PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

DISEÑO DE UN SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES BASADO EN LA NORMA ISO/IEC 27701:2019

Tesis para obtener el título profesional de Ingeniero Informático

AUTOR:

Christian Diego Girbau Roque

ASESOR:

Fernando Miguel Huamán Monzón

Lima, febrero, 2022

Resumen

La presente tesis consiste en la investigación y aplicación de las regulaciones y estándares relacionados a la protección de datos personales para una institución cuyo principal servicio consiste en la provisión de evaluaciones de competencias profesionales y académicas. En la introducción de la tesis, se muestra que existe un imperativo para las organizaciones de cumplir con las regulaciones establecidas para la protección de datos personales, así como también de cumplir con los requerimientos de los titulares de los datos personales procesados por las entidades.

El proyecto consta de cinco objetivos, los cuales abarcan el diseño de procesos, políticas y marcos para cumplir con las cláusulas necesarias para un sistema de gestión de seguridad de la información, según el estándar ISO 27001:2013, incluyendo las respectivas extensiones que presenta el estándar ISO 27701:2019 para incluir la gestión de protección de datos personales. Esto implica el diseño de componentes que detallan el contexto de la organización en relación a la protección de datos personales, la gestión de riesgos de protección de datos personales, y componentes de soporte para el sistema de gestión, tales como la matriz de comunicaciones y el estándar de gestión documental. También se desarrollaron marcos para la implementación del sistema de gestión, así como para la medición, monitoreo y mejora continua de este.

A lo largo del trabajo, se muestra como los diferentes componentes del sistema de gestión interactúan entre sí para generar una mayor eficiencia en el manejo de la protección de datos personales en una organización. Del mismo modo, se muestra como el estándar ISO 27005:2018 de gestión de riesgos de seguridad de la información puede ser adaptado y tomado como marco para la gestión de riesgos en un sistema de gestión de protección de datos personales.

Tabla de Contenido

Capítulo 1. Generalidades 1

1.1 Problemática 1
1.2 Objetivos 4
1.2.1 Objetivo general 4
1.2.2 Objetivos específicos 4
1.2.3 Resultados esperados 5
1.3 Herramientas y Métodos 5
1.3.1 Mapeo de objetivos, resultados y verificación 5
1.3.2 Herramientas 7

Capítulo 2. Marco conceptual y marco regulatorio 9

2.1 Marco Conceptual 9
2.1.1 Datos personales / Información personal de identificación: 9
2.1.2 Titular de los datos personales: 9
2.1.3 Controlador de los datos personales: 9
2.1.4 Procesador de los datos personales: 9
2.1.5 Confidencialidad: 9
2.1.6 Integridad: 9
2.1.7 Disponibilidad: 10
2.1.8 Sistema de gestión 10
2.2 Marco Regulatorio 10
2.2.1 Estándares Relacionados 10
2.2.2 Ámbito legal 13

Capítulo 3. Estado del arte 15

3.1 Revisión y discusión 16
3.1.1 Patrones de privacidad 16
3.1.2 Políticas de privacidad conforme al estándar ISO 29100:2011 18
3.1.3 Heurísticas de privacidad 19
3.2 Conclusiones 20

Capítulo 4. Contexto, alcance y políticas del sistema de gestión de protección de datos personales 22

4.1 Contexto y alcance 22
4.2 Políticas del sistema de gestión 23
4.3 Conclusiones 23

Capítulo 5. Gestión de riesgos 25

5.1 Metodología de gestión de riesgos 25
5.2 Iteración inicial de la gestión de riesgos 25
5.3 Declaración de aplicabilidad 27
5.4 Conclusiones 27

Capítulo 6. Componentes de soporte 29

6.1 Matriz de comunicaciones (Anexo K) 29
6.2 Estándar de gestión documental (Anexo L) 29
6.3 Conclusiones 29

Capítulo 7. Directrices para la implementación del sistema de gestión 31

7.1 Directrices para la implementación de controles (Anexo M) 31
7.2 Cuadro de control del sistema de gestión (Anexo O) 31
7.3 Conclusiones 32

Capítulo 8. Conclusiones y trabajos futuros 33

8.1 Conclusiones 33
8.2 Trabajos futuros 34

Referencias 35

Anexos 1

Anexo A: Plan de proyecto 1

Anexo B: Informe de contexto 7

Anexo C: Procesos del alcance del sistema de gestión de protección de datos personales 10

Anexo D: Políticas de privacidad y seguridad de la información 12

Anexo E: Metodología de gestión de riesgos 18

Anexo F: Listado de activos de información 31

Anexo G: Listado de amenazas y vulnerabilidades de privacidad y seguridad de la información 34

Anexo H: Identificación, análisis y evaluación de escenarios de incidentes 38

Anexo I: Controles de privacidad y seguridad de la información propuestos 42

Anexo J: Declaración de aplicabilidad 44

Anexo K: Matriz de comunicación 64

Anexo L: Estándar de gestión documental del sistema de gestión 66

Anexo M: Guía de implementación de controles de ISO/IEC 27001:2013 e ISO/IEC 27701:2019 68

Anexo N: Políticas específicas del sistema de gestión..... 75

Anexo O: Cuadro de control del sistema de gestión..... 82

Anexo P: Cuadro de validación de entregables 86

Índice de Figuras

Figura 3.1 Interfaz gráfica del catálogo online de patrones de privacidad. Adaptado de (Drozd, 2016) 18

Figura 3.2 Mapeo para la sección "What information we collect" de la política de privacidad de LinkedIn. Los símbolos de "+" indican que la cobertura del principio fue de mayor grado, mientras que el símbolo de "°" indica que la cobertura fue parcial. 19

Índice de Tablas

Tabla 3.1 Criterios de inclusión y exclusión 15

Tabla 3.2 Mapeo de patrones de privacidad con los once principios establecidos por ISO 29100 17

Tabla 3.3 Heurísticas de privacidad 20

Capítulo 1. Generalidades

1.1 Problemática

La rápida difusión de las tecnologías de información y comunicación supusieron muchos cambios para la sociedad, tales como la facilidad de comunicación a larga distancia, fácil acceso a información, la mejora de los servicios y el acceso a estos desde la comodidad de un hogar (Pfeiffer, 2011). Si bien es posible argumentar que muchos de estos cambios dieron lugar a una mejor calidad de vida (Pfeiffer, 2011), esta nueva era supuso también nuevos retos y problemáticas. Uno de estos retos es el de la gestión de la privacidad. Entiéndase por privacidad a la rama de la seguridad de la información encargada del correcto manejo del ciclo de vida de los datos (NIST).

La importancia de la privacidad para las personas se hace notar dado que la violación de esta puede traer consecuencias como el robo de identidad, la privación de la capacidad para un individuo para gestionar su reputación, vulnerabilidad ante avisos publicitarios dirigidos, entre otras. A raíz de esto, se dieron a lo largo de los años numerosos congresos alrededor del mundo con el fin de definir estándares y regulaciones para la protección de la privacidad (Acosta, 2017), los cuales dieron origen a las diversas normativas que existen hoy en día.

En el Perú, particularmente, se cuenta con la Ley de Protección de Datos Personales (Ley 29733), la cual establece obligaciones y restricciones para aquellas entidades que administren información personal. Entre estas obligaciones está obtener el consentimiento del titular de esta información para el procesamiento de esta, así como mantenerlo informado sobre el uso de la información. El titular posee además derechos sobre la modificación de sus datos personales y a ser indemnizado en caso de que se incumpla esta ley. Además de esto, se imponen sanciones por el incumplimiento de la ley en forma de multas que pueden alcanzar hasta un valor de 100 UIT según la gravedad del incumplimiento. (Ley de Protección de Datos Personales, 2011)

La aplicación de esta ley dio lugar a la Autoridad Nacional de Protección de Datos Personales en el año 2011, la cual se encarga de brindar las directivas relacionadas a la protección de datos personales, así como de otorgar las sanciones apropiadas para las organizaciones que incumplen con la ley de protección de datos personales. Hasta la fecha, ha sancionado a múltiples organizaciones por incumplir con las regulaciones impuestas para la protección de datos personales. Un caso reciente de esto es el de una entidad bancaria que fue multada con 40 UITs debido a que sufrió un ciberataque que permitió a los atacantes acceder a números de tarjetas, cuentas y saldos de un grupo de clientes (Ministerio de justicia, 2020). Otros casos conocidos en el Perú son el de un hospital de emergencias, por tratar y divulgar datos personales de un paciente sin su consentimiento (Autoridad nacional de protección de datos personales, 2020), y el de la ONPE, la cual recientemente fue multada debido a una brecha de seguridad la cual expuso la información grandes cantidades de votantes (Guerrero, 2019).

Resguardar la privacidad de los datos personales implica garantizar la confidencialidad de estos; es decir, asegurar que los datos solo puedan ser visibles por aquellas partes que tengan la autorización para verlos. Es de esta forma que la privacidad de datos personales es un concepto ligado al de seguridad de información.

En respuesta a esta necesidad de seguridad de información, se publicó en el año 2014 la norma técnica peruana NTP ISO/IEC 27001:2013, y se impuso su uso por entidades públicas en el año 2016, con lo cual se contempla la implementación de sistemas de gestión de la seguridad de la información para estas entidades, con la finalidad de disminuir los riesgos que vienen asociados a la gestión de seguridad de la información. (Presidencia del consejo de ministros, 2016)

Existen además otras leyes relacionadas a la seguridad de la información que afectan a las empresas en el Perú. Entre estas se tiene a la Ley de Delitos Informáticos, la cual establece los tipos de delito informático y sanciones respectivas (Ley de Delitos Informáticos, 2013). Todas

estas normativas en conjunto establecen un imperativo legal para las organizaciones de velar por la confidencialidad de los datos que procesan.

Casos como los mencionados anteriormente dan a entender que es necesario implementar el uso eficaz de tecnologías con la finalidad de proteger la información personal (como, por ejemplo, la implementación de la criptografía). Sin embargo, ciertos casos en los cuales la violación de la privacidad se debió a un incumplimiento de políticas de gestión de datos y no a un ataque a los sistemas, hacen evidente que para resguardar la privacidad de los usuarios de un sistema de información no basta con ceñirse solamente a la aplicación de tecnologías de información para resguardar la seguridad de los datos personales, sino que también es necesaria la introducción de regulaciones y políticas organizacionales para garantizar dicha privacidad.

En el Perú, así como en muchos otros países del mundo, la crisis generada por la pandemia de COVID-19 ha funcionado como un catalizador para la transformación digital (Zelada, 2021). Esto a su vez agranda la necesidad de garantizar la protección de datos personales de los sistemas de información que los almacenan.

Se hace evidente, entonces, la necesidad de una solución que responda tanto a las necesidades tecnológicas como administrativas de una organización con el fin de mejorar la gestión de la privacidad de datos personales. La solución que se propone en esta tesis es un sistema de gestión de la protección de datos personales. Un sistema de gestión es la forma en la que una organización administra las partes interrelacionadas del negocio para lograr sus objetivos. Si bien existen medidas que se están tomando por diversas organizaciones para gestionar la privacidad de datos personales, un sistema de gestión puede traer nuevos beneficios tales como el uso eficiente de recursos, mejoras en la gestión de riesgos y la capacidad de entregar servicios y productos mejorados y consistentes, agregando de esta forma valor a la organización. (“Management system standards”, s/f)

El sistema de gestión propuesto estará basado en el estándar ISO/IEC 27701:2019, el cual establece los requisitos y controles necesarios para la implementación y mantenimiento de un sistema de gestión de protección de datos personales como extensión de un sistema de gestión de seguridad de información. (ISO, 2019)

Por último, cabe recalcar que un sistema de gestión de protección de datos personales es un sistema de gestión de seguridad de la información que aborda la protección de datos personales, la cual es potencialmente afectada por el procesamiento de estos (ISO, 2019). Esto significa que el sistema a diseñar, no solo tomará en cuenta al estándar ISO/IEC 27701:2019, sino también al estándar ISO/IEC 27001:2013, el cual será la primera base para este diseño.

1.2 Objetivos

1.2.1 Objetivo general

Diseñar un sistema de gestión de protección de datos personales basado en la norma ISO/IEC 27701:2019

1.2.2 Objetivos específicos

O 1. Establecer el contexto de la organización y las políticas de seguridad de la información y privacidad

O 2. Diseñar componentes para la gestión de riesgos para el sistema de gestión de protección de datos personales

O 3. Elaborar componentes de soporte del sistema de gestión de protección de datos personales

O 4. Establecer directrices para la implementación de controles de privacidad y seguridad de la información

O 5. Establecer directrices para la medición y mejora del PIMS

1.2.3 Resultados esperados

R1 para O1. Informe de contexto

R2 para O1. Modelo de los procesos dentro del alcance del PIMS

R3 para O1. Política de privacidad y seguridad de la información

R1 para O2. Metodología de gestión de riesgos

R2 para O2. Catálogo de activos de información

R3 para O2. Plan de tratamiento de riesgos

R4 para O2. Declaración de aplicabilidad del PIMS

R1 para O3. Matriz de comunicaciones

R2 para O3. Estándar de gestión documental del PIMS

R1 para O4. Guía de implementación de controles

R1 para O5. Cuadro de control del PIMS

1.3 Herramientas y Métodos

1.3.1 Mapeo de objetivos, resultados y verificación

O1 - Establecer el contexto de la organización y las políticas de seguridad de la información y privacidad			
Resultado	Medio de verificación	Indicador objetivamente verificable	Herramientas
R1 - Informe de contexto	Revisión por especialistas	Completitud del documento	-
R2 - Modelo de los procesos dentro del alcance del SGPDP	Revisión por especialistas	Porcentaje de procesos definidos	- BPMN - Camunda Modeler
R3 - Política de privacidad y seguridad de la información	Revisión por especialistas	Completitud del documento	- ISO 29100 - ISO 27002 - ISO 27701

O2 – Diseñar componentes para la gestión de riesgos para el sistema de gestión de protección de datos personales			
Resultado	Medio de verificación	Indicador objetivamente verificable	Herramientas
R1 - Catálogo de activos de información	Revisión por especialistas	Porcentaje de activos de información catalogados	- ISO 27005 - ISO 29100 - ISO 27701
R2 - Metodología de gestión de riesgos	Revisión por especialistas	Porcentaje de etapas de gestión de riesgo documentadas	- ISO 27005 - ISO 29100 - ISO 27701
R3 - Plan de tratamiento de riesgos	Revisión por especialistas	Porcentaje de riesgos analizados	- ISO 27005 - ISO 29100 - ISO 27701
R4 - Declaración de aplicabilidad del PIMS	Revisión por especialistas	Porcentaje de controles analizados del anexo A de ISO 27001 y sus extensiones en ISO 27701	- ISO 27001 - ISO 27701

O3 - Elaborar componentes de soporte del sistema de gestión de protección de datos personales			
Resultado	Medio de verificación	Indicador objetivamente verificable	Herramientas
R1 - Matriz de comunicaciones	Revisión por especialistas	Porcentaje de comunicaciones documentadas	- ISO 27001 - ISO 27701
R2 – Estándar de gestión documental del PIMS	Revisión por especialistas	Completitud del documento	- ISO 27001 - ISO 27701

O4 - Establecer directrices para la implementación de controles de privacidad y seguridad de la información			
Resultado	Medio de verificación	Indicador objetivamente verificable	Herramientas
R1 – Guía de implementación de controles	Revisión por especialistas y conformidad por parte de la empresa	Porcentaje de controles incluidos del Anexo A de ISO 27001 e ISO 27701	- ISO 27002 - ISO 27701

O5 - Establecer directrices para la medición y mejora del PIMS			
Resultado	Medio de verificación	Indicador objetivamente verificable	Herramientas
R1 – Cuadro de control del PIMS	Revisión por especialistas	Porcentaje de objetivos de privacidad y seguridad de la información evaluados	- ISO 27701 - ISO 29100

1.3.2 Herramientas

ISO/IEC 27001:2013

Brinda los requerimientos para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información.

ISO/IEC 27002:2013

Este estándar consiste en una guía de implementación de los controles que se encuentran en el anexo A del estándar ISO 27001. Si bien las directrices para cada control se encuentran de manera general en este estándar, lo que el proyecto busca es brindar directrices específicas para una determinada organización, por lo cual la guía de implementación a diseñarse será más detallada.

ISO/IEC 27701:2019

Como extensión de los estándares ISO/IEC 27001: 2013 y ISO/IEC 27002:2013, este estándar amplía los requerimientos presentados en ISO/IEC 27001:2013 para un sistema de gestión de seguridad de la información y agrega controles, de modo que este sistema se transforma en un sistema de gestión de protección de datos personales.

