo: Prevenir la explotación de vulnerabilidades técnicas.						
A.12.6.1	Gestión de vulnerabilidades técnicas	Información sobre vulnerabilidades técnicas de los sistemas de información utilizados debe ser obtenida de manera oportuna, la exposición de la organización a dichas vulnerabilidades debe ser evaluada y las medidas apropiadas deben ser tomadas para resolver el riesgo asociado.	SÍ			.
A.12.6.2	Restricciones sobre la instalación de software	Reglas que gobiernen la instalación de software por parte de los usuarios deben ser establecidas e implementadas.	SÍ			.
A.12.7 Consideraciones para la auditoría de los sistemas de información						
Objetivo: Minimizar el impacto de las actividades de auditoría en los sistemas operacionales.						
A.12.7.1	Controles de auditoría de sistemas de información	Requisitos de las auditorías y las actividades que involucran la verificación de sistemas operacionales deben ser cuidadosamente planificados y acordados para minimizar la interrupción a los procesos del negocio.	SÍ			.
A.13 Seguridad de las comunicaciones						
A.13.1 Gestión de seguridad de la red						
Objetivo: Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de la información de apoyo.						
A.13.1.1	Controles de la red	Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y las aplicaciones.	SÍ			.
A.13.1.2	Seguridad de servicios de red	Mecanismos de seguridad, niveles de servicio y requisitos de gestión de todos los servicios de red deben ser identificados e incluidos en acuerdos de servicios de red, ya sea que estos servicios se provean internamente o sean tercerizados.	SÍ			.

A.13.1.3	Segregación en redes	Grupos de servicios de información, usuarios y sistemas de información deben ser segregados en redes.	SÍ			.
A.13.2 Transferencia de información						
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.						
A.13.2.1	Políticas y procedimientos de transferencia de la información	Políticas, procedimientos y controles de transferencia formales deben aplicarse para proteger la transferencia de información a través del uso de todo tipo de instalaciones de comunicación.	SÍ			.
A.13.2.2	Acuerdo sobre transferencia de información	Los acuerdos deben dirigir la transferencia segura de información del negocio entre la organización y partes externas.	SÍ			.
A.13.2.3	Mensajes electrónicos	La información involucrada en mensajería electrónica debe ser protegida apropiadamente.	SÍ			.
A.13.2.4	Acuerdos de confidencialidad o no divulgación	Requisitos para los acuerdos de confidencialidad o no divulgación que reflejan las necesidades de la organización para la protección de la información deben ser identificados, revisados regularmente y documentados.	SÍ			.
A.14 Adquisición, desarrollo y mantenimiento de sistemas						
A.14.1 Requisitos de seguridad de los sistemas de información						
Objetivo: Garantizar que la seguridad de la información es una parte integral de los sistemas de información a través del ciclo de vida completo. Esto también incluye los requisitos para sistemas de información que proporcionen servicios sobre redes públicas.						
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Requisitos relacionados a la seguridad de la información deben ser incluidos dentro de los requisitos para nuevos sistemas de información o mejoras a los sistemas de información existentes.	SÍ			.
A.14.1.2	Aseguramiento de servicios de aplicaciones sobre redes públicas	La información involucrada en servicios de aplicaciones que pasa sobre redes públicas debe ser protegida de actividad fraudulenta, disputa de contratos o divulgación no autorizada y modificación.	SÍ			.
A.14.1.3	Protección de transacciones en servicios de aplicación	La información involucrada en las transacciones de servicios de aplicación debe ser protegida para prevenir transmisión incompleta, ruteo incorrecto, alteración no autorizada de mensajes, divulgación no autorizada, duplicación o respuesta no autorizada de mensajes.	SÍ			.
A.14.2 Seguridad en los procesos de desarrollo y soporte						
Objetivo: Garantizar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.						
A.14.2.1	Política de desarrollo seguro	Reglas para el desarrollo de software y sistemas deben ser establecidas y aplicadas a desarrollos dentro de la organización.	SÍ			.
A.14.2.2	Procedimientos de control de cambio del sistema	Cambios a los sistemas dentro del ciclo de vida del desarrollo deben ser controlados por medio del uso de procedimientos formales de control de cambios.	SÍ			.
A.14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa	Cuando se cambian las plataformas operativas, las aplicaciones críticas para el negocio deben ser revisadas y probadas para asegurar que no haya impacto adverso en las operaciones o en la seguridad de la organización.	SÍ			.
A.14.2.4	Restricciones sobre cambios a los paquetes de software	Modificaciones a los paquetes de software deben ser disuadidas, limitadas a los cambios necesarios y todos los cambios deben ser estrictamente controlados.	SÍ			.
A.14.2.5	Principios de ingeniería de sistemas seguros	Principios para la ingeniería de sistemas seguros deben ser establecidos, documentados, mantenidos y aplicados a cualquier esfuerzo de implementación de sistemas de información.	SÍ			.
A.14.2.6	Ambiente de desarrollo seguro	Las organizaciones deben establecer y proteger apropiadamente los ambientes de desarrollo seguros para los esfuerzos de desarrollo e integración de sistemas que cubren todo el ciclo de vida del desarrollo del sistema.	SÍ			.
A.14.2.7	Desarrollo contratado externamente	La organización debe supervisar y monitorear la actividad de desarrollo de sistemas contratado externamente.	SÍ			.
A.14.2.8	Pruebas de seguridad del sistema	Pruebas de funcionalidad de la seguridad deben ser llevadas a cabo durante el desarrollo.	SÍ			.
A.14.2.9	Pruebas de aceptación del sistema	Programas de pruebas de aceptación y criterios relacionados deben ser establecidos para nuevos sistemas de información, actualizaciones y nuevas versiones.	SÍ			.
A.14.3 Datos de prueba						
Objetivo: Asegurar la protección de datos utilizados para las pruebas						
A.14.3.1	Protección de datos de prueba	Los datos de prueba deben ser seleccionados cuidadosamente, protegidos y controlados.	SÍ			.
A.15 Relaciones con los proveedores						
A.15.1 Seguridad de la información en las relaciones con los proveedores						
Objetivo: Asegurar protección a los activos de la organización que son accesibles por los proveedores						
A.15.1.1	Política de seguridad de la información para las relaciones con los proveedores	Requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso por parte del proveedor a los activos de la organización deben ser acordados con el proveedor y documentados.	SÍ			.
A.15.1.2	Abordar la seguridad dentro de los acuerdos con proveedores	Todos los requisitos relevantes de seguridad de la información deben ser establecidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar, o proveer componentes de infraestructura de TI para la información de la organización.	SÍ			.
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	SÍ			.
A.15.2 Gestión de entrega de servicios del proveedor						

Objetivo: Mantener un nivel de seguridad de la información y entrega de servicios acordado en línea con los acuerdos con proveedores.						
A.15.2.1	Monitoreo y revisión de servicios de los proveedores	Las organizaciones deben monitorear, revisar y auditar regularmente la entrega de servicios por parte de los proveedores.	SÍ			.
A.15.2.2	Gestión de cambios a los servicios de proveedores	Los cambios a la provisión de servicios por parte de proveedores, incluyendo el mantenimiento y mejoramiento de políticas, procedimientos y controles existentes de seguridad de la información deben ser gestionados tomando en cuenta la criticidad de la información del negocio, sistemas y procesos involucrados y una reevaluación de riesgos.	SÍ			.
A.16 Gestión de incidentes de seguridad de la información						
A.16.1 Gestión de incidentes de seguridad de la información y mejoras						
Objetivo: Asegurar un enfoque consistente y efectivo a la gestión de incidentes de seguridad de la información, incluyendo la comunicación sobre eventos de seguridad y debilidades.						
A.16.1.1	Responsabilidades y procedimientos	Las responsabilidades de gestión y los procedimientos deben ser establecidos para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.	SÍ			.
A.16.1.2	Reporte de eventos de seguridad de la información	Los eventos de seguridad de la información deben ser reportados a través de canales de gestión apropiados tan rápido como sea posible.	SÍ			.
A.16.1.3	Reporte de debilidades de seguridad de la información	Empleados y contratistas que usan los sistemas y servicios de información de la organización deben ser exigidos a advertir y reportar cualquier debilidad observada o de la que se sospecha en cuanto a seguridad de la información en los sistemas o servicios.	SÍ			.
A.16.1.4	Evaluación y decisión sobre eventos de seguridad de la información	Los eventos de seguridad de la información deben ser evaluados y debe decidirse si son clasificados como incidentes de seguridad de la información.	SÍ			.
A.16.1.5	Respuesta a incidentes de seguridad de la información	Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.	SÍ			.
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	El conocimiento adquirido a partir de analizar y resolver los incidentes de seguridad de la información debe ser utilizado para reducir la probabilidad o el impacto de incidentes futuros.	SÍ			.
A.16.1.7	Recolección de evidencia	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	SÍ			.
A.17 Aspectos de seguridad de la información en la gestión de continuidad del negocio						
A.17.1 Continuidad de seguridad de la información						
Objetivo: La continuidad de seguridad de la información debe estar embebida en los sistemas de gestión de continuidad del negocio de la organización						
A.17.1.1	Planificación de continuidad de seguridad de la información	La organización debe determinar sus requisitos de seguridad de la información y continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	SÍ			
A.17.1.2	Implementación de continuidad de seguridad de la información	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de seguridad de la información durante una situación adversa.	SÍ			.
A.17.1.3	Verificación, revisión y evaluación de continuidad de seguridad de la información	La organización debe verificar los controles de continuidad de seguridad de la información que han establecido e implementado a intervalos regulares para asegurarse que son válidos y efectivos durante situaciones adversas.	SÍ			.
A.17.2 Redundancias						
Objetivo: Asegurar la disponibilidad de las instalaciones y procesamiento de la información						
A.17.2.1	Instalaciones de procesamiento de la información	Las instalaciones de procesamiento de la información deben ser implementadas con redundancia suficiente para cumplir con los requisitos de disponibilidad.	SÍ			.
A.18 Cumplimiento						
A.18.1 Cumplimiento con requisitos legales y contractuales						
Objetivo: Evitar infracciones de las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas a la seguridad de la información y a cualquier requisito de seguridad.						
A.18.1.1	Identificación de requisitos contractuales y de legislación aplicables	Todos los requisitos legislativos, estatutarios, regulatorios y contractuales relevantes, así como el enfoque de la organización para cumplir con estos requisitos deben ser explícitamente identificados, documentados y mantenidos al día para cada sistema de información y para la organización.	SÍ			.
A.18.1.2	Derechos de propiedad intelectual	Procedimientos apropiados deben ser implementados para asegurar el cumplimiento de requisitos legislativos, regulatorios y contractuales relacionados a los derechos de propiedad intelectual y uso de productos de software propietario.	SÍ			.
A.18.1.3	Protección de registros	Los registros deben ser protegidos de cualquier pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, de acuerdo con los requisitos legislativos, regulatorios, contractuales y del negocio.	SÍ			.
A.18.1.4	Privacidad y protección de datos personales	La privacidad y la protección de datos personales deben ser aseguradas tal como se requiere en la legislación y regulación relevantes donde sea aplicable.	SÍ			
A.18.1.5	Regulación de controles criptográficos	Controles criptográficos deben ser utilizados en cumplimiento con todos los acuerdos, legislación y regulación relevantes.	SÍ			
A.18.2 Revisiones de seguridad de la información						
Objetivo: Asegurar que la seguridad de la información está implementada y es operada de acuerdo con las políticas y procedimientos organizativos.						
A.18.2.1	Revisión independiente de la seguridad de la información	El enfoque de la organización para manejar la seguridad de la información y su implementación (por ejemplo, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) debe ser revisado independientemente a intervalos planeados o cuando ocurran cambios significativos.	SÍ			