ISO 31000: 2018 e ISO/IEC 27005:2018

Estos estándares proveen de principios y procesos para la gestión de riesgos. El segundo de estos estándares, en particular, se enfoca en la gestión de riesgos en seguridad de información. El marco de trabajo establecido será utilizado como base para el objetivo de gestión de riesgos.

Camunda Modeler y BPMN

Se utilizará BPMN (Business Process Model and Notation) para modelar los procesos relevantes al sistema de gestión de protección de datos personales. El software que se utilizará para este propósito es Camunda Modeler.

ISO 29100

Establece un marco de trabajo para la privacidad. Este estándar será considerado para la elaboración de las políticas, así como para la evaluación de los activos de información y los riesgos relacionados a estos.

Capítulo 2. Marco conceptual y marco regulatorio

2.1 Marco Conceptual

El objetivo de esta sección es definir algunos de los términos que se utilizarán a lo largo de este documento.

2.1.1 Datos personales / Información personal de identificación:

Toda información que (a) puede ser usada para vincular dicha información y la persona natural a la que se relaciona (b) es o puede ser directa o indirectamente vinculada a una persona natural. (ISO, 2011)

2.1.2 Titular de los datos personales:

Persona natural a la que la información de identificación se relaciona. (ISO, 2011)

2.1.3 Controlador de los datos personales:

Parte interesada que determina los propósitos y medios para el procesamiento de datos personales aparte de las personas naturales que usan la data para propósitos personales. (ISO, 2011)

2.1.4 Procesador de los datos personales:

Parte interesada que procesa los datos personales en nombre del controlador y según las instrucciones de este. (ISO, 2011)

2.1.5 Confidencialidad:

Propiedad de la información de no estar disponible para individuos, entidades o procesos sin autorización. (ISO, 2018)

2.1.6 Integridad:

Propiedad de proteger la precisión y completitud de la información. (ISO, 2018)

2.1.7 Disponibilidad:

Propiedad de la información de ser accesible y usable ante la demanda de una entidad autorizada. (ISO, 2018)

2.1.8 Sistema de gestión

Un sistema de gestión es la forma en la que una organización administra las partes interrelacionadas del negocio para lograr sus objetivos.

2.2 Marco Regulatorio

2.2.1 Estándares Relacionados

ISO 29100:2011 – Marco de Referencia de Privacidad

Propone un marco de trabajo para la protección de información personal para las organizaciones. Esta norma establece once principios que deben ser implementados en los sistemas de gestión de privacidad, basándose en principios ya empleados por las legislaciones en diversos estados. Los once principios son:

- Consentimiento y elección: Obtener el consentimiento de los titulares de la información personal para la recolección y tratamiento de esta. Proveer de toda información necesaria previa a la obtención del consentimiento.
- Legitimidad de propósito y especificación: Asegurar que el propósito del procesamiento de los datos cumpla con la ley.
- Limitación de colección de datos: Limitar la obtención de datos personales a aquellos que sean estrictamente necesarios para el propósito establecido.
- Minimización de los datos: Minimizar el procesamiento de datos personales. Eliminar todo dato personal una vez que el procesamiento de este haya finalizado.

- Limitación de uso, retención y divulgación: Limitar el uso de los datos personales al propósito establecido antes de la obtención.
- Precisión y calidad: Asegurar que los datos procesados sean precisos completos, actualizados, adecuados y relevantes para el propósito establecido.
- Sinceridad, transparencia y anunciación: Proveer al titular de los datos con información sobre las políticas del procesamiento y propósito de los datos. Mantener al titular informado de todo cambio que se de en el proceso.
- Participación y acceso individual: Proporcionar al titular con la capacidad de acceder y revisar la información que provisionó para el procesamiento. Permitir a los titulares el cuestionamiento de la precisión y completitud de los datos y la corrección de estos.
- Responsabilidad: Adoptar medidas prácticas y concretas para la protección de datos personales. Notificar a todas las partes interesadas en caso de brechas de privacidad y brindar al afectado acceso a compensaciones.
- Seguridad de información: Proteger los datos personales con controles apropiados a nivel operacional, funcional y estratégico para asegurar la confidencialidad, integridad y disponibilidad de los datos.
- Cumplimiento de privacidad: Asegurar y demostrar que el procesamiento cumple con los requerimientos para la protección de los datos personales y salvaguardia de la privacidad.

ISO 27000:2018 – Glosario de términos relacionados a Sistemas de Gestión de Seguridad de Información

Define los términos utilizados por la familia de estándares 27000. Entre estos se encuentran términos relacionados al campo de seguridad de información como confidencialidad, integridad y disponibilidad.

ISO 27001:2013 – Requerimientos para Sistemas de Gestión de Seguridad de Información

Proporciona un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un sistema de gestión de seguridad de la información (SGSI). Recalca la importancia de la gestión de riesgos y establece controles de seguridad de la información, los cuales están divididos en 14 grupos:

1. Políticas de seguridad de la información
2. Organización de la seguridad de la información
3. Seguridad de los recursos humanos
4. Gestión de activos
5. Control de acceso
6. Criptografía
7. Seguridad física y de entorno
8. Seguridad de operaciones
9. Seguridad de comunicaciones
10. Adquisición, desarrollo y mantenimiento de sistemas
11. Relaciones con proveedores
12. Gestión de incidentes de seguridad de información
13. Aspectos de seguridad de información en la gestión de continuidad del negocio
14. Cumplimiento

ISO/IEC 27701:2019

Este documento funciona como una extensión de los estándares ISO/IEC 27001:2013 y 27002:2013. Establece requisitos y controles adicionales necesarios para la implementación y mantenimiento de un sistema de gestión de protección de datos personales. Análogamente a la naturaleza del documento, el sistema de gestión protección de datos personales mencionado funciona como una extensión del sistema de gestión de seguridad de la información. Se proporciona un mapeo entre la estructura de este estándar y los principios establecidos por la norma ISO/IEC 29100:2011.

2.2.2 Ámbito legal

Ley de Protección de Datos Personales y su reglamento

Regulación publicada en el año 2011 que establece obligaciones y restricciones para todas las entidades (privadas o públicas) que administran información personal. Entre estas obligaciones está obtener el consentimiento del titular de esta información para el procesamiento de esta, así como mantenerlo informado sobre el uso de la información. El titular posee además derechos sobre la modificación de sus datos personales y a ser indemnizado en caso de que la privacidad de estos sea vulnerada. Además de esto, se establecen grados para el incumplimiento de esta ley y las sanciones respectivas en forma de multas que pueden alcanzar hasta un valor de 100 UIT en el grado más alto.

Esta ley da origen a la Autoridad Nacional de Protección de Datos Personales adscrita al Ministerio de Justicia. Esta entidad tiene entre sus funciones establecer los requisitos y condiciones para la seguridad de bancos de datos personales.

El reglamento de esta ley incluye directrices específicas para el cumplimiento de los principios rectores de la ley.

Reglamento General de Protección de Datos (RGPD)

Exige a las organizaciones que mantienen y procesan datos privados de ciudadanos de la unión europea respetar la privacidad de estos ciudadanos y proteger su información personal. Establece una política de transparencia para que el cliente de las organizaciones tenga conocimiento sobre la información personal que es retenida por estas y la forma en la que se procesará. Establece también el derecho al olvido, lo cual brinda la capacidad a los titulares de información personal de solicitar la eliminación de esta información de los bancos de datos de toda organización que los procese. Establece siete principios para el tratamiento de datos personales, los cuales son los siguientes:

- Licitud, lealtad y transparencia
- Limitación de la finalidad
- Minimización de datos
- Exactitud
- Limitación del plazo de conservación
- Integridad y confidencialidad
- Responsabilidad proactiva

NTP ISO/IEC 27001:2014

Norma técnica peruana que traduce el estándar ISO 27001:2013. Trata de la implementación de sistemas de gestión de la seguridad de la información por entidades públicas, con la finalidad de disminuir los riesgos que vienen asociados a la gestión de la información. El seguimiento de esta norma es de carácter obligatorio para entidades públicas.

Capítulo 3. Estado del Arte

En esta sección se resumen los estudios que ya existen respecto al tema de sistemas de gestión de la privacidad de datos personales. La revisión sistemática para el estado del arte se basó en el método propuesto por Kitchenham.

Se partió de la pregunta: ¿Qué se está implementando en las organizaciones para gestionar la privacidad de datos personales? Para responder esta pregunta se buscó artículos a sistemas de gestión de la privacidad en la base de datos Scopus. La búsqueda se realizó sobre los títulos, resúmenes y palabras clave de los artículos, y para esto la cadena de búsqueda que se utilizó fue: TITLE-ABS-KEY ("privacy management system" OR (ISO W/2 29100)). Se establecieron los siguientes criterios de inclusión y exclusión:

Tabla 3.1 Criterios de inclusión y exclusión

Criterios de Inclusión	Criterios de Exclusión
Artículos relacionados al tema de sistemas de gestión de la privacidad de datos personales aplicados en organizaciones.	Textos duplicados
Revisiones de literatura sobre implementación de la privacidad	Textos que no abarquen la temática establecida.
Textos publicados entre los años 2010 y 2019	Textos publicados antes del año 2010
Textos escritos en español o inglés.	

La búsqueda devolvió 46 papers como resultado. Luego de comparar las fechas de publicación, títulos, palabras clave y resúmenes de los papers con los criterios de inclusión y exclusión establecidos, se procedió a excluir a aquellos papers que no son pertinentes a la investigación. El resultado final consiste en 6 papers, uno de los cuales es una revisión sistemática y el resto son papers de conferencias.

3.1 Revisión y discusión

3.1.1 Patrones de privacidad

Una de las obligaciones establecidas en la GDPR es la de privacidad y seguridad por diseño. Esto implica que la integración de la protección de los datos en el procesamiento de estos debe darse desde el momento en el que se inicia el proceso (General Data Protection Regulation, 2016). Para esto, existen múltiples patrones de diseño propuestos relacionados a la privacidad.

El termino patrón de diseño fue introducido a mediados de los años 70 para hacer referencia a soluciones reusables a problemas de diseño (Alexander et al., 1977). Si bien es un término que nació en el campo de la arquitectura, este fue usado en muchas áreas, siendo la ingeniería de software una de ellas. De este modo, los patrones de privacidad son soluciones para la ingeniería de software cuyo objetivo es la implementación de la privacidad por diseño.

En la revisión sistemática realizada por Aljohani, Blustein y Hawkey, se identificaron 14 patrones de privacidad, los cuales fueron validados mediante comparaciones con los principios propuestos por la norma ISO 29100 (ver Tabla 3.2). Los patrones enumerados por el estudio fueron:

1. Informed Consent
2. Masked Online Traffic
3. Obtaining Explicit Consent
4. Access Control
5. Minimal Information Asymmetry
6. Privacy Dashboard
7. Instant User Interface

8. Non-Repudiation
9. Data Abstraction
10. Ambient Notice
11. Private Link
12. Outsourcing
13. Notification
14. Limit Disclosure

Tabla 3.2 Mapeo de patrones de privacidad con los once principios establecidos por ISO 29100

Patrones	**Principios de privacidad de ISO 29100**								
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
1	✓	✓	✓	✗	✓	✗	✓	✓	✓
2		✓	✓	✓	✗	✓		✓	✓
3	✓	✓	✓	✗	✗	✓	✓		✓
4		✓	✗	✗	✓	✗	✓	✓	✗
5	✓	✓	✗	✗	✓	✗	✓	✓	✗
6	✗	✓	✗	✗	✗	✗	✓	✓	✗
7	✗	✗	✗	✗	✓	✓	✓	✗	✓
8	✗	✓	✓	✗	✓	✓		✗	✗
9	✗	✗	✓	✗	✓	✓	✓	✓	✗
10	✗	✓	✗	✗		✗	✓	✗	✗
11	✗	✓	✓	✗	✓	✗	✓	✗	✓
12	✓	✓	✓	✗	✓	✗	✓	✓	✗
13	✓	✓	✓	✗	✓	✗	✓	✓	✗
14	✓	✓	✓	✓	✗	✗	✓	✓	✓

Adaptado de (Aljohani, Blustein, & Hawkey, 2018)

En el estudio realizado por Drozd, se propone un catálogo de patrones de privacidad interactivo en línea. El proyecto, dirigido a arquitectos y desarrolladores de software, realiza un mapeo similar al del anterior estudio mencionado, con la diferencia de que el mapeo de los patrones es con las instrucciones de los principios de la norma ISO 29100, mas no con los principios en sí.

Para la navegación, se establece una jerarquía en la que cada principio tiene un conjunto de instrucciones y cada instrucción tiene un conjunto de patrones asociados. El catálogo tiene funciones de búsqueda y generación de reportes.

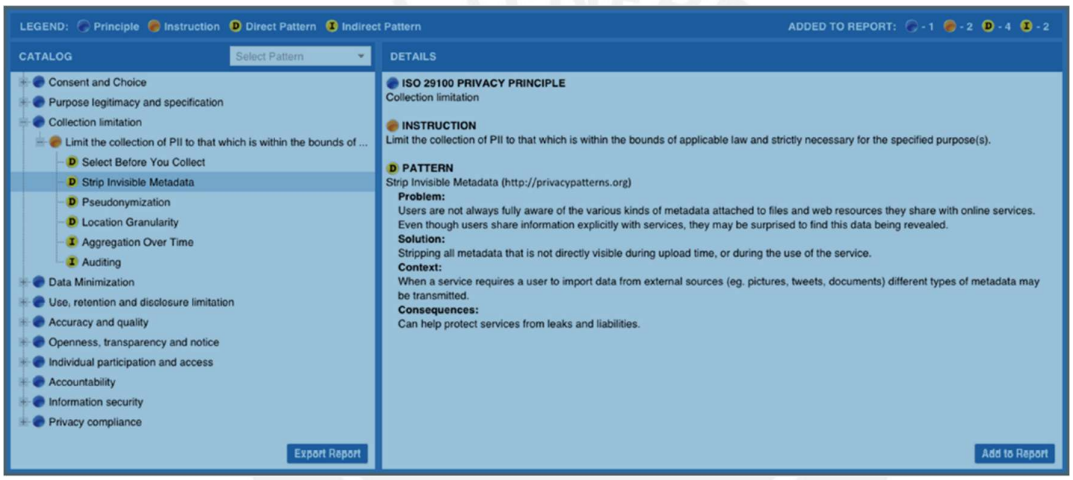


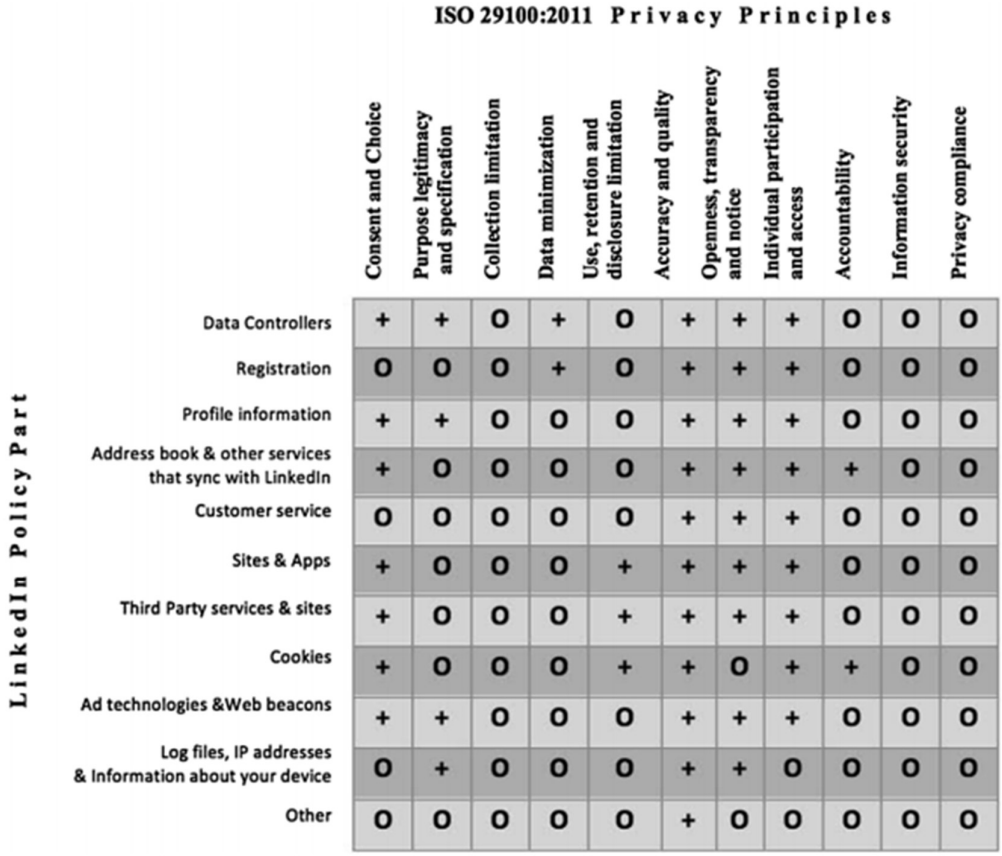
Figura 3.1 Interfaz gráfica del catálogo online de patrones de privacidad. Adaptado de (Drozd, 2016)

Se contempla también la posibilidad de extender el catálogo con la inclusión de tecnologías de mejora de privacidad (PET), de manera que cada patrón pueda tener PETs asociados.

3.1.2 Políticas de privacidad conforme al estándar ISO 29100:2011

Dos estudios fueron analizados respecto a las políticas de privacidad. Ambos estudios, realizados por Michota y Katsikas, tratan específicamente sobre políticas de privacidad en redes sociales, específicamente en Facebook y LinkedIn. Para ambos casos, el objetivo fue el de investigar si es que las políticas de seguridad de las redes sociales en cuestión satisfacían los once principios mencionados en la norma ISO 29100. Para esto, el método que se usó fue

el de realizar mapeos de los principios de privacidad con cada declaración en las partes principales de la política de privacidad.



LinkedIn Policy Part	Consent and Choice	Purpose legitimacy and specification	Collection limitation	Data minimization	Use, retention and disclosure limitation	Accuracy and quality	Openness, transparency and notice	Individual participation and access	Accountability	Information security	Privacy compliance
	ISO 29100:2011 Privacy Principles										
Data Controllers	+	+	O	+	O	+	+	+	O	O	O
Registration	O	O	O	+	O	+	+	+	O	O	O
Profile information	+	+	O	O	O	+	+	+	O	O	O
Address book & other services that sync with LinkedIn	+	O	O	O	O	+	+	+	+	O	O
Customer service	O	O	O	O	O	+	+	+	O	O	O
Sites & Apps	+	O	O	O	+	+	+	+	O	O	O
Third Party services & sites	+	O	O	O	+	+	+	+	O	O	O
Cookies	+	O	O	O	+	+	O	+	+	O	O
Ad technologies &Web beacons	+	+	O	O	O	+	+	+	O	O	O
Log files, IP addresses & Information about your device	O	+	O	O	O	+	+	O	O	O	O
Other	O	O	O	O	O	+	O	O	O	O	O

Figura 3.2 Mapeo para la sección "What information we collect" de la política de privacidad de LinkedIn. Los símbolos de "+" indican que la cobertura del principio fue de mayor grado, mientras que el símbolo de "○" indica que la cobertura fue parcial.

Adaptado de (Michota & Katsikas, 2015)

En ambos estudios se logra observar que la mayoría de las declaraciones en las políticas de privacidad de estas dos plataformas solo cubrían parcialmente los principios establecidos.

3.1.3 Heurísticas de privacidad

En el estudio de Furano, Kushniruk y Barnett, se propone un conjunto de heurísticas orientadas a la privacidad de datos personales (centrándose en el ámbito de historias clínicas). Estas

heurísticas fueron desarrolladas tomando en cuenta los principios del estándar ISO 29100, y son complementarias a las heurísticas de Nielsen.

Tabla 3.3 Heurísticas de privacidad

Heuristic	Description
1. System contains robust biometric authentication measures. (Kotz, 2011)	The system provides the ability for patients and providers to authenticate themselves through a robust, secure mechanism.
2. System contains a role-based authentication mechanism for providers to access the PHR. (Kotz, 2011)	The system access strategy from a provider perspective involves role-based authentication (i.e. smart card) to be granted access to a patients PHI based on a patients privacy preferences.
3. System provides a means for patients to specify consent directives in terms of access, use and disclosure of their PHI. (Kotz, 2011)	The system should be able to provide patients with a consent management option to specify their preferences or directives in terms of privacy management (access, use & disclosure of PHI).
4. The systems consent management protocol contains an "opt-in" and "opt-out" feature. (Gibson & Abrahams, 2010)	The PHR platform must request the patient "opts-in" or "opts-out" in order to utilize or terminate access to the system; this information should be easily retrieved by the healthcare organization to ensure a record of patients consent (month/date/year; time)
5. The system has an easy-to-use audit trail report available to providers and patients. (Kotz, 2011)	The system should have a built in audit trail allowing providers/patients to be aware at any point in time "who" is accessing their PHI. For patients, the report should include: what type of PHI was accessed and by what type of provider. For providers, the same question must be addressed as well as which patients PHI was accessed and by which provider (name).
6. The PHR contains a patient-controlled amendable privacy policy. (Li, 2015)(Samavi, Consens & Cignell, 2014) (Samavi & Topaloglou, 2008)	The system should have the ability to contain: a) vendors privacy policy b) organizational privacy policy and c) a patient-amendable privacy policy to include patient specific privacy preferences based on the organization providing different privacy options to accommodate PHI privacy needs.
7. The system provides an easy-to-use communication tool to contact privacy officer. (Gibson & Abrams, 2010)	The PHR should contain a visible and accessible communication tool to contact a privacy officer or personnel in the event of a suspected privacy breach or inquest. This communication tool should be accessible within each interface in the PHR.
8. The system should ensure data protection through "break-the-glass" functionality. (Samavi & Topaloglou, 2008)	For sensitive PHI, patients may choose to indicate certain information as part of their PHR is indeed sensitive therefore access logic must be built into the PHR to ensure providers attempting to access sensitive information are prompted with "break-the-glass" functionality.
9. The system has the ability to restrict access to data (structured or unstructured) on a field-by-field basis. (Brodie, Karat, Karat & Feng, 2005)	A patient should be able to specify information entered by the patient as being sensitive or confidential on a field-by-field basis. This will 'lock' the information provided by the patient from further processing. The data fields should be able to handle structured and unstructured PHI data (based on the organizations information-handling policies).
10. The PHR system provides the ability for patients to edit historical patient-entered information. (Clark et al., 2014)	The PHR should be able to allow customizable data fields to allow patients to enter either structured or unstructured information based on the healthcare organization data collection strategy; historical information should be editable by the patient if required.
11. The system provides the ability for organizations to classify their data once entered by patients. (Clark et al., 2014)	Data entered by patients and/or providers must be able to be classified into the following categories: public, internal, confidential or restricted. Public ensures anyone with access to the PHR portal can view this information. Internal ensures only members identified as the patients circle of care has access to this information. Confidential ensures the information is only accessible to providers who "break-the-glass". Restricted ensures only providers specified as being able to access the information will be able to access the PHI.

Adaptado de (Furano, Kushniruk, & Barnett, 2017)

3.2 Conclusiones

Se observa que, si bien ha habido estudios respecto a la protección de datos personales en los años recientes, estos han estado más orientados al desarrollo de software que a los sistemas de gestión. Si bien algunos de los textos rechazados en esta revisión incluían el término “sistema

de gestión de privacidad", estos hacían referencia a sistemas de software como parte de otros sistemas más complejos (por ejemplo "sistema de gestión de privacidad para dispositivos Android"), mas no a lo que se entiende como sistema de gestión según ISO.

Algo que se recalca de los trabajos presentados es que la metodología suele consistir en un mapeo de los principios de privacidad establecidos en la norma ISO 29100 y los objetos a analizar. Este método será utilizado también en el desarrollo de este proyecto, pues de esta forma se podrá verificar de manera puntual que las políticas de privacidad cumplan con todos los principios mencionados en la norma ISO 29100.

Capítulo 4. Contexto, alcance y políticas del sistema de gestión de protección de datos personales

En este capítulo se presentan los tres resultados correspondientes al primer objetivo del proyecto.

4.1 Contexto y alcance

La base de la elaboración de este sistema de gestión es identificar el contexto de la organización para la cual se está proponiendo. En este caso, dicha organización es una institución dentro de una universidad privada en el Perú, que ofrece servicios de evaluación para estudiantes de secundaria, personal de diferentes organizaciones y postulantes al proceso de admisión de la universidad.

Para la elaboración de este informe se toma en cuenta la identificación de partes interesadas, tanto externas como internas, para el sistema de gestión de protección de datos personales propuesto. Este informe se encuentra en el Anexo B.

Se determinó que el alcance del sistema de gestión de protección de datos personales será llamado “proceso de evaluación”. Este proceso abarca todas las actividades que se dan desde el momento en el que se firma el contrato del servicio con el cliente, hasta la emisión de reportes sobre los resultados de las evaluaciones. Por propósitos de orden, este proceso principal se divide en cinco subprocesos los cuales son:

- Proceso de inscripción
- Proceso de elaboración de ítems
- Proceso de diagramación de instrumentos de evaluación
- Proceso de aplicación de la prueba

- Proceso de calificación
- Proceso de elaboración de reportes

Todos estos procesos fueron modelados como uno solo utilizando BPMN. Esto puede apreciarse en el Anexo C.

Como requisito del estándar ISO 27701, se determinó el rol de la institución en estudio en cuanto a la gestión de datos personales. Se pudo observar que esta recopila datos personales en partes del proceso del alcance, lo cual significa que actúa como procesador de datos personales. También se identifica a la alta dirección de la institución en estudio como el controlador de los datos personales. La identificación de estos roles fue necesaria para la elaboración de la declaración de aplicabilidad del sistema de gestión.

4.2 Políticas del sistema de gestión

Para dar cumplimiento al requisito correspondiente a la cláusula 5.2 de ISO 27001 (y las consideraciones de ISO 27701 adicionales para esa cláusula), se elaboró un documento de políticas para el sistema de gestión de protección de datos personales (ver Anexo D). En este documento, se indicaron los objetivos de privacidad y seguridad de la información, los roles que existirán para la operación del sistema de gestión y los lineamientos generales para cada uno de los procesos de la gestión de privacidad y seguridad de la información.

4.3 Conclusiones

Durante las entrevistas con representantes de la institución en estudio, con el fin de levantar información acerca de la organización, se observó que existían controles de privacidad y seguridad de la información ya implementados como esfuerzos aislados (protocolos de seguridad, seguimiento de la política de privacidad de la universidad privada a la que pertenece la institución en estudio, controles de seguridad física para las bóvedas). A pesar de esto, no

era posible decir que existía una gestión de privacidad y seguridad de la información, debido a que estos controles consistían en esfuerzos aislados.

Lo que se buscó es que, por medio de políticas y directrices, estos controles y todo otro control que pueda ser implementado en el futuro sean más fáciles de gestionar al estar integrados en un solo sistema.

Capítulo 5. Gestión de riesgos

La gestión de riesgos del sistema de gestión de protección de datos personales para la institución en estudio se llevó a cabo según el procedimiento propuesto en ISO 27005 y tomando en consideración el marco de ISO 29100.

5.1 Metodología de gestión de riesgos

Se detalla la metodología de gestión de riesgos de privacidad en el Anexo E. En esta se detalla cómo se llevará a cabo la gestión de riesgos en cuatro pasos principales, los cuales son la identificación, el análisis, la evaluación y el tratamiento de los riesgos.

Dado que ISO 27005 consiste en la gestión de riesgos para seguridad de la información, pero sin profundizar en temas de privacidad, se propone un análisis adicional en la metodología de gestión de riesgos para que en dicha gestión se tome en cuenta la privacidad.

5.2 Iteración inicial de la gestión de riesgos

Para la elaboración del catálogo de activos de información de la institución en estudio (Anexo F), se debe indicar quién es titular de los datos personales asociados a cada activo. Del mismo modo, se indicará si estos datos (si es que el activo los contiene) son considerados datos sensibles según la ley de protección de datos personales. La razón de esto es que dicha ley exige priorizar aquellos datos personales que hayan sido determinados como sensibles. Esta información extra sobre los activos, será considerada para la fase de análisis, ya que parte de esta consiste en la valoración de los activos de información. Si bien es usual que esta valoración se de en términos de la confidencialidad, integridad y disponibilidad esperada de cada activo, para este caso se toma en cuenta también la existencia de datos personales y sensibles.

La fase de identificación de riesgos consiste no solo en identificar a los activos de información, sino también en la identificación de vulnerabilidades, amenazas, escenarios de riesgos y sus consecuencias respectivas.

Para la identificación de amenazas se tomó en cuenta el listado propuesto en ISO 27005. Si bien estas amenazas son muy genéricas y no necesariamente se aplican al caso de la institución en estudio, el propósito de este listado es poder relacionarlo con el listado de vulnerabilidades (el cual debe ser más específico, pues hace referencia a las vulnerabilidades de cada activo) para así poder tener un listado de escenarios específicos a la institución en estudio. En el Anexo G se presentan los catálogos de amenazas y vulnerabilidades que se desarrollaron para este sistema.

La identificación de escenarios se lleva a cabo describiendo como una determinada amenaza puede explotar una determinada vulnerabilidad. En base a esto se identifica también la consecuencia de cada escenario, y el activo de información afectado.

La fase de análisis consiste en llevar a cabo la valoración de los activos de información, como ya se mencionó anteriormente, y de estimar la probabilidad de ocurrencia de los escenarios, así como también el nivel de impacto de las consecuencias para asignar un valor a cada riesgo en base a estos dos factores.

La fase de evaluación de los riesgos consiste en priorizar cada uno de estos riesgos una vez que poseen un valor asignado. Esta priorización se hace en base a una matriz 5x5 de evaluación de riesgos.

Una vez que se realizaron todos estos pasos, se procede al tratamiento de los riesgos, el cual consiste en proponer si los escenarios serán modificados, evitados, compartidos o retenidos. Se lleva a cabo un segundo análisis de escenarios, pero asumiendo que se llevó a cabo la acción de tratamiento propuesta, de modo que se pueda estimar un nivel de riesgo residual. Se debe

también elaborar un listado de controles para todos aquellos escenarios en los cuales se escogió la opción de modificar.

Si bien este proyecto es de diseño mas no de implementación, fue necesario llevar a cabo una iteración de la gestión de riesgos para obtener el plan de tratamiento de riesgos y la declaración de aplicabilidad para el sistema de gestión de protección de datos personales de la institución en estudio. El resultado de llevar a cabo el procedimiento detallado es el listado de escenarios de riesgos y acciones de tratamiento en el Anexo H y los controles propuestos en el Anexo I.

Para llevar a cabo la gestión de riesgos, se contó con el apoyo del personal de la institución en estudio para las fases de valoración de activos y análisis de escenarios de riesgos, pues la metodología establece que esto ha de ser llevado a cabo por los propietarios de cada activo.

5.3 Declaración de aplicabilidad

Una vez llevada a cabo la gestión de riesgos, se procedió a elaborar la declaración de aplicabilidad (Anexo J). En esta se justifica no solo los controles de seguridad de la información del anexo A de ISO 27001, sino también los controles para controladores de datos personales (Anexo A de ISO 27701) y los controles para procesadores de datos personales (Anexo B de ISO 27001), pues durante el análisis del contexto del sistema de gestión de protección de datos personales, se identificó que la institución en estudio actúa como controladora de datos personales tanto como procesadora de estos.

5.4 Conclusiones

Durante la elaboración de los entregables correspondientes a este capítulo, se hizo cambios menores respecto al estándar ISO/IEC 27005:2018 con el fin de que la gestión de riesgos de seguridad de la información abarque también a los posibles riesgos de protección de datos personales.

Se pudo observar que no basta con simplemente tomar a ISO 27005 como una metodología de gestión de riesgos y aplicarla tal cual, a la organización, sino que esta debe ser usada como la base para una metodología que se adapte al contexto y los requisitos de la organización.

Capítulo 6. Componentes de soporte

Los componentes de soporte que se desarrollaron como parte del diseño del sistema de gestión de protección de datos personales se elaboraron tomando en cuenta los requisitos 7.4 (comunicación) y 7.5 (Información documentada) de ISO 27001. De ese modo, se cuentan con los siguientes entregables:

6.1 Matriz de comunicaciones (Anexo K)

Documento en el cual se detallan los aspectos del sistema de gestión de protección de datos personales a comunicar. Para cada aspecto, se indica el emisor, receptor, cuando se comunicará y cómo se comunicará.

6.2 Estándar de gestión documental (Anexo L)

En este documento se indican los lineamientos para la gestión de la información documentada que se puede generar durante la operación del sistema de gestión de protección de datos personales. Se indican las consideraciones que han de ser tomadas a lo largo del ciclo de vida de los documentos (desde que son elaborados hasta que son eliminados).

6.3 Conclusiones

Tomando en consideración lo desarrollado en la matriz de comunicaciones y las directrices para la gestión de información documentada, se puede lograr una mayor eficiencia en los procesos de comunicación interna de la institución en estudio. Muchos de los documentos relacionados a políticas (políticas del sistema de gestión y políticas específicas) hacen referencia a las actividades de comunicación dentro de la institución en estudio, y esto se puede complementar con la matriz de comunicaciones. Del mismo modo, como parte de la implementación del sistema de gestión, se puede realizar una revisión de los documentos

presentados en este proyecto para asegurar el cumplimiento con los estándares de gestión documental.