A.18.2.2	Cumplimiento de políticas y normas de seguridad	Los gerentes deben revisar regularmente el cumplimiento del procesamiento de la información y de los procedimientos dentro de su área de responsabilidad con las políticas, normas y otros requisitos de seguridad apropiados.	SÍ			
A.18.2.3	Revisión del cumplimiento técnico	Los sistemas de información deben ser revisados regularmente respecto al cumplimiento de las políticas y normas de seguridad de la información de la organización.	SÍ			

Guía para el registro de la Declaración de Aplicabilidad

1. Aplicabilidad	Indica si el control referido es o no aplicable al OEFA.
2. Justificación de la inclusión o exclusión	Muestra las razones que sustentan la inclusión o exclusión del control en el OEFA.
	En casos de inclusión. Se fundamenta en al menos uno de los siguientes motivos: •Establecidos para cumplir con normativas internas del OEFA (políticas, procedimientos, etc.). •Establecidos por normatividad estatal (leyes, normas con rango de ley, normas reglamentarias y resolución de carácter general). •Establecidos por obligaciones contractuales del OEFA con terceros. •Establecidos para prevenir la ocurrencia de riesgos (eliminar o reducir riesgos mediante controles identificados durante las gestiones de riesgos).
	En casos de exclusión. Detalla el análisis sustentado en base al cual el OEFA ha determinado que no corresponde la inclusión del control.
3. Evidencia	Describe la situación actual de la implementación del control en el OEFA.
4. Status	Se define si el control se encuentra - en proceso: en ejecución con plan de tratamiento - culminado: control implementado con evidencia correspondiente

4. Otras consideraciones	
Responsable	Oficial de Seguridad y Confianza Digital (OSCD)
Frecuencia de actualización	Mínima anual, o cuando ocurran cambios significativos en el alcance del Sistema de Gestión de Seguridad de la información (SGSI)

Formato PA0306-F02
Versión: ***01***
Fecha de aprobación: 22/12/2022

1. MATRIZ DE OPORTUNIDADES																		
1. Identificación del Proceso y factor del contexto				2. Identificación, análisis, evaluación y tratamiento de oportunidades							3. Plan de Acción							
N°	Objetivo del Sistema de Gestión	Proceso Nivel 0	Objetivo del Proceso	Código de la oportunidad	Descripción de la oportunidad	Evaluación				Tratamiento de la oportunidad	Medida de acción adicional	Medida de seguimiento a la acción adicional	Órgano o Unidad Orgánica Responsable	Plazo de implementación		Medios de Verificación (Evidencia de implementación)	Comentarios u Observaciones	Estado de la Medida de Control (seguimiento)
						Probabilidad de la oportunidad	Impacto de la oportunidad	Valor	Nivel					Fecha de Inicio	Fecha de Término			

Formato PA0306-F03
Versión: ***01***
Fecha de aprobación: 22/12/2022

2.1 CRITERIOS DE VALORIZACIÓN PARA OPORTUNIDADES

CRITERIOS PARA EL ANÁLISIS DE OPORTUNIDADES				
Nivel	Probabilidad de la oportunidad	Valor	Impacto de la oportunidad	Valor
Bajo	Bajo potencial de ocurrir en el periodo.	4	Eventual, capaz de aprovecharse inmediatamente	4
Medio	Considerable potencial de ocurrir en el periodo.	6	Temporal, puede colaborar con los resultados esperados por un tiempo corto, generando una contribución final menor al 5%.	6
Alto	Alto potencial de ocurrir en el periodo.	8	Prolongado, puede colaborar con los resultados esperados hasta en un 20%.	8
Muy Alto	Muy alto potencial de ocurrir en el periodo, información disponible al respecto.	10	Duradero, capaz de generar resultados muy superiores a los esperados, por encima del 20%.	10

2.2 TRATAMIENTO DE OPORTUNIDADES

Nivel	Tratamiento de la oportunidad	Valor
BAJO	Observar la oportunidad.	R<32
MEDIO	Observar la oportunidad.	32<=R<48
ALTO	Promover la oportunidad.	48<=R<80
MUY ALTO	Promover la oportunidad.	80<=R<=100

6.1 PROCESOS NIVEL 0

Proceso Nivel 0
PE01 PLANEAMIENTO INSTITUCIONAL
PE02 INNOVACIÓN Y GESTIÓN POR PROCESOS
PE03 COMUNICACIONES
PE04 SOCIO AMBIENTAL
PM01 POLÍTICAS Y ESTRATEGIAS EN FISCALIZACIÓN AMBIENTAL
PM02 SUPERVISIÓN A ENTIDADES DE FISCALIZACIÓN AMBIENTAL
PM03 EVALUACIÓN AMBIENTAL
PM04 SUPERVISIÓN AMBIENTAL
PM05 FISCALIZACIÓN E INCENTIVOS
PA01 RECURSOS HUMANOS
PA02 ADMINISTRACIÓN Y FINANZAS
PA03 TECNOLOGÍAS DE LA INFORMACIÓN
PA04 ASESORÍA JURÍDICA

pendiente

en proceso

implementado

6.2 VALORES DE PROBABILIDAD DE OPORTUNIDAD

Probabilidad de la oportunidad	Valor
Bajo	4
Medio	6
Alto	8
Muy Alto	10

6.3 VALORES DE IMPACTO DE OPORTUNIDAD

Impacto de la oportunidad	Valor
Bajo	4
Medio	6
Alto	8
Muy Alto	10

6.4 VALORES DE RESULTADO DE OPORTUNIDAD

Resultado de la oportunidad	LS	LI	Valor	Tratamiento
Nivel bajo	0	31	Bajo	Observar la oportunidad
Nivel medio	32	47	Medio	Observar la oportunidad
Nivel alto	48	79	Alto	Promover la oportunidad
Nivel muy alto	80	160	Muy alto	Promover la oportunidad

6.5 LISTA DE PROCESOS/DOCUMENTOS Y OTROS

Procesos Nivel 0 y Nivel 1
SGI
PE01 PLANEAMIENTO INSTITUCIONAL
PE02 INNOVACIÓN Y GESTIÓN POR PROCESOS
PE03 COMUNICACIONES
PE04 SOCIO AMBIENTAL
PM01 POLÍTICAS Y ESTRATEGIAS EN FISCALIZACIÓN AMBIENTAL
PM02 SUPERVISIÓN A ENTIDADES DE FISCALIZACIÓN AMBIENTAL
PM03 EVALUACIÓN AMBIENTAL
PM04 SUPERVISIÓN AMBIENTAL
PM05 FISCALIZACIÓN E INCENTIVOS
PA01 RECURSOS HUMANOS
PA02 ADMINISTRACIÓN Y FINANZAS
PA03 TECNOLOGÍAS DE LA INFORMACIÓN
PA04 ASESORÍA JURÍDICA
PE0101 Elaboración o Modificación del Plan Estratégico Institucional
PE0102 Seguimiento del PEI y Evaluación de Resultados del PEI-POI
PE0103 Formulación, aprobación y publicación del Plan Operativo Institucional y del Presupuesto Institucional de Apertura
PE0104 Aprobación, modificación y análisis de resultados de Planes Temáticos y Planes Internos
PE0105 Certificación de crédito presupuestario y Constancia de Previsión Presupuestaria
PE0106 Formalización de Notas de Modificación Presupuestaria
PE0107 Modificación y/o Reprogramación del Plan Operativo Institucional
PE0108 Modificaciones presupuestarias internas
PE0109 Modificaciones presupuestarias externas

PE0110 Seguimiento y Evaluación del Plan Operativo Institucional
PE0111 Evaluación del Presupuesto Institucional
PE0112 Programación multianual de inversiones y programación de iniciativas de cooperación técnica y financiera
PE0113 Formulación y evaluación de Inversiones y formulación de iniciativas de cooperación técnica y financiera
PE0114 Registro de consistencia en la fase de ejecución de las inversiones
PE0115 Seguimiento de la ejecución de inversiones y de iniciativasde cooperación técnica y financiera nacional e internacional
PE0201 Elaboración, aprobación y actualización de Políticas, Lineamientos, Reglamentos, Manuales y Protocolos
PE0202 Elaboración, aprobación, difusión y actualización de los Manuales de Procedimientos
PE0203 Formulación, suscripción, ejecución y seguimiento de convenios de cooperación interinstitucional
PE0204 Elaboración y/o actualización del mapa de procesos
PE0205 Seguimiento, control y mejora de procesos
PE0206 Gestión de riesgos y oportunidades
PE0207 Evaluación de la satisfacción del cliente interno y partes interesadas externas
PE0208 Control de productos y servicios no conformes
PE0209 Gestión de auditorías internas
PE0210 Gestión de no conformidades, acciones correctivas y de mejora
PE0301 Planificación, coordinación y desarrollo de eventos dirigidos a los grupos de interés
PE0302 Identificación y participación de las partes interesadas en la fiscalización ambiental
PE0303 Administración de contenidos del Portal Institucional
PE0304 Elaboración de material informativo institucional
PE0305 Actualización del Portal de Transparencia Estándar - PTE
PE0306 Atención de consultas de el/la ciudadano/a
PE0307 Atención de solicitudes de acceso a la información pública
PE0308 Atención de sugerencias
PE0309 Atención de reclamaciones
PE0310 Administración de medios de comunicación
PE0311 Administración de redes sociales
PE0401 Evaluación de conflictividad socioambiental
PE0402 Acompañamiento socioambiental en el marco de la fiscalización ambiental
PE0403 Participación en espacios de diálogo y seguimiento al cumplimiento de compromisos
PM0101 Formulación, aprobación y evaluación posterior de propuestas de mejora regulatoria
PM0102 Formulación de opiniones a proyectos normativos externos sobre fiscalización ambiental.
PM0103 Gestión de actividades académicas
PM0104 Organización y Difusión de Información Bibliográfica Especializada
PM0105 Gestión de actividades de Promoción de investigación e Innovación
PM0106 Gestión de actividades de intercambio técnico de pares
PM0107 Gestión de denuncias ambientales
PM0108 Gestión de requerimientos de operadores de justicia
PM0109 Gestión de requerimientos de información sobre problemas ambientales de competencia de Entidades de Fiscalización Ambiental
PM0111 Gestión de la sistematización y control de calidad de información transaccional de las acciones de Fiscalización Ambiental
PM0112 Gestión de las estadísticas de las acciones de fiscalización ambiental
PM0113 Gestión de los servicios de información con componente geoespacial para la fiscalización ambiental
PM0114 Gestión del registro de administrados y unidades fiscalizables
PM0115 Gestión del registro de Instrumentos de Gestión Ambiental
PM0116 Administración y mantenimiento del Portal Interactivo de Fiscalización Ambiental
PM0201 Priorización anual para supervisión de Entidades de Fiscalización Ambiental
PM0202 Programación mensual de Entidades de Fiscalización Ambiental a supervisar
PM0203 Planificación de la supervisión a Entidades de Fiscalización Ambiental
PM0204 Ejecución de la Acción de supervisión a Entidades de Fiscalización Ambiental in situ
PM0205 Ejecución de la Acción de supervisión a Entidades de Fiscalización Ambiental en gabinete
PM0206 Elaboración de informe de supervisión
PM0207 Seguimiento posterior y cierre de expediente de supervisión a Entidades de Fiscalización Ambiental
PM0301 Programación y seguimiento de la evaluación ambiental
PM0302 Evaluación ambiental de causalidad
PM0303 Evaluación ambiental temprana
PM0304 Evaluación ambiental de seguimiento con intervención continua
PM0305 Evaluación ambiental de seguimiento con intervención periódica
PM0306 Evaluación ambiental focal
PM0307 Evaluación ambiental para la identificación de sitios impactados
PM0308 Evaluación ambiental para la identificación de pasivos ambientales del subsector de hidrocarburos
PM0309 Aprovisionamiento y devolución de equipamiento
PM0310 Aprovisionamiento de materiales
PM0311 Gestión de transporte de equipamiento, materiales y muestras
PM0312 Gestión de mantenimiento y calibración de equipamiento
PM0313 Gestión de ensayos analíticos
PM040101 Determinación y registro de la priorización de la supervisión
PM040102 Elaboración y Aprobación del Plan de Supervisión
PM040201 Ejecución de la Acción de supervisión in situ
PM040202 Ejecución de la Acción de supervisión en gabinete

PM040301 Análisis de resultados y elaboración de Informe de Supervisión
PM0501 Determinación de inicio o no inicio del Procedimiento Administrativo Sancionador
PM0502 Determinación del Informe Final de Instrucción
PM0503 Determinación de la responsabilidad administrativa o de archivo
PM0504 Atención del recurso de reconsideración
PM0505 Verificación de Medidas Correctivas
PM0506 Atención del recurso de apelación
PM0507 Atención de quejas por defecto de tramitación
PA0101 Planificación de necesidades de personal con Contrato Administrativo de Servicios
PA0102 Planificación de los instrumentos de gestión de recursos humanos
PA0103 Selección de el/la servidor/a civil
PA0104 Incorporación de practicantes y secigristas
PA0105 Vinculación de el/la servidor/a civil y practicantes
PA0106 Gestión de la inducción
PA0107 Designación de puestos de confianza
PA0108 Elaboración y aprobación del plan de desarrollo de las personas
PA0109 Ejecución y evaluación de la capacitación
PA0110 Administración de legajos de el/la servidor/a civil
PA0111 Registro, permisos, licencias, control de asistencia y programación de vacaciones y otras acciones
PA0112 Desvinculación de el/la servidor/a civil o practicantes
PA0113 Administración de remuneraciones, compensaciones y declaración de la planilla mensual (PLAME)
PA0114 Variación de la modalidad convencional de trabajo a las modalidades de trabajo a distancia: Teletrabajo y Trabajo Remoto
PA0115 Elaboración, ejecución y seguimiento del plan anual de bienestar social y desarrollo humano
PA0116 Gestión y seguimiento de los seguros personales
PA0117 Seguimiento de descanso médico, validación de descanso médico y subsidio
PA0118 Elaboración de la matriz de identificación de peligros, evaluación de riesgos y determinación de controles relativos a la seguridad y salud en el trabajo - IPERC
PA0119 Vigilancia médico ocupacional
PA0120 Reporte e Investigación de incidentes, accidentes y enfermedades ocupacionales
PA0121 Inspecciones de Seguridad y Salud en el Trabajo y Gestión de No Conformidades, Acciones Correctivas y Preventivas
PA0122 Procedimiento administrativo disciplinario
PA0123 Atención de denuncias por actos de corrupción y reporte de inquietudes del Sistema de Gestión Antisoborno, en el OEFA
PA0201 Gestión de las actuaciones preparatorias de los procedimientos de selección
PA0202 Contrataciones de bienes y servicios con procedimiento de selección
PA0203 Contrataciones de bienes y servicios por adjudicación sin procedimiento
PA0204 Atención de los recursos de apelación en las contrataciones de bienes y servicios
PA0205 Seguimiento a los contratos
PA0206 Ampliaciones de plazo a las contrataciones
PA0207 Adicionales y reducciones a los contratos
PA0208 Contrataciones complementarias de bienes y servicios
PA0209 Gestión del expediente para el pago de bienes y servicios
PA0210 Administración y toma de inventario de bienes de Almacén
PA0211 Actos de gestión patrimonial de los bienes muebles de propiedad del OEFA
PA0212 Pérdida, robo, hurto o daño de bienes muebles
PA0213 Inventario de los bienes muebles
PA0214 Administración de los vehículos de transporte
PA0215 Mantenimiento de activos fijos e infraestructura
PA0216 Contratación de boletos aéreos nacionales
PA0217 Apertura, atención, reposición de fondos y liquidación de caja chica
PA0218 Arqueo de caja chica
PA0219 Registro de ingresos
PA0220 Control de la recaudación y determinación de la deuda
PA0221 Fiscalización de Sujetos de aporte por regulación
PA0222 Procedimientos no contenciosos tributarios
PA0223 Procedimientos contenciosos tributarios
PA0224 Solicitud de viáticos, pasajes y otros gastos por comisión de servicios en el territorio nacional
PA0225 Solicitud de encargos
PA0226 Solicitud de viáticos por comisión de servicios al exterior
PA0227 Rendición de cuentas de anticipos otorgados
PA0228 Pago a proveedores y planilla
PA0229 Gestión de garantías
PA0230 Control y devolución de fondos de garantía
PA0231 Registro de cuentas de orden y cuentas por cobrar
PA0232 Registro contable de activos fijos, activos intangibles, bienes no depreciables y bienes de consumo
PA0233 Integración contable y emisión de estados financieros y presupuestarios
PA0234 Ejecución Coactiva
PA0235 Ingreso y digitalización de documentos
PA0236 Mensajería y notificación de documentos
PA0237 Organización y transferencia documental
PA0238 Servicio de solicitud de documentos

PA0239 Habilitación de servicios y registro en la Plataforma Única de Servicios Digitales
PA0301 Formulación e implementación de proyecto tecnológico
PA0302 Desarrollo y mantenimiento de sistemas de información
PA0303 Atención de solicitud de servicio de tecnologías de la información
PA0304 Monitoreo y mantenimiento de la infraestructura de tecnologías de la información
PA0305 Monitoreo y control de seguridad informática
PA0401 Emisión de opiniones legales y absolución de consultas jurídicas
PA0402 Alerta de normas legales
PA0403 Sistematización de dispositivos jurídicos
PA0404 Atención de Derechos ARCO y Derecho de Información
Otros (Describir)

Anexo 1 - Inventario de activos

Paso 1: Inventario de activos

Las actividades de esta etapa consisten en identificar los activos de información y sus características para generar un inventario que permita definir la valoración y el nivel de criticidad de los activos.