Capítulo 7. Directrices para la implementación del sistema de gestión

Si bien, como ya se mencionó en anteriores capítulos, este proyecto abarca el diseño mas no implementación de un sistema de gestión de protección de datos personales, se elaboraron documentos que pueden ser utilizados como guía una vez que la organización opte por implementar el sistema de gestión.

Las directrices que se brindan son específicamente sobre la implementación de los controles de la declaración de aplicabilidad y sobre los procesos de monitoreo y medición.

7.1 Directrices para la implementación de controles (Anexo M)

En este documento se indican las consideraciones que han de tomarse al momento de implementar los controles que han de aplicarse a la institución en estudio según la declaración de aplicabilidad. Se observó que gran parte de los controles a implementar correspondían a la implementación de políticas específicas (sobre todo para los controles de privacidad de ISO 27701). Adicionalmente, se proponen controles para la seguridad física en las bóvedas de la institución en estudio y se detalla a grandes rasgos un procedimiento para la gestión de incidentes. Una versión inicial de las políticas específicas de protección de datos personales y seguridad de la información se encuentra en el Anexo N.

7.2 Cuadro de control del sistema de gestión (Anexo O)

Los lineamientos para el monitoreo y medición ya fueron establecidos en un entregable anterior (Anexo D – Políticas del sistema de gestión). El propósito de este documento es brindar indicadores de desempeño y efectividad para los objetivos del sistema de gestión, los procesos de este y la implementación de controles.

7.3 Conclusiones

Si bien la gestión de incidentes no fue una parte mayor del proyecto (como lo fue la gestión de riesgos), se concluye que esta puede ser una base importante para la operación del sistema de gestión de protección de datos personales. Se podría considerar la elaboración de un documento de gestión de incidentes (análogo al documento de metodología de gestión de riesgos) para un diseño más eficaz del sistema de gestión de protección de datos personales.

Capítulo 8. Conclusiones y trabajos futuros

8.1 Conclusiones

La relevancia de este proyecto se hace más evidente al tomar en cuenta que se complementa un estándar reconocido de seguridad de la información (ISO/IEC 27001:2013) con un estándar reciente al desarrollo del proyecto (ISO/IEC 27701:2019).

Si bien ya existían medidas implementadas de seguridad de la información y protección de datos personales en la institución en estudio, se identificó que no existía una gestión de estos controles, por lo cual se determinó importante la necesidad de diseñar e implementar un sistema de gestión de protección de datos personales. Mediante las directrices brindadas por este sistema de gestión, se puede facilitar el mantenimiento de los controles que ya existían como esfuerzos aislados, así como también la implementación de nuevos controles que se determinen como necesarios.

Previo al proceso de gestión de riesgos, se observó que el estándar ISO 27005 es de gran relevancia para este, debido a que brinda un marco para la gestión de riesgos de seguridad de la información. Es importante mencionar que este marco tuvo que ser adaptado para ser aplicado al proceso del alcance del sistema de gestión y para que la gestión de riesgos abarque la protección de datos personales.

Debido a que este proyecto es de diseño, mas no de implementación, no se desarrollaron a gran detalle los puntos como la gestión de incidentes de protección de datos personales, la gestión de accesos, o la seguridad física. Sin embargo, se elaboró un entregable que puede funcionar como un marco para la implementación de los diferentes componentes del sistema de gestión.

En el Anexo P, se puede observar las validaciones que se realizaron para los entregables de este proyecto.

8.2 Trabajos futuros

Se propone como trabajo futuro a la elaboración de documentación para llevar a cabo la gestión de incidentes de privacidad y seguridad de la información en la institución en estudio. En esta documentación se debe detallar de manera más específica cada fase del ciclo de vida de los incidentes de privacidad y seguridad de la información, y se brindarían instrucciones para la identificación y análisis de estos, con el fin de cumplir con el acápite 16 del Anexo A de ISO/IEC 27001:2013, el cual es extendido por ISO/IEC 27701:2019 para tomar en cuenta la gestión de incidentes relacionados a la protección de datos personales.

Adicionalmente, se plantea la implementación de los controles de protección de datos personales, de modo que se tenga mecanismos establecidos para la recopilación de datos personales, así como para el procesamiento de estos, la minimización de dicho procesamiento, y la gestión de solicitudes por parte de los titulares de datos personales. Para dicho trabajo futuro, podría utilizarse como marco a ISO 29100, y a la guía de integración de COBIT 5 con los principios de privacidad de ISACA.

Por último, se propone el desarrollo e implementación de un software que permita automatizar con mayor facilidad los procesos de gestión de protección de datos personales. Del mismo modo, se puede diseñar un software que haga uso de los patrones de privacidad mencionados en el capítulo Estado del Arte de este documento, para el análisis de los controles y requerimientos de protección de datos personales. Esto se realizaría con el fin de lograr una gestión eficiente de la seguridad de la información y protección de datos personales.

Referencias

Acosta, D. (2017). ISO/IEC 29100:2011 Una introduccion al marco de trabajo de privacidad para la proteccion de informacion de identificacion personal (PII).

Alexander, C., Ishikawa, S., Silverstein, M., Jacobson, M., Fiksdahl-King, I., & Angel, S. (1977). A Pattern Language: Towns, Buildings, Construction. New York: Oxford University Press.

Aprueban 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. , (2016).

ANPD sanciona a entidad bancaria con S/ 166 mil (40 UITs) por no resguardar la confidencialidad de los datos personales de sus clientes. (2020, setiembre 17). Recuperado el 3 de enero de 2022, de https://www.gob.pe/institucion/minjus/noticias/303011-anpd-sanciona-a-entidad-bancaria-con-s-166-mil-40-uits-por-no-resguardar-la-confidencialidad-de-los-datos-personales-de-sus-clientes

Resolución Directoral N° 2077 -2020-JUS/DGTAIPD-DPDP. 01 de diciembre de 2020. Autoridad nacional de protección de datos.

Cadwalladr, C., & Graham-Harrison, E. (2018, marzo 17). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian. Recuperado de https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Drozd, O. (2016). Privacy Pattern Catalogue: A Tool for Integrating Privacy Principles of ISO/IEC 29100 into the Software Development Process. En D. Aspinall, J. Camenisch, M. Hansen, S. Fischer-Hübner, & C. Raab (Eds.), Privacy and Identity Management. Time for a Revolution? 10th IFIP WG 9.2, 9.5, 9.6/11.7, 11.4, 11.6/SIG 9.2.2 International Summer School, Edinburgh, UK, August 16-21, 2015, Revised Selected Papers (pp. 129–140). https://doi.org/10.1007/978-3-319-41763-9_9

Guerrero, C. (2019, septiembre 24). Dirección de Protección de Datos Personales multa a ONPE por filtrar datos personales de votantes. Recuperado el 18 de noviembre de 2019, de Hiperderecho website: https://hiperderecho.org/2019/09/direccion-de-proteccion-de-datos-personales-multa-a-onpe-por-filtrar-datos-personales-de-votantes/

ISO/IEC 2382:2015(en), Information technology—Vocabulary. (2015, mayo). Recuperado el 6 de septiembre de 2019, de https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v1:en

ISO/IEC 27000: Information technology—Security techniques—Information security management systems—Overview and vocabulary. , Pub. L. No. ISO/IEC 27000 (2012).

ISO/IEC 27701: Information Technology—Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management—Requirements and guidelines. , Pub. L. No. ISO/IEC 27701 (2019).

ISO/IEC 29100: Information Technology—Security Techniques—Privacy Framework. , Pub. L. No. ISO/IEC 29100 (2011).

Ley de Delitos Informaticos. , Ley 30096 § (2013).

Ley de Protección de Datos Personales. , Ley 29733 § (2011).

Management system standards. (s/f). Recuperado el 25 de septiembre de 2019, de ISO website: http://www.iso.org/cms/render/live/en/sites/isoorg/home/standards/popular-standards/management-system-standards.html

Michota, A., & Katsikas, S. (2015). Compliance of the LinkedIn privacy policy with the principles of the ISO 29100:2011 standard. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 9051, 72–83. https://doi.org/10.1007/978-3-319-20370-6_6

Pfeiffer, R. (2011, febrero 4). Improvement in Quality of Life with Information Technology. Recuperado el 27 de septiembre de 2019, de The Business Thinker website: https://businessthinker.com/improvement-in-quality-of-life-with-information-technology/

REGULATION (EU) 2016/ 679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL - of 27 April 2016—On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/ 46/ EC (General Data Protection Regulation). (2016). Official Journal of the European Union, 88.

Zelada, S (s/f). COVID-19, un acelerador de la transformación digital. Recuperado el 2 de octubre de 2021, de Deloitte website: https://www2.deloitte.com/pe/es/pages/technology/articles/COVID19-un-acelerador-de-la-transformacion-digital.html

Anexos

Anexo A: Plan de Proyecto

- **Justificación**

Como se mencionó anteriormente, una de las razones por las cuales es conveniente para una organización implementar un sistema de gestión es que este permite el uso de recursos de manera más eficiente y la entrega mejores productos y servicios, todo esto con el objetivo de aumentar el valor de la organización y orientarla al logro de sus objetivos.

Además, es imperativo para las organizaciones peruanas (ya sean privadas o estatales) cumplir con el marco regulatorio establecido por el estado. La ley más relevante al tema de privacidad es la Ley de Protección de Datos Personales (Ley N° 29733). Parte de la función del sistema de gestión propuesto en este proyecto es asegurar el cumplimiento de la Ley N° 29733 y otras relacionadas al tema.

En el caso de la institución en estudio, existen controles de privacidad y seguridad con el fin de proteger los activos de información del negocio y dar cumplimiento al marco legal. Sin embargo, estos existen como esfuerzos aislados, lo cual puede ocasionar una gestión ineficiente. Uno de los propósitos del sistema de gestión es el de integrar estos controles existentes, así como todos los controles futuros, en una sola solución más simplificada y coordinada.

- **Viabilidad**

El proyecto es viable para la organización, dado que cuenta con los recursos suficientes para la implementación de todos los controles. Además, se estima una duración de cuatro

meses para el proyecto, lo cual es generalmente aceptado para el diseño de un sistema de gestión.

- **Alcance**

El alcance de este proyecto se centra en el diseño del sistema de gestión propuesto y no se detallará la implementación y mantenimiento de este (aunque se brindarán directrices para estos procesos). Se busca desarrollar por lo menos una iteración del ciclo de mejora continua en el que se basan los sistemas de gestión.

- **Limitaciones**

Una posible limitación es el hecho de que el proyecto consista únicamente en el diseño del sistema de gestión de protección de datos personales, mas no en la implementación de este. Esto significa que no se llevaran a cabo los pasos propios de la implementación tales como la auditoría interna del sistema, por ejemplo. Es por eso que para las etapas de evaluación y mejora solo se brindaran directrices.

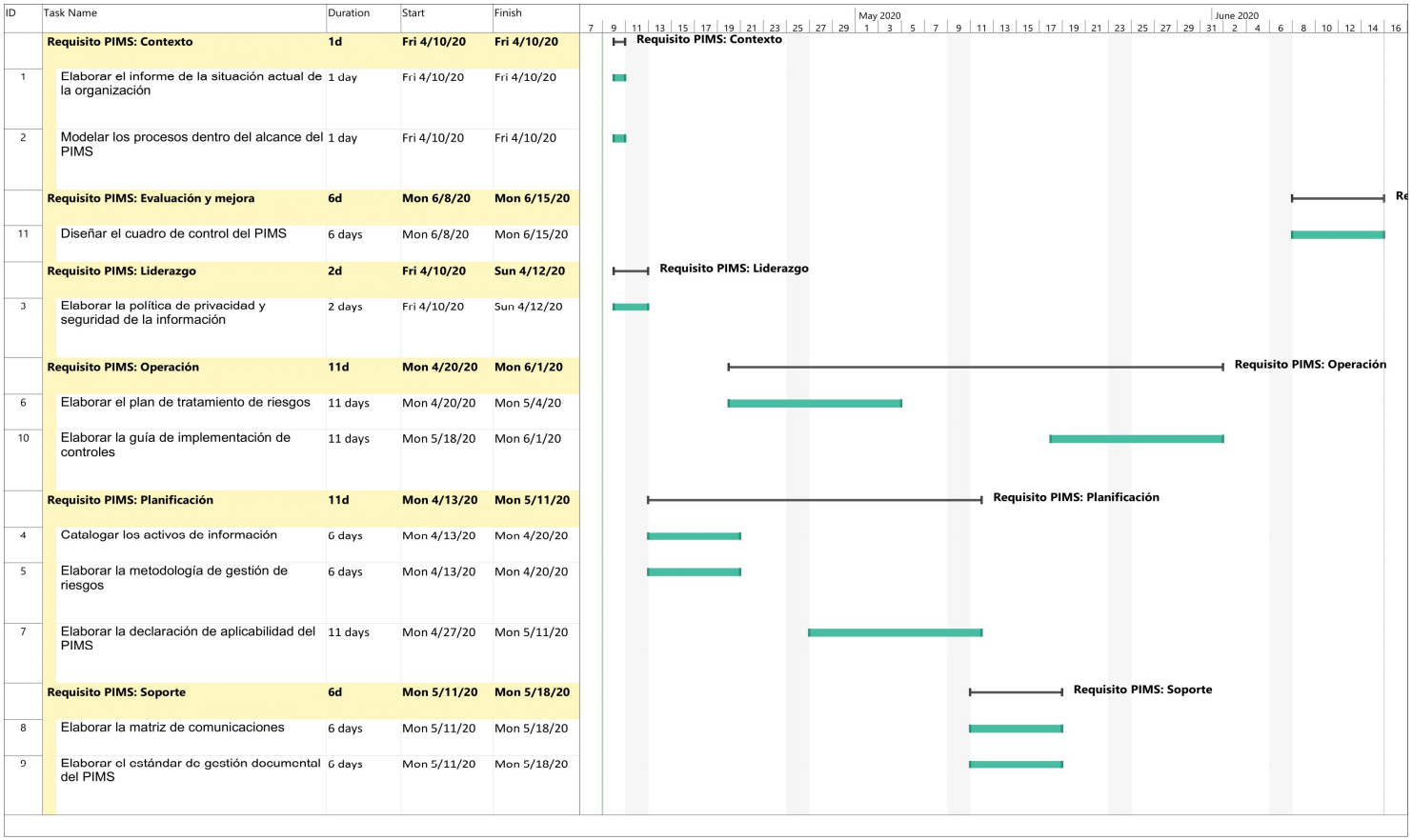
- **Identificación de los riesgos del proyecto**

La tabla 1.2 presenta los riesgos que pueden afectar al proyecto, así como el posible impacto de estos y las medidas que se tomaran para mitigarlos.

Riesgo	Impacto (del 1 al 5)	Medidas de mitigación
No presentar los entregables del proyecto dentro del plazo establecido	5	Elaborar un plan de gestión de tiempo y seguirlo de manera rigurosa
No disponibilidad de información de las organizaciones	4	Obtener acuerdos con las organizaciones para adquirir acceso a la información relevante para el proyecto
Inconsistencia entre lo presentado y los resultados propuestos	4	Mantener la comunicación y frecuentes reuniones entre el tesista y el asesor para asegurar el buen encaminamiento del proyecto
Actualización de estándares utilizados	3	Tener en cuenta el tiempo de publicación de futuras actualizaciones para gestionar su adquisición de forma anticipada
Incapacitación del tesista o asesor	5	Comunicar al comité de tesis con el fin de gestionar una nueva planificación de los entregables
No disponibilidad de material bibliográfico	3	Gestionar con la biblioteca de la universidad la adquisición del material bibliográfico necesario que no se encuentre a disposición del tesista o del asesor

Ocurrencia de una pandemia	3	Mantener las reuniones mediante plataformas de videoconferencias

- **Cronograma del proyecto**



- **Recursos y costos**

Ítem	Descripción	Unidad	Cantidad	Valor unitario (S/.)	Monto total (S/.)	Monto acumulado (S/.)
1	ISO/IEC 27001:2013	Documento PDF	1	399.78	399.78	399.78
2	ISO/IEC 27002:2013	Documento PDF	1	603.13	603.13	1,002.91
3	ISO/IEC 27005:2018	Documento PDF	1	603.13	603.13	1,606.04
4	ISO/IEC 27701:2019	Documento PDF	1	603.13	603.13	2,209.17
5	ISO/IEC 29100:2011	Documento PDF	1	0.00	0.00	2,209.17
6	ISO/IEC 31000:2018	Documento PDF	1	298.14	298.14	2,507.31

Anexo B: Informe de contexto

- **Visión general**

La institución en estudio se encarga de diseñar y desarrollar procesos de evaluación para medir y certificar competencias vinculadas a perfiles específicos.

La estructura organizacional de la institución puede apreciarse en el siguiente organigrama:

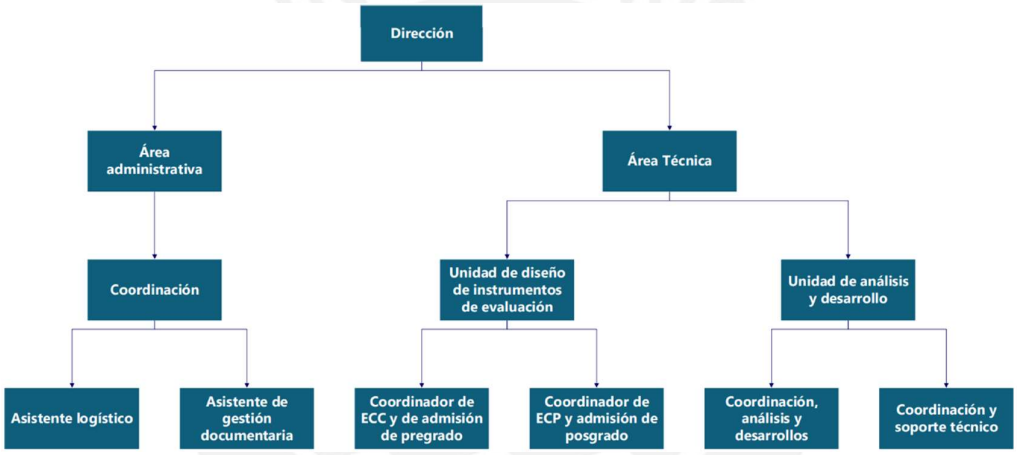


Ilustración 1 Organigrama de la institución en estudio (Versión 2018)

Actualmente, la institución en estudio ofrece los siguientes servicios:

Evaluación de competencias en colegios (ECC): Dirigido a instituciones de educación básica regular que requieren información confiable sobre el desempeño académico de sus estudiantes en competencias fundamentales.

Evaluación de competencias profesionales (ECP): Dirigido a instituciones que requieren evaluaciones para la selección o promoción de profesionales.

Evaluación de competencias para la admisión (ECA): Dirigido a la universidad a la que pertenece la institución en estudio. Consiste en la elaboración y desarrollo de los exámenes de admisión.

Capacitaciones y asesorías: Talleres presenciales y semipresenciales sobre temas relacionados a medición y evaluación.

- **Contexto externo**

Marco legal: La organización se encuentra sujeta a cumplir con las leyes en el Perú relacionadas a la protección de datos y seguridad de la información.

  - Ley de protección de datos personales (Ley 29733)
  - Ley de delitos informáticos (Ley 30096)

Clientes importantes

  - Superintendencia de banca y seguros
  - Junta nacional de justicia
  - Policía nacional del Perú
  - Presidencia del consejo de ministros
  - Tribunal Fiscal

- **Partes interesadas y requisitos**

Clientes de la organización: Instituciones educativas y organizaciones que requieren evaluaciones de personal. Toman los papeles de titular de datos personales y de controlador de datos personales.

  - Disponibilidad del servicio
  - Protección de datos personales

- Cumplimiento con los estándares de privacidad y seguridad de la información
- Rápida respuesta ante incidentes

Alta dirección: Área encargada del gobierno de la organización. Incluye al vicerrectorado de la universidad privada a la que pertenece la institución en estudio.

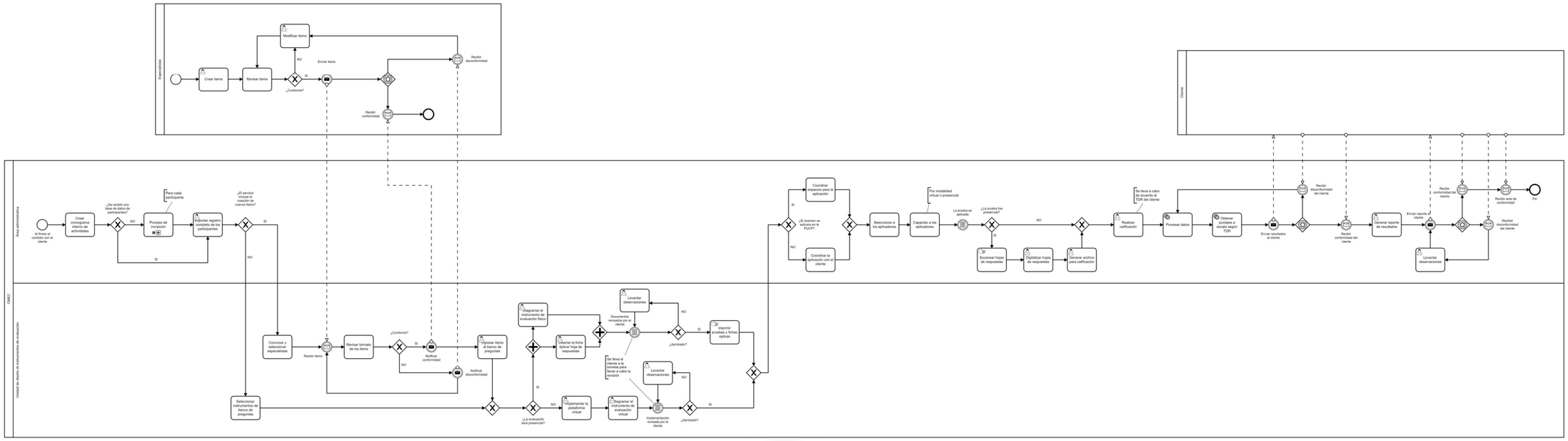
- Cumplimiento con el marco legal
- Confidencialidad, integridad y disponibilidad de los activos de información de la organización

Participantes de las evaluaciones: Personas naturales a ser evaluadas como parte del servicio ofrecido por la institución en estudio. Son titulares de datos personales.

- Protección de datos personales
- Comité consultivo
- Cumplimiento de indicadores clave
- Garantía de la seguridad de la información en los procesos del negocio

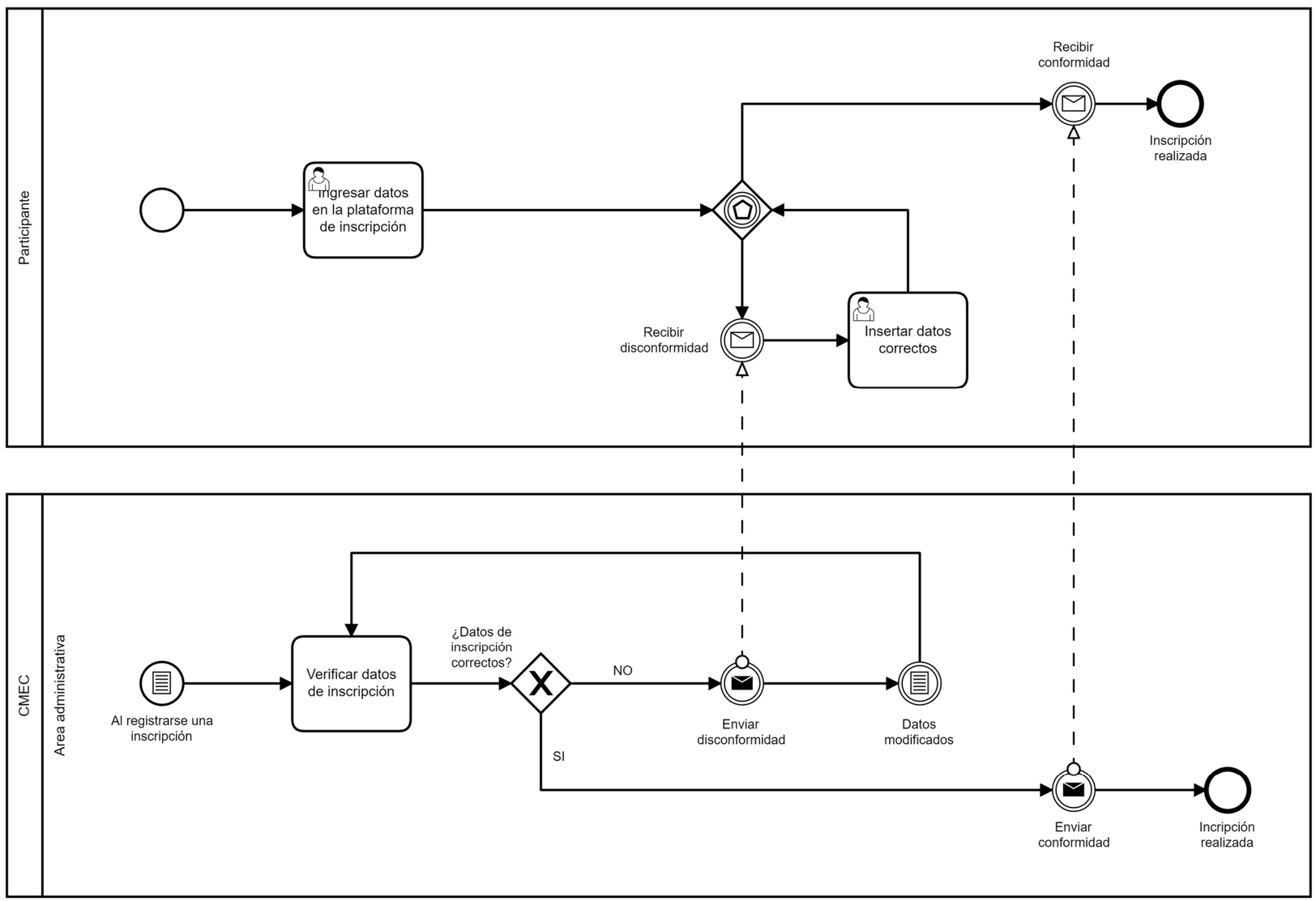
Anexo C: Procesos del alcance del sistema de gestión de protección de datos personales

- **Proceso de evaluación de la institución en estudio**



**Debido a la situación actual, ocasionada por la pandemia de COVID-19, en la que muchas organizaciones emplean la modalidad de teletrabajo, se considera que actualmente solo se ejecuta la parte del proceso correspondiente a las pruebas virtuales. Sin embargo, el alcance del sistema de gestión cubre tanto la modalidad virtual como presencial.*

- **Sub-proceso de inscripción**



Anexo D: Políticas de privacidad y seguridad de la información

- **Disposiciones generales**
    - Los objetivos del sistema de gestión de protección de datos personales se encuentran en todo momento alineados a la visión, misión y objetivos estratégicos de la institución en estudio.
    - Se debe designar a un gestor del sistema de gestión de protección de datos personales, quien es la persona encargada de la planificación y organización de todas las actividades que forman parte de la operación, mantenimiento y mejora del sistema de gestión de protección de datos personales.
    - Todo lineamiento descrito en este documento ha de ser revisado por el comité de privacidad y seguridad de la información cada semestre o cuando se den cambios importantes en la organización.
- **Objetivos de privacidad y seguridad de la información**

Tomando en cuenta los objetivos estratégicos de la organización y la necesidad de alinear los objetivos de privacidad y seguridad de la información a estos, se establecen los siguientes objetivos:

- Asegurar el cumplimiento con el marco legal para privacidad y seguridad de la información
- Garantizar la disponibilidad del proceso de evaluación en todo momento
- Garantizar la confidencialidad e integridad del contenido de instrumentos de evaluación
- Garantizar la confidencialidad e integridad de los datos personales de los participantes de las evaluaciones

El gestor del sistema de gestión de protección de datos personales será el responsable de llevar a cabo la medición del cumplimiento de estos objetivos, haciendo uso del cuadro de control del sistema de gestión de protección de datos personales.

- **Funciones y responsabilidades dentro del sistema de gestión de protección de datos personales**

Alta dirección:

- Revisar y aprobar las políticas de privacidad y seguridad de la información
- Proporcionar los recursos necesarios para operar y mantener el sistema de gestión de protección de datos personales
- Propiciar la gobernabilidad del sistema de gestión de protección de datos personales pidiendo la rendición de cuentas a través del proceso de revisión por la alta dirección
- Solucionar conflictos de interés de las operaciones del sistema de gestión
- Revisar periódicamente el desempeño del sistema de gestión de protección de datos personales

Comité de privacidad y seguridad de la información:

- Plantear y presentar las estrategias para la operación del sistema de gestión de protección de datos personales
- Difundir la política de privacidad y seguridad de la información, así como los objetivos de privacidad.
- Revisar periódicamente la eficacia del sistema de gestión de protección de datos personales
- Dar seguimiento a las auditorías del sistema de gestión de protección de datos personales y a los resultados de estas (no conformidades y acciones de mejora)

- Realizar la revisión preliminar de información a ser presentada en las actividades de revisión por la alta dirección
- Revisar la información documentada del sistema de gestión de protección de datos personales antes de la aprobación, formalización y comunicación a ser realizada la alta dirección
- Dar seguimiento a los resultados de la gestión de riesgos de privacidad y seguridad de la información
- Asegurar los recursos necesarios para contribuir con las mejoras del sistema de gestión de protección de datos personales

Gestor del sistema de gestión de protección de datos personales:

- Mantener a la alta dirección y al comité de privacidad y seguridad de la información informados en cuanto al rendimiento de los procesos del sistema de gestión de protección de datos personales
- Proponer las directivas de alto nivel y específicas para la gestión de protección de datos personales y seguridad de la información
- Convocar y participar en las revisiones del sistema de gestión de protección de datos personales
- Asegurar la implementación, mantenimiento y gestión de los procesos del sistema de gestión de protección de datos personales
- Coordinar la ejecución de iniciativas, proyectos y actividades especializadas en privacidad y seguridad de la información
- Verificar el cumplimiento de las directivas de privacidad y seguridad de la información
- Preparar la información para la revisión del sistema de gestión de protección de datos personales

- Planificar la ejecución de auditorías internas
- Planificar las actividades de capacitación y concientización en privacidad y seguridad de la información
- Llevar a cabo el seguimiento a las acciones de mejora identificadas durante la revisión por la alta dirección
- Organizar sesiones de capacitación con el fin de fomentar la cultura organizacional de privacidad y seguridad de la información

Personal de la institución:

- Cumplir y hacer cumplir al personal a su cargo, a los proveedores de servicios y a los terceros con quienes coordine, las directivas, objetivos, lineamientos y cualquier información documentada vigente que forme parte del sistema de gestión de protección de datos personales
- Reportar todo incidente de privacidad o seguridad de la información que sea identificado
- Asumir y fomentar la cultura organizacional de privacidad y seguridad de la información
- Mantener el compromiso permanente de participar en las actividades de capacitación y sensibilización a las que sea convocado
- Utilizar los activos de acuerdo con las políticas del buen uso de activos de información

- **Lineamientos para los procesos del sistema de gestión de protección de datos personales**

Gestión de riesgos de privacidad y seguridad de la información:

El marco metodológico para la gestión de riesgos de privacidad y seguridad de la información se aprecia en el documento de metodología de gestión de riesgos, el cual abarca la identificación, análisis, evaluación y tratamiento de los riesgos de privacidad y seguridad de la información.

Para llevar este proceso a cabo, se establece un comité de gestión de riesgos a cargo del gestor del sistema de gestión de protección de datos personales. Este comité está formado por los siguientes integrantes:

- Un representante de la dirección
- El gestor del sistema de gestión de protección de datos personales
- Un representante de las áreas de coordinación
- Un representante de los responsables de la bóveda
- Un representante del soporte administrativo
- Todo aquel personal que haya sido identificado como propietario de algún activo de información

Monitoreo y medición del sistema de gestión

- La evaluación del desempeño del sistema de gestión se establece en base a los objetivos y al alcance de este.
- Las actividades de monitoreo y medición del sistema de gestión de protección de datos personales están a cargo del gestor del sistema de gestión.
- En base a los resultados de esta actividad, el comité de privacidad y seguridad de la información propondrá acciones de mejora para el sistema de gestión de protección de datos personales.
- Se debe mantener documentación para todos los resultados del monitoreo y medición del sistema de gestión, incluyendo las propuestas de acciones de mejora.

Auditoría interna

- Se llevará a cabo un proceso de auditoría interna semestralmente con la finalidad de verificar el cumplimiento con los requisitos de ISO/IEC 27001:2013 y ISO/IEC 27701:2019 para el sistema de gestión de protección de datos personales.
- Los resultados de las auditorías internas deben presentarse al gestor del sistema de gestión como información documentada.
- El informe de auditoría interna debe contener un listado de no conformidades y acciones de mejora identificadas durante este proceso.
- El gestor del sistema de gestión de protección de datos personales informará a las áreas responsables para llevar a cabo los planes de acción generados como resultado de las auditorias.