1. Identificar los activos que forman parte del alcance del SGSI

El responsable de los activos de información identifica los activos de información que su proceso requiere, utiliza, depende, almacena, transmite, entre otros, y los registra en la Matriz de Riesgos de Seguridad de la Información.

1.1. **Código de identificación del activo:** Identificador o nomenclatura del activo de información.
Por ejemplo, PA03-01 (código de proceso-código de activo). Se registra un número correlativo por cada línea-activo de información.

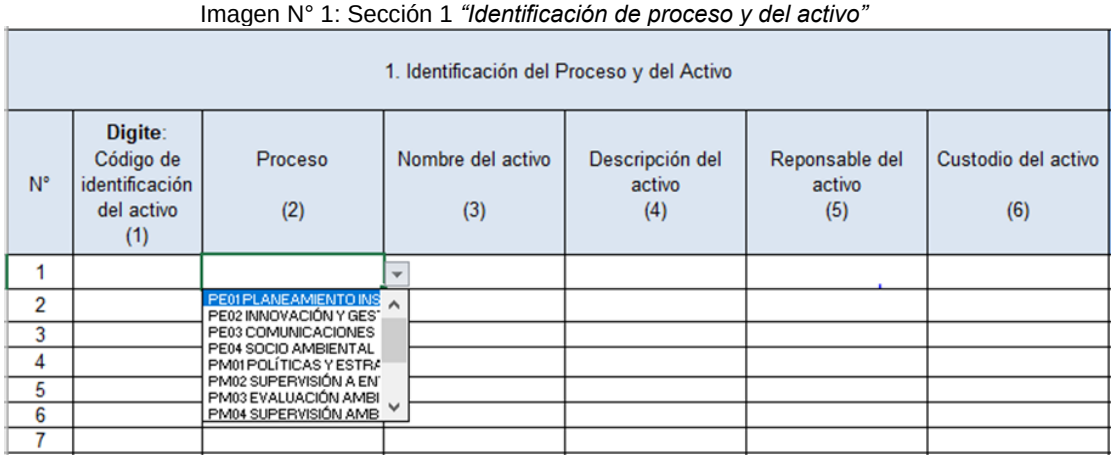
1.2. **Proceso:** Nombre del proceso a identificar sus activos de información.

1.3. **Nombre del activo:** Nombre del activo de la información que permita identificar claramente el activo al que se hace referencia.
Por ejemplo: archivo de planillas de pago.

1.4. **Descripción del activo:** Reseña del uso, funcionalidad u otro del activo de información.

1.5. **Custodio de activo de la información:** Persona que cuente con la responsabilidad asignada y aprobada por la dirección para controlar todo el ciclo de vida de un activo en su proceso. El responsable identificado no necesariamente tiene derechos de propiedad del activo.

Imagen N° 1: Sección 1 *"Identificación de proceso y del activo"*



2. Establecer las características del activo

En esta etapa se definen aquellas características de activos según categoría, tipo, clasificación, entre otros, según los siguientes criterios.

2.1. Categoría del activo: Indica el tipo de activo de información. Por ejemplo: Información, físico, servicio, personal, software.

A continuación, se describen las categorías de los activos de información:

- **Información:** Conjunto de datos físicos o electrónicos que tiene valor para el proceso y/o área.
- **Software:** Programas, sistemas de información, aplicaciones, entre otro aplicativo que contenga la lógica del proceso.
- **Activos físicos:** Soporte físico que es relevante para el procesamiento, comunicación, almacenamiento y/u operación del activo.
- **Servicios:** Conjunto de actividades internas o externas que brindan funcionalidades y requerimientos específicos.
- **Personal:** Recurso humano que dispone información y/o experiencia importante que no se encuentra en algún otro medio.

2.2. Tipo de activo según categoría: Se detallan los tipos de activos de información según la categoría a la que pertenecen.

Categoría	Tipo de activo
Información	Información electrónica
	Información escrita
	Información hablada
	Otro tipo de información
Software	Software comercial o herramientas, utilitarios
	Software desarrollado por terceros
	Software desarrollado internamente
	Software de administración de base de datos
	Otro software
Físicos	Equipo de procesamiento
	Equipo de comunicaciones
	Medio de almacenamiento
	Mobiliario y equipamiento
	Otros equipos
Servicios	Procesamiento y comunicaciones
	Servicios generales
	Otros servicios
Personal	Clientes/administrados
	Servidores/as civiles, Colaboradores
	Alta Dirección
	Entidades Públicas
	Personal externo/proveedores

2.3. Clasificación del uso del activo: Describe la clasificación de uso del activo en la entidad. Por ejemplo: Público, uso interno, confidencial o restringida.

Clasificación de uso	Descripción de Clasificación de uso
Pública	Son todos aquellos activos que se presumen públicos, y que pueden ser accedidos tanto por miembros de la organización como por personas externas a ella (público en general), sin estar sujetos a ningún control.
Reservada	Son todos aquellos activos que son reservados exclusivamente por personal interno y cuyo acceso excepcional por parte de personal externo (auditores, entidades reguladoras, consultores externos) puede darse pero se encuentra regulado y sujeto a condiciones específicas de acceso.
Secreta	Son todos aquellos activos que pertenecen a un proceso o unidad orgánica y que por su naturaleza son accedidos por el personal del área o proceso específico y cuyo acceso excepcional por parte de personal externo (auditores, entidades reguladoras, consultores externos) puede darse pero se encuentra regulado y sujeto a condiciones específicas de acceso.
Confidencial	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 o nivel específico de poder dentro de la organización

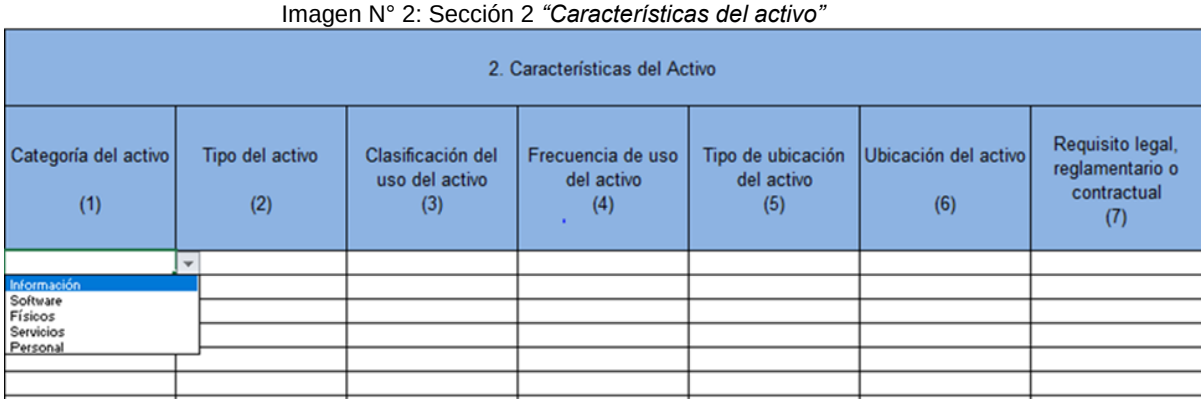
2.4. Frecuencia de uso: Indica cada cuanto tiempo se usa el activo de información. Por ejemplo: Diario, semanal, quincenal, mensual, anual, eventual.

2.5. Tipo de ubicación del activo: Ubicación física o lógica del activo.

2.6. Ubicación del activo: Lugar, dirección física o lógica donde se ubica el activo. Por ejemplo: dirección de una sede, dirección de un proveedor, una oficina, dirección lógica en un servidor (ruta) entre otros.

2.7. Requisito legal, reglamentario o contractual: Se coloca sólo cuando la existencia del activo de información se debe al cumplimiento de requisitos legales, regulatorios o contractuales.

Imagen N° 2: Sección 2 *"Características del activo"*



3. Criticidad y tasación del Activo (Valoración de los activos de información)

Los activos de información tienen distintos niveles de prioridad y relevancia para el OEFA, la discriminación de aquellos que son más críticos que otros están en función de su confidencialidad, integridad y disponibilidad; por ello, se establece una fórmula de valoración del activo de información.

- **Confidencialidad (C):** Grado de confidencialidad requerido por el activo de información.
- **Disponibilidad (D):** Grado de disponibilidad requerido por el activo de información.
- **Integridad (I):** Grado de integridad requerido por el activo de información.

- **Valor del activo:** Valoración del activo para la entidad en función al grado de confidencialidad, integridad y confidencialidad.

Imagen N° 3: Sección 3 *"Criticidad y tasación del activo"*

La siguiente fórmula permite valorar el activo de información (promedio) sobre la base de las características de confidencialidad, integridad y disponibilidad del activo de información:

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

Asimismo, en la Tabla N° 1: Niveles de valorización de los activos, se definen los valores y la descripción de cada nivel de valorización de los activos de información.

Tabla N° 1: Niveles de valorización de los activos

Valor	Confidencialidad	Integridad	Disponibilidad
Muy alto 4	La información asociada al activo solo es accedida por la Alta Dirección, su divulgación sería catastrófica para la Entidad	El activo no puede tolerar pérdida o alteración de todos sus componentes, la alteración de su integridad comprometería varios procesos de la Entidad.	El activo siempre debe estar disponible, pues su carencia afectaría el flujo de producción de varios procesos de la Entidad.
Alto 3	La información asociada al activo es restringida y solo personal de un proyecto específico puede acceder a ella, su divulgación comprometería la reputación e imagen de la Entidad.	El activo no puede tolerar una alteración de alguno de sus componentes, la alteración de su integridad afectaría parte de la información de los procesos de la Entidad.	El activo no puede estar *"no disponible"* por más de un día, su carencia afectaría la operación de los procesos de la Entidad

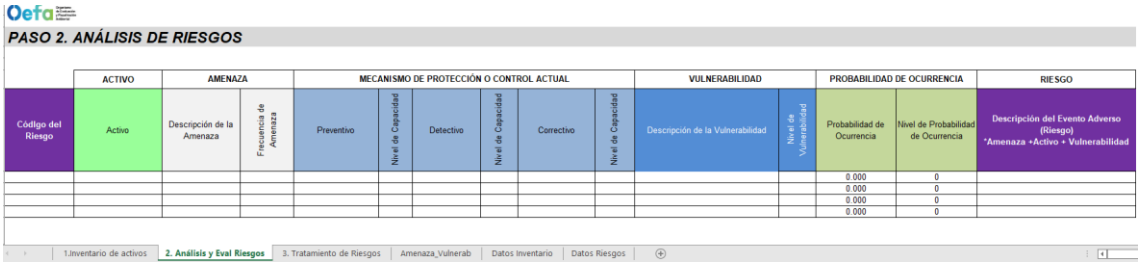
Valor	Confidencialidad	Integridad	Disponibilidad
Medio 2	La información asociada al activo es confidencial o interna y solo personal de algunas áreas del OEFA pueden acceder a ella, su divulgación afectaría los procesos de las áreas involucradas.	El activo puede tolerar una alteración media de sus componentes, la alteración de su integridad afectaría una o más actividades importantes de los procesos de la Entidad.	El activo puede estar no disponible por más de dos días, su carencia afectaría una o más actividades de los procesos de la Entidad.
Bajo 1	La información asociada al activo es de uso general y cualquier colaborador/a puede acceder a ella, pues no impacta a la Entidad.	El activo puede tolerar una alteración menor de sus componentes, la alteración de integridad afectaría una actividad menor en los procesos de la Entidad.	El activo puede estar no disponible por más de tres días, su carencia afectaría una actividad menor en los procesos de la Entidad.

Anexo 2 - Análisis y Evaluación de Riesgos

Paso 2: Análisis de Riesgo

El análisis de riesgos de seguridad de la información se desarrolla con aquellos activos de información que obtuvieron una valoración de "**alto" o "muy alto"** en el inventario de activos; en atención a ello; los activos de información que se analicen con valoración de "alto" o "muy alto" deben contar con un identificador o código de riesgo.

Imagen N° 1: Matriz de análisis y evaluación de riesgos de SI - Paso 2: Análisis de riesgos



1. Código de riesgo

Contiene la siguiente nomenclatura:
Los cuatro primeros caracteres corresponden al código del proceso, seguido de la letra *"R"* y el número correlativo de la línea de análisis de riesgo. Ej, PM04* - R - 01
(*) PM04: Supervisión Ambiental

2. Amenaza sobre los activos de la información

En este paso se identifican y registran las vulnerabilidades de los activos de información. Los activos de información están sujetos a fuentes de amenazas que explotan sus vulnerabilidades; a continuación, se detallan algunos ejemplos de fuentes de amenazas:

- Desastres naturales: Incendio, terremoto, avalancha, huayco, inundación, tornado, viento, volcán, tsunami, tormenta.
- Humanas: Divulgación de información por correo electrónico, sabotaje, terrorismo, acciones de los hackers, ingeniería social, errores de mantenimiento, huelga, errores de usuario, etc.
- Tecnológicas: Fuga de información, virus y malware, caída de red, sobre tráfico, falla de sistemas de información (hardware y software), entre otros de invierno, tormenta solar, tormenta eléctrica/relámpago, entre otros.

La frecuencia de la amenaza se detalla según los siguientes valores:

Tabla N° 1: Escala de frecuencia de amenazas

Nivel	Frecuencia
Extremo 4	El evento podría ocurrir de manera diaria o semanal.
Alto 3	El evento podría ocurrir de manera quincenal o mensual.
Medio 2	El evento podría ocurrir entre 3 o 4 veces al año.
Bajo 1	El evento podría presentarse al menos 1 vez en el año.

3. Mecanismos de protección o controles actuales de los activos de información

En el contexto de los riesgos, la aplicación de un control desalienta la ocurrencia de una amenaza (reduce la probabilidad de ocurrencia) o mitiga el impacto de la misma (mitiga el impacto del daño).

Para ello, resulta necesario identificar los controles de los activos de información existentes e implementados, de acuerdo con el siguiente detalle:

- Controles Preventivos: Aquellos controles que están involucrados dentro de los procesos y tienen como propósito evitar la ocurrencia y frecuencia de una amenaza.
- Controles Detectivos: Controles que detecta la ocurrencia de una amenaza. Supone que la amenaza ya se ha materializado, pero por si mismo no la corrige.
- Controles Correctivos: Control que corrige el impacto de una amenaza antes de que produzca pérdidas relevantes. Supone que la amenaza ya se ha materializado pero que se corrige.

*Para la identificación de controles actuales, se toma como referencia la hoja *"Inventario de controles"* de la PA0306-F01*"Matriz de riesgos de seguridad de la información"*.

Por cada control identificado se debe valorar su capacidad según la Tabla N° 2 "*Niveles de capacidad de los controles"* que se detalla a continuación:

Tabla N° 2: Niveles de capacidad de los controles

Valor	Nivel	Descripción
5	Optimizado	El control cuenta con marcos de uso, hitos, responsables y se monitorea a través de la recopilación y análisis de mediciones, a partir de las cuales se aplican mejoras.
4	Predecible	El control cuenta con marcos de uso, hitos, responsables y se monitorea a través de la recopilación y análisis de mediciones.
3	Definido	El control implementado cuenta con una especificación o marco de su uso o aplicación permanente con hitos y responsables designados.
2	Documentado	El control implementado cuenta con una declaración que obliga su aplicación permanente.
1	Realizado	Control implementado no riguroso ni documentado.

4. Vulnerabilidades de los activos de información

En esta actividad el/la responsable del activo identifica las vulnerabilidades de los activos de información según la amenaza y las registra en el Formato PA0306-F01: *"Matriz de riesgos de seguridad de la información"*.

Determina el nivel de vulnerabilidad acorde a la siguiente fórmula:

$$\text{Nivel de Vulnerabilidad} = 5 - \frac{\text{efectividad de controles Preventivos} + \text{efectividad de controles Detectivos} + \text{Nivel de efectividad de controles Correctivos}}{3}$$

Los valores obtenidos se muestran en la Tabla N° 3 "*Escalas que definen los niveles de vulnerabilidad"*, de acuerdo con el siguiente detalle:

Tabla N° 3: Escalas que definen los niveles de vulnerabilidad

Nivel	Descripción
Extremo 4	No existen controles de seguridad de la información que permitan mitigar la amenaza.
Alto 3	Existen controles, pero no son los suficientes para mitigar la amenaza.
Medio 2	Existen controles que mitigan parcialmente la amenaza y/o reducen el impacto generado.
Bajo 1	Los controles necesarios se encuentran implementados y permiten mitigar la amenaza.

5. Probabilidad de ocurrencia del riesgo

La probabilidad de ocurrencia del riesgo se calcula automáticamente en la Matriz de Riesgos de Seguridad de la Información, promediando el nivel de vulnerabilidad y la frecuencia de la amenaza, de acuerdo con la siguiente fórmula:

$$\text{Probabilidad de Ocurrencia} = \frac{\text{Nivel de Vulnerabilidad} + \text{Frecuencia de Amanaza}}{2}$$

Para determinar si una amenaza es significativa respecto a un activo, se identifica la probabilidad de ocurrencia dentro del rango del nivel de ocurrencia establecido según en la Tabla N° 4 "*Tasación de la probabilidad de ocurrencia del riesgo"*, detallada a continuación:

Tabla N° 4: Tasación de la probabilidad de ocurrencia del riesgo

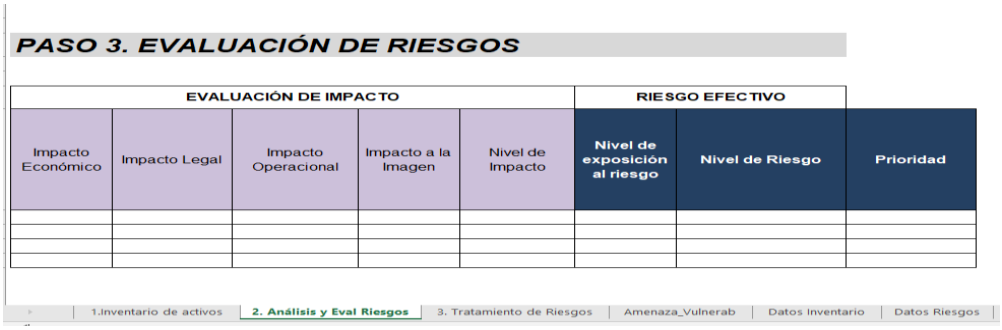
Valor	Nivel
3.01 - 4.00	Muy Alto
2.01 - 3.00	Alto
1.01 - 2.00	Medio
1.00 - 1.00	Bajo

Para nombrar o enunciar el riesgo en función a la definición de la amenaza y la descripción de la vulnerabilidad.

Paso 3: Evaluación de Riesgo

Para la evaluación de riesgos, se determina la evaluación de impacto; de tal manera que la Matriz de Riesgos de Seguridad de la Información, calcula el riesgo efectivo y la prioridad según niveles de riesgo.