Revisión por la alta dirección

- Semestralmente, se llevarán a cabo reuniones entre el gestor del sistema de gestión de protección de datos personales y la alta dirección con el fin de revisar el desempeño del sistema de gestión.
- La revisión por la alta dirección tomará en cuenta los cambios en el contexto interno y externo del sistema de gestión de protección de datos personales, el estado de las no conformidades, los resultados del monitoreo y medición, los resultados de las auditorías internas y los resultados de la gestión de riesgos.
- Todas las acciones de mejora propuestas durante la revisión por la alta dirección deben ser documentadas y comunicadas según se encuentra establecido en la matriz de comunicaciones del sistema de gestión de protección de datos personales.

Anexo E: Metodología de gestión de riesgos

- **Introducción**

Objetivo

El objetivo de este documento es brindar las directrices para llevar a cabo la gestión de riesgos como parte del sistema de gestión de protección de datos personales. Esta gestión se llevará a cabo en cuatro principales pasos, los cuales serán:

- Identificación de riesgos
- Análisis de riesgos
- Evaluación de riesgos
- Tratamiento de riesgos

Alcance

La gestión de riesgos se circunscribe al alcance del sistema de gestión de protección de datos personales, el cual consiste en el proceso de evaluación. Este proceso abarca todas las actividades que se dan desde la inscripción a las pruebas hasta la emisión de reportes de resultados.

Contexto

El contexto de la gestión de riesgos es el mismo que se detalló en el informe de contexto del sistema de gestión de protección de datos personales.

Comité de gestión de riesgos

Periódicamente se llevarán a cabo sesiones en las que se llevará a cabo una iteración de la gestión de riesgos según el estándar ISO 27005:2018. Estas sesiones han de realizarse por el comité de gestión de riesgos, el cual está conformado por las siguientes personas:

- Un representante de la dirección

- El gestor del sistema de gestión de protección de datos personales
- Un representante de las áreas de coordinación
- Un representante de los responsables de la bóveda
- Un representante del soporte administrativo

Se tomará en cuenta también la inclusión de todo personal que haya sido denominado como propietario de un activo de información.

- **Identificación de riesgos**

La primera etapa del proceso consiste en identificar todas las partes que constituyen un escenario de incidente de privacidad y seguridad de la información. Para esto, se identifican los activos de información de la organización, así como también las amenazas y vulnerabilidades relacionadas a estos. La descripción de esa relación es lo que constituye a un escenario de incidente.

Inventario de activos de información

El responsable del sistema de gestión de protección de datos personales mantendrá un registro de los activos de información que estén dentro del alcance del sistema de gestión. Este inventario de activos indicará el tipo de activo de información, según la siguiente tabla. Se debe indicar también la responsable de cada activo.

Tipo	Ejemplos
Actividades y procesos de negocio	o Procesos de logística o Procesos de gestión de TI o Proyectos
Información	o Contratos o Actas o Archivos virtuales o Documentación física

	○ Planes de negocio
Hardware	○ Laptops ○ Servidores ○ Impresoras ○ Discos duros externos ○ CD
Software	○ Sistemas operativos ○ Software de administración de servicios ○ Software de gestión de bases de datos ○ ERP ○ CRM
Redes	○ Redes ethernet ○ Routers ○ Hubs ○ Switches ○ Redes Wi-Fi
Personal	○ Alta dirección ○ Líder de proyectos ○ Gestores de riesgos ○ Gestión de recursos humanos ○ Administrador de sistemas
Instalaciones	○ Oficinas ○ Centros de procesamiento de datos ○ Edificios ○ Salas de servidores ○ Servicios de energía eléctrica
Organización	○ Autoridades ○ Áreas de la organización ○ Proveedores

Tomando en cuenta a los requisitos de protección de datos personales, también se indicará quienes son los propietarios de los datos personales que el activo pueda contener, en caso de que estos existan. En caso de presentarse datos personales, se debe indicar si entre estos se encuentran datos sensibles, para lo cual se puede tomar como referencia la tabla a continuación.

Datos sensibles
Datos biométricos
Datos referidos al origen racial y étnico
Ingresos económicos
Opiniones políticas, religiosas, filosóficas o morales
Afiliación sindical
Información relacionada a la salud o a la vida sexual

Identificación de amenazas

El comité de gestión de riesgos debe elaborar un listado de todas las amenazas que puedan afectar a los activos de información identificados. Se debe tener en cuenta el origen de las amenazas, el cual puede ser accidental, intencional o medio ambiental. Es posible extraer este listado, de catálogos de amenazas disponibles para el público.

La siguiente tabla muestra un listado de amenazas de seguridad de la información propuesto en ISO 27005:2011, la cual puede ser utilizada como un listado inicial

Amenaza	**Tipo**	**Accidental**	**Intencional**	**Ambiental**
Fuego	Daño físico	X	X	X
Daño por agua	Daño físico	X	X	X
Contaminación	Daño físico	X	X	X
Accidentes mayores	Daño físico	X	X	X
Destrucción de equipo o medios de almacenamiento	Daño físico	X	X	X

Polvo, corrosión, congelamiento	Daño físico	X	X	X
Fenómenos climáticos	Eventos naturales			X
Sismos, terremotos	Eventos naturales			X
Erupción volcánica	Eventos naturales			X
Fenómenos meteorológicos	Eventos naturales			X
Inundaciones	Eventos naturales			X
Falla en aire acondicionado o servicio de agua	Perdida de servicios esenciales	X	X	
Pérdida de energía eléctrica	Perdida de servicios esenciales	X	X	X
Falla en los equipos de telecomunicaciones	Perdida de servicios esenciales	X	X	
Radiación electromagnética	Disturbios por radiación	X	X	X
Radiación térmica	Disturbios por radiación	X	X	X
Pulsos electromagnéticos	Disturbios por radiación	X	X	X
Interceptación de señales de interferencia comprometidas	Compromiso de información		X	
Espionaje remoto	Compromiso de información		X	
Espionaje local o remoto	Compromiso de información		X	
Robo de documentos o medios de almacenamiento	Compromiso de información		X	
Robos de equipos	Compromiso de información		X	
Recuperación de medios de almacenamiento descartados o reciclados	Compromiso de información		X	

Revelación de información confidencial	Compromiso de información	X	X	
Datos de fuentes no confiables	Compromiso de información	X	X	
Manipulación mediante hardware	Compromiso de información		X	
Manipulación mediante software	Compromiso de información	X	X	
Localización de ubicaciones	Compromiso de información		X	
Falla de equipos	Fallas técnicas	X		
Malfuncionamiento de equipos	Fallas técnicas	X		
Saturación de sistemas de información	Fallas técnicas	X	X	
Malfuncionamiento de software	Fallas técnicas	X		
Incumplimiento del mantenimiento de los sistemas de información	Fallas técnicas	X	X	
Uso no autorizado de equipos	Acciones no autorizadas		X	
Copia fraudulenta de software	Acciones no autorizadas		X	
Uso de software falsificado o copiado	Acciones no autorizadas	X	X	
Corrupción de datos	Acciones no autorizadas		X	
Procesamiento ilegal de datos	Acciones no autorizadas		X	
Error de uso	Compromiso de funciones	X		
Abuso de derechos	Compromiso de funciones	X	X	
Falsificación de derechos	Compromiso de funciones		X	
Denegación de acciones	Compromiso de funciones		X	

Abuso de la disponibilidad del personal	Compromiso de funciones	X	X	X

Identificación de vulnerabilidades

El comité de gestión de riesgos identificará aquellas características de los activos de información que puedan ser explotadas por alguna amenaza. En base a esto se elaborará un listado de vulnerabilidades donde se indique el activo al que se relaciona cada vulnerabilidad.

Identificación de escenarios de incidentes y consecuencias

Una vez que se cuenta con los listados de amenazas y vulnerabilidades, el comité de gestión de riesgos procede a identificar los escenarios de incidentes. Esto consiste en describir como una amenaza puede explotar a una o más vulnerabilidades. Se debe indicar también la consecuencia de cada incidente como una descripción del impacto que este puede tener en el negocio, haciendo énfasis en los aspectos de privacidad y seguridad de la información.

- **Análisis de riesgos**

Valoración de activos

El valor de cada activo debe ser establecido por su respectivo propietario. Para esto, primero se valorizan los activos en función a los requisitos de seguridad de la información (confidencialidad, integridad y disponibilidad) para cada uno. Esto se lleva a cabo siguiendo los criterios de las tablas a continuación.

Niveles de confidencialidad

Nivel	Valor cuantitativo	Descripción
Público	0	La información se encuentra a disposición del público general.
Uso interno	1	Información que puede ser necesaria por el personal para llevar a cabo sus funciones. Es accesible por todo

		el personal. La divulgación de esta información al público puede implicar perdidas leves.
Restringido	2	Toda información de uso exclusivo para un área particular de la institución en estudio. La divulgación de esta al público puede implicar perdidas moderadas.
Confidencial	3	Información solo accesible para la alta dirección y el personal involucrado en el proceso de diagramación de instrumentos de evaluación. La divulgación de esta información puede traer severas pérdidas económicas o reputacionales.

Niveles de integridad

Nivel	Valor cuantitativo	Descripción
Normal	0	No se necesita mucha precisión en los datos. La modificación no autorizada de la información no incurre en ningún tipo de perdida para la institución en estudio.
Importante	1	Es necesario para llevar a cabo ciertos procesos en los que se requiere información precisa. La modificación no autorizada de la información puede traer pérdidas económicas leves.
Muy importante	2	Toda información que requiera de precisión alta o que se utilice en procesos contables o financieros de la institución en estudio. La modificación no autorizada de la información puede traer pérdidas económicas moderadas o graves.
Crítico	3	Toda información que requiera máxima precisión o que esté involucrada en los procesos de diagramación de instrumentos de evaluación y calificación de pruebas. La modificación no autorizada de esta información puede implicar que el servicio de evaluación de la institución en estudio se brinde de manera incorrecta.

Niveles de disponibilidad

Nivel	Valor cuantitativo	Descripción
Sustituible	0	El activo es fácilmente reemplazable y la falta de este no ocasiona ninguna pérdida para el negocio.
Necesario	1	El activo no puede ser reemplazado fácilmente, y es necesario para llevar a cabo los procesos del negocio. El máximo tiempo de indisponibilidad es de un día.

Muy necesario	2	El activo puede tener un tiempo de inaccesibilidad máximo de una hora.
Indispensable	3	El activo es esencial para el negocio y debe mantenerse accesible en todo momento.

Una vez hecho esto, se utiliza la suma de los tres valores cuantitativos para calcular el valor total del activo. En caso de que el activo posea datos personales, se le sumará uno al valor total. En caso de que los datos personales del activo constituyan datos sensibles, el valor que se sumará será 3, debido a la exigencia en las regulaciones de priorizar este tipo de información. De este modo, se obtiene un listado de activos con valores cuantitativos en un intervalo de 0 y 12. Esto permite una mayor facilidad al momento de priorizar los activos de información.

Evaluación de las consecuencias

El comité de gestión de riesgos evaluará los impactos que tendrán las consecuencias de los escenarios de incidentes previamente identificados. Para esto se tomarán en cuenta los siguientes factores:

- Valor financiero del activo en caso de perdida
- Costo de las operaciones suspendidas
- Violación de la ley de protección de datos
- Violación de acuerdos con los clientes
- Cantidad de titulares de datos personales afectados

El criterio para la evaluación de impactos es detallado en la siguiente tabla:

Nivel de impacto	**Valor numérico**	**Descripción**
Insignificante	0	El impacto es mínimo y solo implica pérdidas menores de tiempo
Menor	1	Implica pérdidas económicas menores

Moderado	2	El impacto implica pérdidas económicas o reputacionales moderadas
Significativo	3	Implica mayores pérdidas económicas y reputacionales. Los principales servicios de la institución en estudio son interrumpidos.
Catastrófico	4	Puede causar severas pérdidas económicas y reputacionales, o impide la realización del negocio de manera temporal o permanente.

Evaluación de probabilidades

El comité de gestión de riesgos determinará la probabilidad de ocurrencia para escenario identificado anteriormente. Para esto, se utilizarán los criterios de la tabla a continuación. Como se aprecia en la tabla, la probabilidad se basa en una estimación de la frecuencia de ocurrencia de los incidentes.

Probabilidad	Valor numérico	Descripción
Muy raro	0	Puede suceder una vez cada muchos años
Raro	1	Múltiples veces un año, pero no más de una vez al mes
Probable	2	Múltiples veces en un mes, pero no más de una vez a la semana
Común	3	Múltiples veces en una semana, pero no más de una vez al día
Certero	4	Múltiples veces en un día

Determinación del nivel de riesgo

El responsable del sistema de gestión de protección de datos personales determinará el nivel del riesgo una vez que se determinó la probabilidad de ocurrencia de los escenarios de incidentes y el impacto de sus consecuencias. El nivel de riesgo, será determinado como la suma de los valores cuantitativos de la probabilidad y el impacto.

- **Evaluación de riesgos**

Esta etapa consiste en priorizar los riesgos, una vez que se establecieron los niveles de riesgo para los escenarios de incidentes.

La priorización de los riesgos se basará en los niveles previamente hallados y servirá más adelante para priorizar los tratamientos de ciertos riesgos o para tomar decisión entre aceptar el riesgo o implementar controles para este. La siguiente tabla muestra el criterio para establecer la prioridad del riesgo según el nivel de este.

Prioridad	**Intervalo**
Aceptable	$N \in [0,1]$
Baja	$N = 2$
Media	$N \in [3,5]$
Alta	$N \in [6,8]$

Esta priorización se puede apreciar con mayor claridad en una matriz de evaluación de riesgos 5x5, como se presenta a continuación

	Insignificante	**Menor**	**Moderado**	**Significativo**	**Catastrófico**
Muy raro	Aceptable	Aceptable	Bajo	Medio	Medio
Raro	Aceptable	Bajo	Medio	Medio	Medio
Probable	Bajo	Medio	Medio	Medio	Alto
Común	Medio	Medio	Medio	Alto	Alto
Certero	Medio	Medio	Alto	Alto	Alto

- **Tratamiento de riesgos**

Una vez que se cuenta con la lista de riesgos, el comité de gestión de riesgos decidirá si es que los riesgos serán modificados, retenidos, evitados o compartidos.

Tratamiento	Descripción
Modificar	Implica la implementación de controles para mitigar la probabilidad o reducir el impacto del riesgo.
Retener	Se escoge retener el riesgo cuando se determina que este será aceptado y no se implementarán controles.
Evitar	Esta acción consiste en evitar toda actividad que conlleve a la posible materialización de un riesgo.
Compartir	La responsabilidad sobre el riesgo es compartida con una entidad externa.

El comité de gestión de riesgos estimará los nuevos valores de impacto y probabilidad para los riesgos asumiendo que las acciones de tratamiento son implementadas, y se calcula de este modo el nivel de riesgo residual. Este valor ha de ser evaluado según los criterios de evaluación y tratamiento de riesgos para determinar si el riesgo residual será aceptado o es necesario llevar a cabo otra iteración del proceso de tratamiento de riesgos.

Modificación de riesgos

En caso de que la acción a tomar sea la modificación del riesgo, el comité de gestión de riesgos mantendrá un listado de los controles propuestos para modificar el riesgo. Se debe especificar el riesgo al que corresponde cada control y si este es preventivo o correctivo.

Aceptación de riesgos

El comité de gestión de riesgos decidirá sobre la aceptación de riesgos, según los criterios para que esta se dé. El principal criterio para aceptar un riesgo de privacidad o seguridad de la

información es que el nivel de este sea de 1 o 0, como se puede apreciar en las tablas 9 y 10. Sin embargo, puede ser apropiado llevar a cabo un análisis de costo/beneficio para determinar si existen riesgos fuera de este rango que puedan ser aceptados. Esto se debe a que pueden presentarse situaciones en las que el costo de implementar controles para un riesgo es tan alto, de modo que la alternativa más viable es aceptar el riesgo o evitarlo completamente.