Imagen N° 2: Matriz de análisis y evaluación de riesgos de SI - Paso 3: Evaluación de riesgos



1. Evaluación del impacto

Es necesario determinar el impacto, así como el nivel de afectación a la Entidad, respecto de los distintos factores relevantes como el ámbito legal, económico, operacional e imagen. Para tales efectos, se establecen como factores relevantes los mencionados en la siguiente tabla:

Tabla N° 5: Factores por considerar en el impacto en la entidad

Factor	Descripción
Económico	Grado de afectación sobre la disponibilidad presupuestaria y nivel de recaudación (Multas o Aporte por Regulación y Ejecución Coactiva.
Legal	Estimación de la probabilidad de que el riesgo identificado pueda producir el incumplimiento del marco legal aplicable o disposiciones contractuales
Operacional	Estimación de la probabilidad de que el riesgo identificado pueda producir la paralización de operaciones de la Entidad
Imagen Institucional	Grado de descenso de prestigio y credibilidad de la Entidad

A continuación, se detallan los tipos de impacto (económico, operacional, legal, imagen) y su efecto:

Tabla N° 6: Correspondencia entre factores de riesgos de seguridad de la información, tipos de impacto y valorización del tipo de impacto

Valor		Impacto Económico	Impacto Operacional	Impacto Legal	Impacto a la Imagen
4	Muy Alto (4)	Pérdidas en millones de soles.	No se pueden reanudar las operaciones.	Se afecta la permanencia de las autoridades de Alta Dirección del OEFA (CD, PCD, GEG).	Deterioro abrupto de la imagen de la Entidad.
3	Alto (3)	Pérdidas en cientos de miles de soles.	Las operaciones tardan meses en reanudarse, suspendiendo los servicios de supervisión ambiental y de TI.	Se afecta la permanencia de personal clave de uno de los órganos de línea del OEFA.	Deterioro de la imagen de diversos Órganos de Línea del OEFA.
2	Medio (2)	Pérdidas en miles de soles.	Las operaciones tardan días en reanudarse, suspendiendo parcialmente los servicios misionales.	Se afecta al personal perteneciente a la Alta Dirección en el OEFA.	Deterioro de la imagen de diversos Órganos de Apoyo o Asesoramiento del OEFA.
1	Bajo (1)	Pérdidas mínimas que no afectan al OEFA	Se opera parcialmente, priorizando los servicios misionales.	Se afecta a los/as colaboradores/as del OEFA.	Afectación mínima de la imagen de los/as colaboradores/as.

El nivel de impacto se obtiene con la siguiente fórmula:

$$\text{Nivel de Impacto} = \frac{\text{ECONÓMICO} + \text{LEGAL} + \text{OPERACIONAL} + \text{IMAGEN}}{4}$$

2. Riesgo efectivo

El nivel de exposición al riesgo se obtiene promediando el resultado del nivel de impacto y la probabilidad de ocurrencia del riesgo, con la siguiente fórmula:

$$\text{Nivel de Exposición al Riesgo} = \frac{\text{Nivel de Impacto} + \text{Probabilidad de Ocurrencia}}{2}$$

Según el resultado obtenido se identifica el nivel de exposición al riesgo:

Tabla N° 7: Tasación del nivel de exposición al riesgo

Valor	Nivel
3.50 - 4.00	Muy Alto
2.51 - 3.49	Alto
1.51 - 2.50	Medio
1.00 - 1.50	Bajo

A continuación, la representación gráfica del mapa de riesgos o calor.

Imagen N° 3: Mapa de calor de riesgos

		PROBABILIDAD			
		1	2	3	4
IMPACTO	4	2.50	3.00	3.50	4.00
	3	2.00	2.50	3.00	3.50
	2	1.50	2.00	2.50	3.00
	1	1.00	1.50	2.00	2.50

La priorización del tratamiento de riesgos se considera como:

Tabla N° 8: Priorización de nivel de riesgos

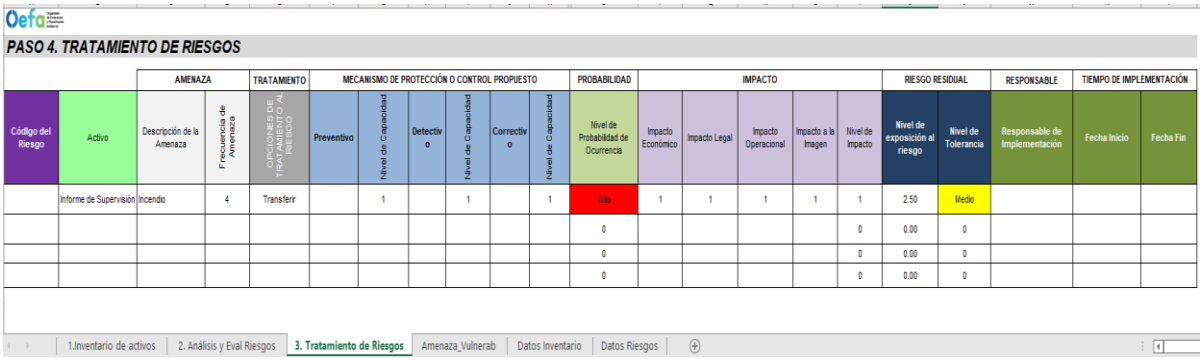
Prioridad	Nivel	Descripción
1	Muy Alto	Plazo de implementación de los planes de acción de hasta 6 meses
2	Alto	Plazo de implementación de los planes de acción de de hasta 12 meses
3	Medio	No requiere planes de acción adicionales
4	Bajo	No requiere planes de acción adicionales

Anexo 3 - Tratamiento de riesgos

Paso 4: Tratamiento de Riesgo

Para el tratamiento del riesgo se considera la inclusión de controles adicionales o a través de la mejora de controles existentes. El tratamiento se realiza sobre los riesgos cuyo resultado en la evaluación obtuvieron nivel de riesgo ***"alto"*** y ***"muy alto"***.

Imagen N° 1: Matriz de análisis y evaluación de riesgos de SI/ Tratamiento de riesgos



PASO 4. TRATAMIENTO DE RIESGOS

		AMENAZA		TRATAMIENTO	MECANISMO DE PROTECCIÓN O CONTROL PROPUESTO						PROBABILIDAD	IMPACTO					RIESGO RESIDUAL		RESPONSABLE	TIEMPO DE IMPLEMENTACIÓN	
Código del Riesgo	Activo	Descripción de la Amenaza	Frecuencia de Amenaza	OPCIONES DE TRATAMIENTO A RIESGO	Preventivo	Nivel de Capacidad	Detectivo	Nivel de Capacidad	Correctivo	Nivel de Capacidad	Nivel de Probabilidad de Ocurrencia	Impacto Económico	Impacto Legal	Impacto Operacional	Impacto a la Imagen	Nivel de Impacto	Nivel de exposición al riesgo	Nivel de Tolerancia	Responsable de Implementación	Fecha Inicio	Fecha Fin
	Informe de Supervisión	Incendio	4	Transferir		1		1		1	Alto	1	1	1	1	1	2.50	Medio			
											0					0	0.00	0			
											0					0	0.00	0			
											0					0	0.00	0			

1.Inventario de activos | 2. Análisis y Eval Riesgos | 3. Tratamiento de Riesgos | Amenaza_Vulnerab | Datos Inventario | Datos Riesgos

1. Tratamiento de riesgo

Los tipos de tratamientos que se aplican a los riesgos de seguridad de la información, así como las razones para aplicar un tipo de tratamiento específico se describen a continuación:

Tabla N° 1: Descripción y sustento para el Tratamiento de riesgos

Tipo de tratamiento de riesgo	Descripción	¿Cuándo seleccionarlo?
Evitar	Dejar de realizar la actividad que genera el riesgo debido a que el nivel de riesgo es inaceptable.	Se selecciona esta alternativa cuando el beneficio de implementar un control sea menor al costo del riesgo inherente y sus posibles consecuencias.
Reducir (mitigar)	Establecer controles para disminuir la probabilidad de ocurrencia del riesgo.	Se selecciona esta alternativa cuando el beneficio de implementar un control sea mayor al costo del riesgo inherente, y la Entidad se encuentre en la capacidad de realizar el tratamiento del riesgo.
Transferir	Transferir a un/a tercero/a con la capacidad financiera o especialización necesaria para administrar adecuadamente el riesgo, o enfrentar las pérdidas originadas ante la ocurrencia de la adversidad.	Se selecciona esta alternativa cuando el beneficio de implementar un control sea mayor al costo del riesgo inherente y, un/a tercero/a tenga una mayor capacidad para realizar el tratamiento del riesgo, debido a su especialización, infraestructura, entre otros factores.
Retener (aceptar)	Aceptar el riesgo en su presente nivel realizando una adecuada administración y monitoreo.	Se selecciona esta alternativa cuando cumpla con alguno de los criterios de aceptación de riesgos (ejemplo):

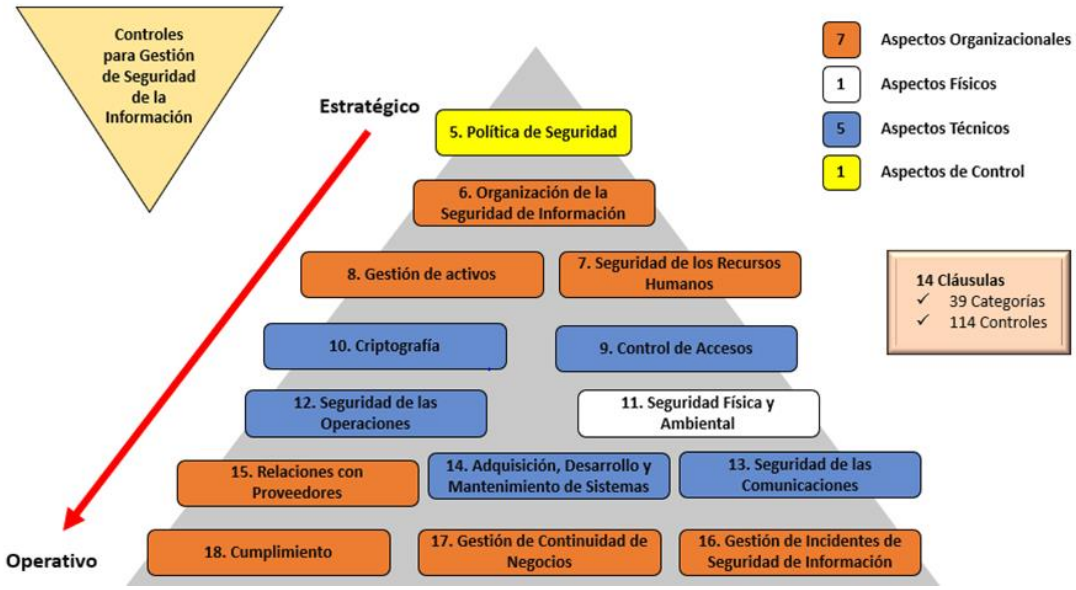
Tipo de tratamiento de riesgo	Descripción	¿Cuándo seleccionarlo?
	Para lo cual se debe verificar que cumpla con los criterios de aceptación de riesgos definidos.	a) El costo de tratar el riesgo se estima como mayor a la pérdida o impacto económico generado por la ocurrencia de este. b) El costo de implementar el control o controles está fuera de presupuesto del año en curso. c) No se dispone de recursos o se sufre recortes de presupuesto por decisión de la Alta Dirección de la entidad.

2. Mecanismos de protección o controles propuestos

En los casos en los cuales se requiera de la implementación de un control, el/la responsable del activo y el Oficial de Seguridad y Confianza digital deben realizar lo siguiente:

- Tomando como referencia la Norma ISO 27002:2013 Tecnologías de Información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información, se procede a establecer el marco de controles de seguridad de la información requeridos para tratar los riesgos.

Imagen N° 2: Cláusulas del marco de controles / Fuente: ISO 27002:2013



- Identificar y describir el control que se requiere para mitigar el riesgo, considerando los controles del Formato PA0306-F02 *"Declaración de aplicabilidad"*.
- Planificar la implementación del control.
- Documentar el control mediante el registro de los siguientes datos:
  - Responsable de la implementación.
  - Tiempo de implementación (colocar fechas específicas o rangos de tiempo).

En el contexto de los riesgos, la aplicación de un control desalienta la ocurrencia de una amenaza (reduce la probabilidad de ocurrencia) o mitiga el impacto de la misma (mitiga el impacto del daño).

Para ello, resulta necesario identificar los controles de los activos de información existentes e implementados, de acuerdo con el siguiente detalle:

- Controles Preventivos: Aquellos controles que están involucrados dentro de los procesos y tienen como propósito evitar la ocurrencia y frecuencia de una amenaza.
- Controles Detectivos: Controles que detecta la ocurrencia de una amenaza. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.
- Controles Correctivos: Control que corrige el impacto de una amenaza antes de que produzca pérdidas relevantes. Supone que la amenaza ya se ha materializado pero que se corrige.

*Para la identificación de controles propuestos, se toma como referencia la hoja *"Inventario de controles"* de la PA0306-F01*"Matriz de riesgos de seguridad de la información"*.

Por cada control identificado se debe valorar su capacidad según la Tabla N° 2 "*Niveles de capacidad de los controles"* que se detalla a continuación:

Tabla N° 2: Niveles de capacidad de los controles

Valor	Nivel	Descripción
5	Optimizado	El control cuenta con marcos de uso, hitos, responsables y se monitorea a través de la recopilación y análisis de mediciones, a partir de las cuales se aplican mejoras.
4	Predecible	El control cuenta con marcos de uso, hitos, responsables y se monitorea a través de la recopilación y análisis de mediciones.
3	Definido	El control implementado cuenta con una especificación o marco de su uso o aplicación permanente con hitos y responsables designados.
2	Documentado	El control implementado cuenta con una declaración que obliga su aplicación permanente.
1	Realizado	Control implementado no riguroso ni documentado.

3. Probabilidad

La probabilidad de ocurrencia del riesgo se calcula automáticamente en la Matriz de Riesgos de Seguridad de la Información, promediando el nivel de vulnerabilidad y la frecuencia de la amenaza, de acuerdo con la siguiente fórmula:

$$\text{Probabilidad de Ocurrencia} = \frac{\text{Nivel de Vulnerabilidad} + \text{Frecuencia de Amenaza}}{2}$$

Para determinar si una amenaza es significativa respecto a un activo, se identifica la probabilidad de ocurrencia dentro del rango del nivel de ocurrencia establecido según en

la Tabla N° 3 "*Tasación de la probabilidad de ocurrencia del riesgo*", detallada a continuación:

Tabla N° 3: Tasación de la probabilidad de ocurrencia del riesgo

Valor	Nivel
3.01 - 4.00	Muy Alto
2.01 - 3.00	Alto
1.01 - 2.00	Medio
1.00 - 1.00	Bajo

4. Impacto

Es necesario determinar el impacto, así como el nivel de afectación a la Entidad, respecto de los distintos factores relevantes como el ámbito legal, económico, operacional e imagen. Para tales efectos, se establecen como factores relevantes los mencionados en la siguiente tabla:

Tabla N° 4: Factores por considerar en el impacto en la entidad

Factor	Descripción
Económico	Grado de afectación sobre la disponibilidad presupuestaria y nivel de recaudación (Multas o Aporte por Regulación y Ejecución Coactiva.
Legal	Estimación de la probabilidad de que el riesgo identificado pueda producir el incumplimiento del marco legal aplicable o disposiciones contractuales
Operacional	Estimación de la probabilidad de que el riesgo identificado pueda producir la paralización de operaciones de la Entidad
Imagen Institucional	Grado de descenso de prestigio y credibilidad de la Entidad

A continuación, se detallan los tipos de impacto (económico, operacional, legal, imagen) y su efecto:

Tabla N° 5: Correspondencia entre factores de riesgos de seguridad de la información, tipos de impacto y valorización del tipo de impacto

Valor		Impacto Económico	Impacto Operacional	Impacto Legal	Impacto a la Imagen
4	Muy Alto (4)	Pérdidas en millones de soles.	No se pueden reanudar las operaciones.	Se afecta la permanencia de las autoridades de Alta Dirección del OEFA (CD, PCD, GEG).	Deterioro abrupto de la imagen de la Entidad.

Valor		Impacto Económico	Impacto Operacional	Impacto Legal	Impacto a la Imagen
3	Alto (3)	Pérdidas en cientos de miles de soles.	Las operaciones tardan meses en reanudarse, suspendiendo los servicios de supervisión ambiental y de TI.	Se afecta la permanencia de personal clave de uno de los órganos de línea del OEFA.	Deterioro de la imagen de diversos Órganos de Línea del OEFA.
2	Medio (2)	Pérdidas en miles de soles.	Las operaciones tardan días en reanudarse, suspendiendo parcialmente los servicios misionales.	Se afecta al personal perteneciente a la Alta Dirección en el OEFA.	Deterioro de la imagen de diversos Órganos de Apoyo o Asesoramiento del OEFA.
1	Bajo (1)	Pérdidas mínimas que no afectan al OEFA .	Se opera parcialmente, priorizando los servicios misionales.	Se afecta a los/as colaboradores/as del OEFA.	Afectación mínima de la imagen de los/as colaboradores/as.

El nivel de impacto se obtiene con la siguiente fórmula:

$$\text{Nivel de Impacto} = \frac{\text{ECONÓMICO} + \text{LEGAL} + \text{OPERACIONAL} + \text{IMAGEN}}{4}$$

5. Riesgo residual

Para estimar el riesgo residual, se considera el cambio pronosticado por la introducción de el/los control/es en las siguientes variables:
(i) nivel de amenaza,
(ii) nivel de vulnerabilidad; y,
(iii) nivel de impacto (legal, económico, operacional y de imagen).

El nivel de exposición al riesgo se obtiene promediando el resultado del nivel de impacto y la probabilidad de ocurrencia del riesgo, con la siguiente fórmula:

$$\text{Nivel de Exposición al Riesgo} = \frac{\text{Nivel de Impacto} + \text{Probabilidad de Ocurrencia}}{2}$$

Según el resultado obtenido se identifica el nivel de exposición al riesgo:

Tabla N° 6: Tasación del nivel de exposición al riesgo

Valor	Nivel
3.50 - 4.00	Muy Alto

Valor	Nivel
2.51 - 3.49	Alto
1.51 - 2.50	Medio
1.00 - 1.50	Bajo

En caso de obtener un nivel de riesgo residual considerado como no es aceptable para el OEFA (niveles alto y muy alto), entonces se reevalúan los riesgos y; de ser el caso, se establecen nuevos controles que logren mantener el riesgo residual en un nivel medio o bajo.

Anexo N° 4
Formato de Informe de seguimiento a la Matriz de riesgos y oportunidades

PERÚ | Ministerio del Ambiente | Organismo de Evaluación y Fiscalización Ambiental - OEFA | OTI: Oficina de Tecnología de Información

Decenio de [Nombre del Decenio]
[Nombre del Año]
[Nombre del Año]

INFORME N° (MODELO PROPUESTO)

A : **[NOMBRE DE EL/LA SERVIDOR/A CIVIL]**
Gerente/a General

ASUNTO : Seguimiento de la Matriz de Riesgos y Oportunidades del Sistema de Gestión de Seguridad de la Información

REFERENCIA : a) [Documento] N° [Número]-[año]-OEFA/[Siglas del Órgano]
b) [Documento] N° [Número]-[año]-OEFA/[Siglas del Órgano]

FECHA : Jesús María, [día] de [mes] de [año]

Tengo el agrado de dirigirme a usted, para informarle acerca de la Matriz de riesgos y oportunidades del Sistema de Gestión de Seguridad de la Información (SGSI, en adelante).

I. ANTECEDENTES

I.1 Mediante el Decreto Supremo N° 004-2013-PCM se aprueba la Política Nacional de Modernización de la Gestión Pública, estableciéndose cinco pilares centrales, entre los cuales se encuentran el de políticas públicas, planes estratégicos y operativos; el presupuesto para resultados y la gestión por procesos.

I.2 Mediante Resolución de la Comisión de Normalización y de Fiscalización de Barreras Comerciales No Arancelarias N° 129-2014/CNB-INDECOPI, que aprueba, entre otras Normas Técnicas Peruanas, la NTP-ISO/IEC 27001:2014 *"Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos. 2a Edición"*.

I.3 Mediante Resolución de Secretaría de Gestión Pública N° 006-2018-PCM/SGP, se aprueba la Norma Técnica N° 001-2018-SGP *"Norma Técnica para la implementación de la gestión por procesos en las entidades de la administración pública"*.