Anexo F: Listado de activos de información

ID	Nombre del activo	Descripción	Tipo de activo	Propietario	Titular de los datos personales	Confidencialidad	Integridad	Disponibilidad	Datos sensibles	Valoración
ACT-001	Drupal	Se utiliza como formulario de inscripción virtual	Software	Jefe de Evaluación	Participantes	Uso interno	Importante	Necesario	No	4
ACT-002	FormReturn	Se utiliza para la diagramación de fichas ópticas	Software	Jefe de Evaluación	Participantes	Uso interno	Importante	Necesario	No	4
ACT-003	Plataforma TIM	Se utiliza para el diseño de ítems con gráficos	Software	Jefe de Evaluación	No	Restringido	Importante	Necesario	No	4
ACT-004	FastTest	Se utiliza para almacenar el banco de preguntas	Software	Jefe de Evaluación	No	Confidencial	Crítico	Indispensable	No	9
ACT-005	InDesign	Se utiliza para la diagramación de los instrumentos de evaluación	Software	Jefe de Evaluación	No	Uso interno	Normal	Necesario	No	2
ACT-006	Chamilo Learning Management System	Plataforma para la aplicación de pruebas virtuales	Software	Jefe de Evaluación	Participantes	Restringido	Muy importante	Muy necesario	No	7
ACT-007	Trello	Plataforma para la organización de tareas	Software	Jefe de Evaluación	Personal administrativo	Uso interno	Importante	Necesario	No	4
ACT-008	Repositorio documental (Google Drive)	Almacena una tabla con datos de los clientes	Software	Dirección	Cliente	Confidencial	Crítico	Muy necesario	No	9
ACT-009	Computadoras de la bóveda	Se utilizan para la diagramación y gestión de instrumentos de evaluación	Hardware	Jefe de Evaluación	Participantes	Confidencial	Crítico	Necesario	No	8
ACT-010	Carpeta de archivos en la computadora de diagramación	Carpeta que contiene la información utilizada para el diseño de instrumentos de evaluación	Información	Dirección	No	Confidencial	Crítico	Indispensable	No	9
ACT-011	Disco duro externo	Almacena copias de respaldo para las computadoras de la bóveda	Hardware	Jefe de Evaluación	No	Confidencial	Muy importante	Muy necesario	No	7
ACT-012	Declaración jurada de confidencialidad	Documento firmado por los diagramadores de los instrumentos de evaluación	Información	Coordinadores ECC / ECP / EPA	Diagramadores	Uso interno	Normal	Necesario	No	3
ACT-013	Guía del constructor de ítems	Documento con directrices para la elaboración de ítems	Información	Coordinadores ECC / ECP / EPA	No	Uso interno	Importante	Sustituible	No	2
ACT-014	Guía del revisor de ítems	Documento con directrices para la revisión de ítems	Información	Coordinadores ECC / ECP / EPA	No	Uso interno	Importante	Sustituible	No	2
ACT-015	Adobe Acrobat Reader	Se utiliza para la lectura de documentos con formato PDF	Software	Jefe de Evaluación	No	Público	Normal	Necesario	No	1

ID	Nombre del activo	Descripción	Tipo de activo	Propietario	Titular de los datos personales	Confidencialidad	Integridad	Disponibilidad	Datos sensibles	Valoración
ACT-016	Dispositivo de almacenamiento externo	Dispositivo utilizado durante el proceso de impresión	Hardware	Direcció	No	Confidencial	Crítico	Muy necesario	No	8
ACT-017	Laptop para imprenta	Los instrumentos de evaluación son guardados en esta laptop para ser transportados a imprenta	Hardware	Jefe de Evaluación	No	Confidencial	Crítico	Muy necesario	No	8
ACT-018	Formato de revisión docente		Información	Coordinadores ECC / ECP / EPA	Diagramadores	Uso interno	Importante	Necesario	No	4
ACT-019	Formato de revisión por personal		Información	Coordinadores ECC / ECP / EPA	Personal	Uso interno	Importante	Necesario	No	4
ACT-020	Formato de supervisión docente		Información	Coordinadores ECC / ECP / EPA	Personal	Uso interno	Importante	Necesario	No	4
ACT-021	Acta de revisión de claves	Documento firmado por los aplicadores	Información	Coordinadores ECC / ECP / EPA	Personal administrativo y especialistas	Uso interno	Importante	Necesario	No	4
ACT-022	Acta de entrega de escáneres y llaves	Documento firmado por los aplicadores	Información	Jefe de Evaluación	Aplicadores	Uso interno	Importante	Necesario	No	4
ACT-023	Instrumento de evaluación físico	Conjunto de ítems de evaluación impresos	Información	Dirección	Participantes	Confidencial	Crítico	Indispensable	No	10
ACT-024	Instrumento de evaluación virtual	Conjunto de ítems de evaluación en la plataforma Camilo	Información	Dirección	Participantes	Confidencial	Crítico	Indispensable	No	10
ACT-025	Diagramadores de instrumentos de evaluación	Personal encargado de dar formato de examen al IE	Personal	Dirección	No	Confidencial	Crítico	Necesario	No	7
ACT-026	Aplicadores de la prueba	Personal encargado de supervisar la aplicación de las pruebas	Personal	Dirección	No	Uso interno	Importante	Necesario	No	3
ACT-027	Bóvedas	Espacios en los que se llevan a cabo los procesos de diagramación	Instalaciones	Dirección	Personal	Confidencial	Crítico	Indispensable	Sí	12
ACT-028	Proceso de inscripción	Proceso en el cual se registran los datos de los participantes de las pruebas	Actividades y procesos de negocio	Dirección	Participantes	Restringido	Muy importante	Muy necesario	No	7
ACT-029	Proceso de diagramación de instrumentos de evaluación	Proceso en el cual se brinda un formato a los instrumentos de evaluación	Actividades y procesos de negocio	Coordinadores ECC / ECP / EPA	No	Confidencial	Crítico	Muy necesario	No	8

ID	Nombre del activo	Descripción	Tipo de activo	Propietario	Titular de los datos personales	Confidencialidad	Integridad	Disponibilidad	Datos sensibles	Valoración
ACT-030	Aplicación de la prueba	Proceso en el cual los participantes pasan por la prueba	Actividades y procesos de negocio	Coordinadores ECC / ECP / EPA	Participantes	Restringido	Muy importante	Indispensable	No	8
ACT-031	Diseño de ítems	Proceso en el cual se diseñan los ítems de los instrumentos de evaluación	Actividades y procesos de negocio	Coordinadores ECC / ECP / EPA	No	Confidencial	Crítico	Indispensable	No	9
ACT-032	Diseñadores de ítems	Especialistas encargados del diseño de los ítems. Usualmente son docentes.	Personal	Coordinadores ECC / ECP / EPA	No	Confidencial	Crítico	Indispensable	No	9

Anexo G: Listado de amenazas y vulnerabilidades de privacidad y seguridad de la información

- **Catálogo de amenazas**

ID	Amenaza	Tipo	Accidental	Intencional	Ambiental
AME-001	Fuego	Daño físico	X	X	X
AME-002	Daño por agua	Daño físico	X	X	X
AME-003	Contaminación	Daño físico	X	X	X
AME-004	Accidentes mayores	Daño físico	X	X	X
AME-005	Destrucción de equipo o medios de almacenamiento	Daño físico	X	X	X
AME-006	Polvo, corrosión, congelamiento	Daño físico	X	X	X
AME-007	Fenómenos climáticos	Eventos naturales			X
AME-008	Sismos, terremotos	Eventos naturales			X
AME-009	Erupción volcánica	Eventos naturales			X
AME-010	Fenómenos meteorológicos	Eventos naturales			X
AME-011	Inundaciones	Eventos naturales			X
AME-012	Falla en aire acondicionado o servicio de agua	Perdida de servicios esenciales	X	X	
AME-013	Pérdida de energía eléctrica	Perdida de servicios esenciales	X	X	X
AME-014	Falla en los equipos de telecomunicaciones	Perdida de servicios esenciales	X	X	
AME-015	Radiación electromagnética	Disturbios por radiación	X	X	X
AME-016	Radiación térmica	Disturbios por radiación	X	X	X

ID	Amenaza	Tipo	Accidental	Intencional	Ambiental
AME-017	Pulsos electromagnéticos	Disturbios por radiación	X	X	X
AME-018	Interceptación de señales de interferencia comprometidas	Compromiso de información		X	
AME-019	Espionaje remoto	Compromiso de información		X	
AME-020	Espionaje local o remoto	Compromiso de información		X	
AME-021	Robo de documentos o medios de almacenamiento	Compromiso de información		X	
AME-022	Robos de equipos	Compromiso de información		X	
AME-023	Recuperación de medios de almacenamiento descartados o reciclados	Compromiso de información		X	
AME-024	Revelación de información confidencial	Compromiso de información	X	X	
AME-025	Datos de fuentes no confiables	Compromiso de información	X	X	
AME-026	Manipulación mediante hardware	Compromiso de información		X	
AME-027	Manipulación mediante software	Compromiso de información	X	X	
AME-028	Localización de ubicaciones	Compromiso de información		X	
AME-029	Falla de equipos	Fallas técnicas	X		
AME-030	Malfuncionamiento de equipos	Fallas técnicas	X		
AME-031	Saturación de sistemas de información	Fallas técnicas	X	X	

ID	Amenaza	Tipo	Accidental	Intencional	Ambiental
AME-032	Malfuncionamiento de software	Fallas técnicas	X		
AME-033	Incumplimiento del mantenimiento de los sistemas de información	Fallas técnicas	X	X	
AME-034	Uso no autorizado de equipos	Acciones no autorizadas		X	
AME-035	Copia fraudulenta de software	Acciones no autorizadas		X	
AME-036	Uso de software falsificado o copiado	Acciones no autorizadas	X	X	
AME-037	Corrupción de datos	Acciones no autorizadas		X	
AME-038	Procesamiento ilegal de datos	Acciones no autorizadas		X	
AME-039	Error de uso	Compromiso de funciones	X		
AME-040	Abuso de derechos	Compromiso de funciones	X	X	
AME-041	Falsificación de derechos	Compromiso de funciones		X	
AME-042	Denegación de acciones	Compromiso de funciones		X	
AME-043	Abuso de la disponibilidad del personal	Compromiso de funciones	X	X	X
AME-044	Incumplimiento de funciones	Negligencias	X	X	
AME-045	Fallas por parte de proveedores	Fallas técnicas	X	X	X
AME-046	Registro de información inconsistente	Negligencias	X	X	
AME-047	Ataques de ransomware	Ciberataque	X	X	

- **Catálogo de vulnerabilidades**

ID	Vulnerabilidad	Activos en los que se puede presentar
VUL-001	Presencia de bugs en el software	Drupal FormReturn Plataforma TIM FastTest InDesign Chamilo Learning Management System Trello
VUL-002	Dependencia en una licencia	Drupal Plataforma TIM Trello
VUL-003	Incompatibilidad con otra plataforma	FastTest
VUL-004	Plataforma es mantenida por terceros	Trello Google Drive
VUL-005	Antivirus susceptible a fallos	Computadoras de la bóveda
VUL-006	Equipo susceptible a fallos	Computadoras de la bóveda Laptop para imprenta
VUL-007	Falta de encriptación	Dispositivo de almacenamiento externo
VUL-008	Requiere de capacitación al personal	InDesign Plataforma TIM FastTest
VUL-009	Falta de capacitación en protocolos de seguridad de la información	Aplicadores de la prueba
VUL-010	Ubicación en una zona sísmica	Bóvedas
VUL-011	Susceptibilidad a incendios	Bóvedas
VUL-012	Falta de proceso formal para la firma de acuerdos de confidencialidad	Proceso de inscripción Proceso de diagramación de instrumentos de evaluación Aplicación de la prueba Proceso de diseño de ítems

Anexo H: Identificación, análisis y evaluación de escenarios de incidentes

- **Identificación de escenarios**

ID	Escenario	Consecuencia	Amenaza	Vulnerabilidad	Activos afectados
ESC-001	No se paga la licencia de Drupal	La plataforma de inscripción no se encuentra disponible para los participantes	AME-044	VUL-002	Drupal
ESC-002	No se paga la licencia de Trello	La plataforma de gestión de tareas no se encuentra disponible	AME-044	VUL-002	Trello
ESC-003	Fallas técnicas por parte del proveedor de Trello	La plataforma de gestión de tareas no se encuentra disponible	AME-045	VUL-004	Trello
ESC-004	No se paga la licencia de la plataforma TIM	La plataforma de elaboración de ítems no se encuentra disponible	AME-044	VUL-002	Plataforma TIM
ESC-005	Ítems creados en TIM no se pueden importar completamente en FastTest	Presencia de inconsistencias en los ítems del banco de preguntas	AME-046	VUL-003	Plataforma TIM FastTest Diseño de ítems Instrumento de evaluación físico Instrumento de evaluación virtual
ESC-006	Fallas técnicas en los servidores de Google	Carpeta de Drive inaccesible	AME-045	VUL-004	Repositorio documental

ESC-007	Las computadoras de diagramación sufren ataques de ransomware	Las carpetas de las computadoras de diagramación son inaccesibles. Indisponibilidad de las computadoras de diagramación	AME-047	VUL-005	Carpetas de archivos en las computadoras de diagramación Computadoras de la bóveda
ESC-008	Fallas en el disco duro de las computadoras de diagramación	Perdida de las carpetas en las computadoras de diagramación Indisponibilidad de las computadoras de diagramación	AME-029	VUL-006	Carpetas de archivos en las computadoras de diagramación Computadoras de la bóveda
ESC-009	Robo del dispositivo de almacenamiento y acceso a la información contenida	Filtración de contenido de instrumentos de evaluación	AME-021	VUL-007	Dispositivo de almacenamiento
ESC-010	La laptop para imprenta deja de funcionar	Imposibilidad de imprimir los instrumentos de evaluación	AME-029	VUL-006	Laptop para imprenta
ESC-011	Uso incorrecto de la herramienta InDesign	Errores en el instrumento de evaluación	AME-039	VUL-008	Instrumento de evaluación físico
ESC-012	El aplicador toma fotografías del instrumento de evaluación	Filtración de contenido de instrumentos de evaluación	AME-024	VUL-009	Instrumento de evaluación físico
ESC-013	Sismo de gran magnitud en Lima	Destrucción de la bóveda Destrucción de las computadoras de diagramación	AME-008	VUL-010	Bóvedas Computadoras de la bóveda

ESC-014	Incendio provocado en la bóveda de diagramación	Indisponibilidad temporal de la bóveda Destrucción de las computadoras de diagramación	AME-001	VUL-011	Bóvedas Computadoras de la bóveda
ESC-015	No se presentan declaraciones juradas de confidencialidad a los diagramadores	No hay forma de responsabilizar al diagramador en caso de incumplimiento	AME-024	VUL-012	Diseño de ítems Declaración jurada de confidencialidad
ESC-016	Uso incorrecto de la plataforma TIM	Errores en la elaboración de los ítems	AME-039	VUL-008	Diseño de ítems
ESC-017	Uso incorrecto de FastTest	Registro incorrecto de los ítems en el banco de preguntas	AME-039	VUL-008	FastTest

- **Análisis y evaluación de escenarios**

ID	Impacto	Probabilidad	Nivel de riesgo
ESC-001	Significativo	Raro	4
ESC-002	Moderado	Raro	3
ESC-003	Moderado	Muy raro	2
ESC-004	Significativo	Raro	4
ESC-005	Moderado	Común	5
ESC-006	Moderado	Muy raro	2
ESC-007	Catastrófico	Muy raro	4
ESC-008	Catastrófico	Muy raro	4
ESC-009	Significativo	Raro	4
ESC-010	Significativo	Muy raro	3
ESC-011	Significativo	Raro	4

ESC-012	Catastrófico	Raro	5
ESC-013	Catastrófico	Muy raro	4
ESC-014	Significativo	Muy raro	3
ESC-015	Significativo	Raro	4
ESC-016	Moderado	Raro	3
ESC-017	Moderado	Raro	3

Anexo I: Controles de privacidad y seguridad de la información propuestos

- **Controles propuestos**

ID	Control	ID del escenario	Tipo de control
CON-001	Implementar notificaciones con anticipación para el pago de la plataforma Drupal	ESC-001	Preventivo
CON-002	Implementar notificaciones con anticipación para el pago de la plataforma Trello	ESC-002	Preventivo
CON-003	Elaborar backups locales de la información contenida en Trello	ESC-003	Preventivo
CON-004	Implementar notificaciones con anticipación para el pago de la plataforma TIM	ESC-004	Preventivo
CON-005	Crear copia de respaldo local de los documentos del Drive	ESC-006	Preventivo
CON-006	Crear copia de respaldo del contenido de las carpetas de las computadoras de diagramación	ESC-007	Preventivo
CON-007	Realizar mantenimientos preventivos periódicos para las computadoras de diagramación	ESC-008	Preventivo
CON-008	Encriptar el dispositivo de almacenamiento externo	ESC-009	Preventivo
CON-009	Realizar mantenimientos preventivos periódicos para las laptops de imprenta	ESC-010	Preventivo
CON-010	Elaborar un manual de uso de InDesign para el proceso de diagramación de instrumentos de evaluación	ESC-011	Preventivo
CON-011	Capacitar al personal en los protocolos de seguridad de la información	ESC-012	Preventivo
CON-012	Implementar políticas estrictas para la aplicación de las pruebas	ESC-012	Preventivo
CON-013	Implementar sistemas de detección y alarma de incendios	ESC-014	Correctivo
CON-014	Establecer procesos formales y detallados para la diagramación de instrumentos de evaluación	ESC-015	Preventivo