I.4 Mediante Resolución de Presidencia del Consejo Directivo Nº 077-2018-OEFA/PCD y modificatorias, se aprueba el Manual de *Procedimientos "Innovación y Gestión por Procesos"*, con el objetivo de contribuir en la formulación, implementación y evaluación de documentos de gestión, así como la implementación de la gestión por procesos y la gestión de la calidad en el Organismo de Evaluación y Fiscalización Ambiental - OEFA; que regula entre otros, el procedimiento PE0201 *"Elaboración,*

aprobación y actualización de políticas, lineamientos, reglamentos, manuales y protocolos".

I.5 Mediante Resolución de Gerencia General xxx -2022 -OEFA/GEG, se aprueba el Manual del Sistema de Gestión Integrado, con el objetivo de contar con una guía para la implementación, mantenimiento y mejora continua del Sistema de Gestión Integrado de la Entidad, que contempla el Sistema de Gestión de la Calidad, Sistema de Gestión de Seguridad de la Información y el Sistema de Gestión Antisoborno, conforme a las Normas Técnicas Peruanas ISO 9001:2015, ISO 27001:2014 e ISO 37001:2017.

I.6 La Oficina de Tecnología de Información, y el cargo de Oficial de Seguridad y Confianza Digital, es la encargada de implementar y realizar el seguimiento de la gestión de la seguridad de la información; proponiendo los correspondientes instrumentos de gestión y realizar las actividades de diseño organizacional basado en el enfoque de procesos.

I.7 **<se incluyen los hechos que originan, motivan o sustentan las acciones realizadas para la gestión de riesgos y oportunidades>**

II. OBJETO DEL PRESENTE INFORME

2.1. El presente informe tiene por objeto informar a la Gerencia General, acerca de las acciones y resultados producto del monitoreo y seguimiento a la Matriz de Riesgos de seguridad de información y Matriz de Oportunidades del SGSI que incluye la implementación del plan de acción de gestión de riesgos y oportunidades, así como la implementación de la debida diligencia.

III. ANÁLISIS

Sobre el seguimiento al Plan de Actividades

III.1 La gestión de riesgos y oportunidades del OEFA constituye un análisis a detalle de cada activo por proceso, identificando riesgos y oportunidades para su evaluación y tratamiento, mediante el uso de criterios para la probabilidad e impacto de éstos, su correspondiente tratamiento, así como los factores de reducción aplicables por controles y asociados a procesos de debida diligencia, para aquellos riesgos que apliquen.

III.2 En ese sentido, la Oficina de Tecnología de Información, con su rol de Oficial de Seguridad y Confianza Digital procedió a realizar el respectivo seguimiento y monitoreo a las actividades del mencionado plan, cuyos plazos vencieron durante los meses de <**meses**>, por lo cual se emitió el Memorando Circular N° 00x-20xx-OEFA/OTI dirigido a los responsables de su implementación, a fin de que informen sobre el cumplimiento de su implementación y a la vez hagan llegar las evidencias que correspondan.

III.3 Es así que la **<nombre del órgano>**, emitió el Informe N° **[Número]-[año]-OEFA/[Siglas del Órgano],** mediante el cual informa las acciones realizadas en la implementación de sus actividades.

III.4 La **<nombre del órgano>**, emitió el Informe N° **[Número]-[año]-OEFA/[Siglas del Órgano],** mediante el cual informa las acciones realizadas en la implementación de sus actividades.

<se detallan los órganos y los números de los documentos>

III.5 Las cuales se detallan a continuación:

<se detallan las acciones realizadas durante el <I / II / III / IV Trimestre>

Sobre la Gestión de riesgos y oportunidades del SGSI

III.6 Se generaron riesgos de SI con diferentes niveles de criticidad, junto con sus respectivos controles actuales y adicionales, de corresponder; los cuales fueron registrados en la PA0306-F01 Matriz de Análisis y Evaluación de Riesgos SGSI, de cada proceso.

III.7 Se generaron oportunidades de SI, con diferentes niveles de criticidad, junto con su respectiva evaluación de probabilidad e impacto, de corresponder; los cuales fueron registrados en la PA0306-F03 Matriz de Oportunidades SGSI, de cada proceso.

III.8 Se realiza el seguimiento a la implementación de los controles actuales de seguridad de la información, con la evidencia correspondiente a partir de la PA0306-F02 Matriz de Declaración de aplicabilidad, que contempla la evaluación de controles técnicos, organizativos y legales sobre seguridad de información.

III.9 De la referida Matriz, se obtiene el cuadro resumen del seguimiento de riesgos por cada proceso, tal como se en la siguiente tabla:

Tabla resumen del seguimiento a la gestión de riesgos del SGSI

		MECANISMO DE PROTECCIÓN O CONTROL PROPUESTO				RESPONSABLE	TIEMPO DE IMPLEMENTACIÓN			
Código del Riesgo	**Activo**	**Descripción de la Amenaza**	**Preventivo**	**Detectivo**	**Correctivo**	**Nivel de Tolerancia**	**Responsable de Implementación**	**Fecha Inicio**	**Fecha Fin**	**Status**
	Informe de Supervisión	**Incendio**				**Medio**				

Matriz de oportunidades SGSI

Código de identificación de oportunidad	Proceso	Estado de la Medida de Control (seguimiento)		Órgano o Unidad Orgánica Responsable	Plazo de implementación		Medios de Verificación (Evidencia de implementación)	Comentarios u Observaciones
		Medida de control adicional	Medida de seguimiento al control adicional		Fecha de Inicio	Fecha de Término		

III.11 Finalmente, a fin de medir el comportamiento de la gestión de riesgos y oportunidades en el presente periodo, se realiza el análisis de los siguientes indicadores:

a) <u>Nivel de cumplimiento en el control del riesgo</u>

III.12 El indicador trimestral de nivel de cumplimiento en el control del riesgo permitió determinar el grado de cumplimiento de los controles propuestos, haciendo uso de la siguiente fórmula:

$$\%\ de\ Cumplimiento = \frac{Número\ de\ controles\ implementados\ dentro\ del\ plazo}{Número\ de\ controles\ programados} \times 100$$

III.13 Para el <**I / II / III / IV Trimestre**>, la medición efectuada del nivel de cumplimiento en el control del riesgo es <**ALTO/MEDIO/BAJO**>, lo cual indica que:

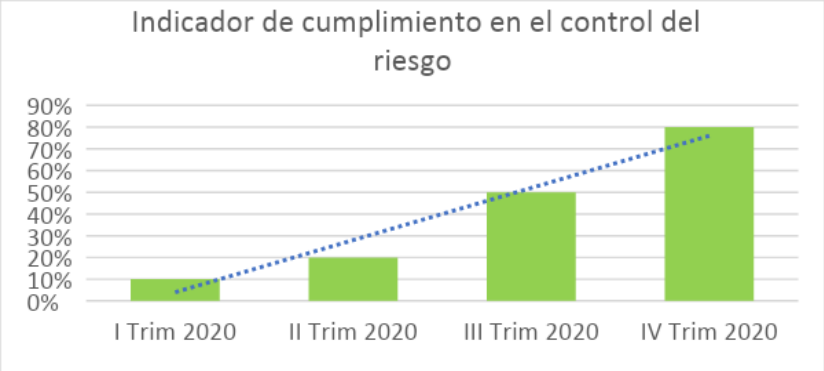
<**De ser ALTO**> El <**XX%**> de los controles adicionales fueron implementados dentro del plazo programado, debido a <**descripción breve de las causas de la implementación de los controles actuales**>.

<**De ser MEDIO**> El <**XX%**> de los controles adicionales fueron implementados dentro del plazo programado, debido a <**descripción breve de las causas de la implementación de los controles actuales**>.

<**De ser BAJO**> El <**XX%**> de los controles adicionales fueron implementados dentro del plazo programado, debido a <**descripción breve de las causas de la implementación de los controles actuales**>.

III.14 El indicador de cumplimiento en el control de riesgo, si bien es cierto, ha mejorado progresivamente, aún se encuentra a nivel de <**MEDIO**>, y requiere la revisión de recursos requeridos para poder completar la implementación pendiente que requiere

el nivel esperado de ALTO. Un retraso permanente en la mejora de este indicador podría afectar el resultado de la eficacia en la reducción del riesgo y se mostraría luego de un periodo adicional en el primer indicador.



b) <u>Nivel de cumplimiento en el control de oportunidad</u>

III.15 El indicador trimestral de nivel de cumplimiento en el control de oportunidades permitió determinar el grado de cumplimiento de los planes de acción propuestos, haciendo uso de la siguiente fórmula:

$$\%\ de\ Cumplimiento = \frac{Número\ de\ controles\ implementados\ dentro\ del\ plazo}{Número\ de\ controles\ programados} \times 100$$

III.16 Para el <**I / II / III / IV Trimestre**>, la medición efectuada del nivel de cumplimiento en el control de oportunidad es <**ALTO/MEDIO/BAJO**>, lo cual indica que:

<**De ser MUY ALTO**> El <**XX%**> de los planes de acción fueron implementados dentro del plazo programado, debido a <**descripción breve de las causas de la implementación de los planes actuales**>.

IV. CONCLUSIÓN

5.1 Se realizó el seguimiento a los siguientes procesos <**detallar procesos a los que se le realizó el seguimiento de la gestión de riesgos y oportunidades**>.

<Conclusión global de la medición de los indicadores utilizados>

V. RECOMENDACIÓN

<Detallar las acciones que se recomiendan implementar para mejorar los resultados obtenidos del informe>

Con relación a los resultados por indicador se recomienda lo siguiente:

a. Indicador de cumplimiento en el control del riesgo	b. Indicador de cumplimiento en el control de oportunidad
<**recomendación**>	< **recomendación** >

<Recomendación global de la medición de los indicadores utilizados>

Atentamente,