CON-015	Elaborar un manual de uso de TIM para el proceso de elaboración de ítems	ESC-016	Preventivo
CON-016	Elaborar un manual de uso de FastTest para el proceso de elaboración de ítems	ESC-017	Preventivo

- **Opciones de tratamiento propuestas y niveles residuales de riesgo**

ID	Opción de tratamiento	Impacto residual	Probabilidad residual	Riesgo residual estimado
ESC-001	Modificar	Significativo	Muy raro	3
ESC-002	Modificar	Moderado	Muy raro	2
ESC-003	Modificar	Insignificante	Muy raro	0
ESC-004	Modificar	Significativo	Muy raro	3
ESC-005	Evitar	Moderado	Muy raro	2
ESC-006	Modificar	Menor	Muy raro	1
ESC-007	Modificar	Moderado	Muy raro	2
ESC-008	Modificar	Moderado	Muy raro	2
ESC-009	Modificar	Moderado	Raro	3
ESC-010	Modificar	Significativo	Muy raro	3
ESC-011	Modificar	Significativo	Muy raro	3
ESC-012	Modificar	Catastrófico	Muy raro	4
ESC-013	Retener	Catastrófico	Muy raro	4
ESC-014	Modificar	Moderado	Muy raro	2
ESC-015	Modificar	Significativo	Muy raro	3
ESC-016	Modificar	Moderado	Muy raro	2
ESC-017	Modificar	Moderado	Muy raro	2

Anexo J: Declaración de aplicabilidad

- **Controles de seguridad de la información según el Anexo A de ISO/IEC 27001:2013**

Objetivo	Número	Nombre	Aplicabilidad	Justificación
Dirección de la alta gerencia para la seguridad de la información	A.05.1.1	Políticas de privacidad y seguridad de la información	Sí	Es necesario contar con directrices para la correcta gestión de los activos de información
Dirección de la alta gerencia para la seguridad de la información	A.05.1.2	Revisión de las políticas de privacidad y seguridad de la información	Sí	Las políticas han de actualizarse constantemente según surjan nuevos requisitos o regulaciones
Organización interna	A.06.1.1	Roles y responsabilidades para la privacidad y seguridad de la información	Sí	Se debe definir responsabilidades dentro del sistema de gestión de privacidad
Organización interna	A.06.1.2	Segregación de funciones	Sí	Es necesario contar con la segregación de funciones para garantizar la integridad de los activos de información
Organización interna	A.06.1.3	Contacto con autoridades	Sí	Se necesita mantener el contacto con las entidades reguladoras según lo indique la legislación
Organización interna	A.06.1.4	Contacto con grupos especiales de interés	Sí	Se identificó la necesidad de mantener contacto con grupos especiales de interés para que la organización se mantenga al día respecto al panorama de riesgos de protección de datos personales

Objetivo	Número	Nombre	Aplicabilidad	Justificación
Organización interna	A.06.1.5	Seguridad de la información en la gestión de proyectos	Sí	Es necesario tomar en cuenta la seguridad información para todos los proyectos desarrollados por la institución en estudio
Dispositivos móviles y teletrabajo	A.06.2.1	Política de dispositivos móviles	No	No se considera el uso de dispositivos móviles para ninguna parte del proceso del alcance
Dispositivos móviles y teletrabajo	A.06.2.2	Teletrabajo	Sí	Es necesario definir políticas para situaciones en las que el personal no puede ejercer sus labores en las instalaciones de la institución en estudio
Previo al empleo	A.07.1.1	Selección	Sí	Se necesitan procesos definidos para la selección de especialistas en el diseño de ítems, diagramadores de instrumentos de evaluación y aplicadores.
Previo al empleo	A.07.1.2	Términos y condiciones del empleo	Sí	Es necesario asegurar que los días ganadores de instrumentos de evaluación, los diseñadores de ítems y los aplicadores de las pruebas firman un acuerdo de confidencialidad
Durante el empleo	A.07.2.1	Responsabilidades de la gerencia	Sí	Se necesita la participación activa de la gerencia para asegurar el cumplimiento de las políticas de privacidad y seguridad de la información

Objetivo	Número	Nombre	Aplicabilidad	Justificación
Durante el empleo	A.07.2.2	Conciencia, educación y capacitación sobre la privacidad y seguridad de la información	Sí	Es necesario capacitar en protocolos de seguridad de la información a todo el personal que forma parte del proceso de alcance del sistema de gestión
Durante el empleo	A.07.2.3	Proceso disciplinario	Sí	Se necesita una política de sanciones para casos de incumplimiento de privacidad y seguridad de la información
Terminación y cambio de empleo	A.07.3.1	Terminación o cambio de responsabilidades del empleo	Sí	La baja de personal no se contempla en el alcance del sistema de gestión
Responsabilidad de los activos	A.08.1.1	Inventario de activos	Sí	Como parte de la identificación de riesgos, es necesario contar con un inventario de activos de información
Responsabilidad de los activos	A.08.1.2	Propiedad de los activos	Sí	Es necesario identificar a los responsables de la gestión de cada activo de información
Responsabilidad de los activos	A.08.1.3	Uso aceptable de los activos	Sí	Es necesario contar con políticas para el uso aceptable de los activos de información
Responsabilidad de los activos	A.08.1.4	Retorno de activos	No	La baja de personal no se contempla en el alcance del sistema de gestión
Clasificación de la información	A.08.2.1	Clasificación de la información	Sí	Como parte del análisis de riesgos, se llevará a cabo la clasificación de los activos de información de la institución en estudio

Objetivo	Número	Nombre	Aplicabilidad	Justificación
Clasificación de la información	A.08.2.2	Etiquetado de la información	Sí	Los documentos de carácter sensible deben de ser etiquetados según corresponda y de acuerdo a la clasificación dada
Clasificación de la información	A.08.2.3	Manejo de activos	Sí	Se debe tener claro cómo es que se usa cada activo para sus respectivos procesos
Manejo de medios	A.08.3.1	Gestión de medios removibles	Sí	Es necesario dado que se usan medios removibles en el proceso de diagramación
Manejo de medios	A.08.3.2	Disposición de medios	Sí	Se necesitan controles para asegurar que los exámenes sean destruidos de manera segura una vez que fueron procesados
Manejo de medios	A.08.3.3	Transferencia de medios físicos	Sí	Es necesario establecer políticas de seguridad para el transporte de instrumentos de evaluación y escáneres
Requerimientos de negocio para el control de acceso	A.09.1.1	Política de control de acceso	Sí	Se necesita una política para la gestión de acceso a las bóvedas de la institución en estudio
Requerimientos de negocio para el control de acceso	A.09.1.2	Acceso a redes y servicios de red	Sí	Las computadoras de la bóveda de la institución en estudio ya se encuentran separadas en una red interna
Gestión de accesos de usuario	A.09.2.1	Registro y baja de usuarios	Si	Las personas que rinden las pruebas se registran en el sistema para la realización de estas
Gestión de accesos de usuario	A.09.2.2	Aprovisionamiento de acceso a usuario	Si	Las personas que rinden las pruebas se registran en el

Objetivo	Número	Nombre	Aplicabilidad	Justificación
				sistema para la realización de estas
Gestión de accesos de usuario	A.09.2.3	Gestión de derechos de acceso privilegiados	No	No está implicado en el proceso del alcance
Gestión de accesos de usuario	A.09.2.4	Gestión de información de autentificación secreta de usuarios	No	No está implicado en el proceso del alcance
Gestión de accesos de usuario	A.09.2.5	Revisión de derechos de acceso de usuarios	No	No está implicado en el proceso del alcance
Gestión de accesos de usuario	A.09.2.6	Remoción o ajuste de derechos de acceso	No	No está implicado en el proceso del alcance
Responsabilidades del usuario	A.09.3.1	Uso de información de autentificación secreta	No	No está implicado en el proceso del alcance
Control de acceso de sistemas y aplicaciones	A.09.4.1	Restricción de acceso a la información	Sí	El acceso a los activos de información debe brindarse según los roles definidos
Control de acceso de sistemas y aplicaciones	A.09.4.2	Procedimientos de ingreso seguro	Si	Se requieren medidas de ingreso seguro a las cuentas de usuario de los participantes de las pruebas
Control de acceso de sistemas y aplicaciones	A.09.4.3	Sistema de gestión de contraseñas	Si	Se requieren medidas de ingreso seguro a las cuentas de usuario de los participantes de las pruebas
Control de acceso de sistemas y aplicaciones	A.09.4.4	Uso de programas utilitarios privilegiados	No	No se hace uso de estos programas en el proceso del alcance
Control de acceso de sistemas y aplicaciones	A.09.4.5	Control de acceso al código fuente de los programas	No	No se presenta desarrollo de software en ninguna parte del alcance
Controles criptográficos	A.10.1.1	Políticas sobre el uso de controles criptográficos	Sí	Se necesita establecer formalmente políticas para el uso de controles criptográficos sobre los activos de información

Objetivo	Número	Nombre	Aplicabilidad	Justificación
				involucrados en el proceso de diagramación de instrumentos de evaluación
Controles criptográficos	A.10.1.2	Gestión de claves	Sí	Se contempla en la gestión de riesgos la necesidad de implementar controles criptográficos de gestión de claves para los dispositivos externos de almacenamiento
Áreas seguras	A.11.1.1	Perímetro de seguridad física	Sí	Se debe establecer el perímetro para aquellas áreas involucradas en los procesos de diagramación de instrumentos de evaluación y diseño de ítems de la institución en estudio
Áreas seguras	A.11.1.2	Controles de ingreso físico	Sí	Es necesario contar con políticas para controlar el ingreso del personal a la bóveda
Áreas seguras	A.11.1.3	Asegurar oficinas, áreas e instalaciones	Sí	Se necesita garantizar la seguridad de los activos de información que se encuentran dentro de la bóveda
Áreas seguras	A.11.1.4	Protección contra amenazas externas y ambientales	Sí	Se necesita garantizar la seguridad de los activos de información que se encuentran dentro de la bóveda
Áreas seguras	A.11.1.5	Trabajo en áreas seguras	No	No se contempla debido a que la modalidad actual de trabajo es virtual

Objetivo	Número	Nombre	Aplicabilidad	Justificación
Áreas seguras	A.11.1.6	Áreas de despacho y carga	No	No existen áreas de despacho y carga para la institución en estudio
Equipo	A.11.2.1	Emplazamiento y protección de los equipos	Sí	Es necesario este control para mitigar los riesgos de robo de dispositivos sensibles
Equipo	A.11.2.2	Utilidades de soporte	Sí	Se necesita para las computadoras de la bóveda
Equipo	A.11.2.3	Seguridad del cableado	Sí	Se necesita para las computadoras de la bóveda
Equipo	A.11.2.4	Mantenimiento de equipos	Sí	Se requiere un mantenimiento preventivo para las computadoras de diagramación en la bóveda y para laptops de imprenta
Equipo	A.11.2.5	Remoción de activos	No	No se lleva a cabo la remoción de activos en ningún proceso del alcance
Equipo	A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Sí	Esto es necesario debido a que hay casos en los cuales las pruebas se dan fuera de las instalaciones de la universidad
Equipo	A.11.2.7	Disposición o reutilización segura de equipos	Sí	Se determinó la necesidad de implementar este control debido al uso de las laptops de imprenta
Equipo	A.11.2.8	Equipos de usuario desatendidos	Sí	Se necesitan políticas relacionadas a esto para los equipos de la bóveda
Equipo	A.11.2.9	Política de escritorio limpio y pantalla limpia	Sí	Se necesitan políticas relacionadas a esto para los equipos de la bóveda

Objetivo	Número	Nombre	Aplicabilidad	Justificación
Procedimientos Operacionales y Responsabilidades	A.12.1.1	Procedimientos operativos documentados	Sí	Todos los procedimientos dentro del alcance del sistema de gestión deben ser documentados de forma detallada
Procedimientos Operacionales y Responsabilidades	A.12.1.2	Gestión del cambio	Sí	Es necesario dar un seguimiento a todos los cambios en los procesos del negocio para actualizar los documentos respectivos
Procedimientos Operacionales y Responsabilidades	A.12.1.3	Gestión de la capacidad	No	No está implicado en el proceso del alcance
Procedimientos Operacionales y Responsabilidades	A.12.1.4	Separación de los entornos de desarrollo, pruebas y operaciones	No	No se presenta desarrollo de software en ninguna parte del alcance
Protección de Software Malicioso	A.12.2.1	Controles contra códigos maliciosos	Sí	Se necesita aplicar estos controles para las computadoras de la bóveda
Respaldo	A.12.3.1	Respaldo de la información	Sí	Se necesita aplicar estos controles para las computadoras de la bóveda
Bitácoras y monitoreo	A.12.4.1	Registro de eventos	Sí	Se necesita registrar los eventos para facilitar la auditabilidad del sistema
Bitácoras y monitoreo	A.12.4.2	Protección de información de registros	Sí	Se observó la necesidad de proteger los registros de accesos a la bóveda
Bitácoras y monitoreo	A.12.4.3	Registros del administrador y del operador	Sí	Es importante saber en qué momento se accede a los registros de acceso a las bóvedas
Bitácoras y monitoreo	A.12.4.4	Sincronización de reloj	No	No se identificó la necesidad durante la gestión de riesgos

Objetivo	Número	Nombre	Aplicabilidad	Justificación
Control de software operacional	A.12.5.1	Instalación de software en sistemas operacionales	Sí	Es necesario contar con políticas respecto a la instalación de software en los dispositivos de cómputo usados por la institución en estudio
Gestión de vulnerabilidades técnicas	A.12.6.1	Gestión de vulnerabilidades técnicas	Sí	Se debe llevar a cabo la identificación de vulnerabilidades técnicas dentro de la gestión de riesgos para el proceso de diagramación de instrumentos de evaluación
Gestión de vulnerabilidades técnicas	A.12.6.2	Restricciones sobre la instalación de software	Sí	Es necesario contar con políticas respecto a la instalación de software en los dispositivos de cómputo usados por la institución en estudio
Consideraciones de auditoría de sistemas de información	A.12.7.1	Controles de auditoría de sistemas de información	Sí	Se identificó la necesidad de auditar periódicamente los accesos en la plataforma Chamilo
Gestión de seguridad en red	A.13.1.1	Controles de la red	Sí	Actualmente, las computadoras utilizadas para la diagramación se encuentran segregadas en una red interna.
Gestión de seguridad en red	A.13.1.2	Seguridad de servicios de red	Sí	Se identificó la necesidad garantizar la seguridad de la red a la que pertenecen las computadoras de diagramación-
Gestión de seguridad en red	A.13.1.3	Segregación en redes	Sí	Actualmente, las computadoras utilizadas para la diagramación se encuentran

Objetivo	Número	Nombre	Aplicabilidad	Justificación
				segregadas en una red interna.
Transferencia de información	A.13.2.1	Políticas y procedimientos de transferencia de información	Sí	Se identificó la necesidad de contar con políticas de transferencia de información personal a terceros, cumpliendo con lo requerido por la Ley 29733
Transferencia de información	A.13.2.2	Acuerdo sobre transferencia de información	Sí	En las políticas de transferencia de información, se debe indicar el requerimiento de acuerdos de transferencia de información
Transferencia de información	A.13.2.3	Mensajes electrónicos	Sí	Se identificó la necesidad de contar con controles que garanticen la seguridad de la información que es compartida por medios electrónicos.
Transferencia de información	A.13.2.4	Acuerdos de confidencialidad o no divulgación	Sí	Es necesario contar con políticas relacionadas a esto para los procesos de diagramación de instrumentos de evaluación diseño de ítems y aplicación de la prueba
Requerimientos de seguridad en sistemas de información	A.14.1.1	Análisis y especificación de requisitos de privacidad y seguridad de la información	Sí	Debido a las regulaciones existentes, se identificó la necesidad de especificar requisitos de seguridad y protección de datos personales
Requerimientos de seguridad en sistemas de información	A.14.1.2	Aseguramiento de servicios de aplicaciones sobre redes públicas	Sí	De observó que se requiere este control debido a que en el proceso de

Objetivo	Número	Nombre	Aplicabilidad	Justificación
				evaluación virtual, los participantes no se conectan directamente a una red de CMEC
Requerimientos de seguridad en sistemas de información	A.14.1.3	Protección de transacciones en servicios de aplicación	Sí	Se identificó la aplicabilidad de este control debido a que el usuario se loguea al sistema de evaluaciones utilizando información personal
Seguridad en el proceso de desarrollo y soporte	A.14.2.1	Política de desarrollo seguro	No	No se presenta desarrollo de software en ninguna parte del alcance
Seguridad en el proceso de desarrollo y soporte	A.14.2.2	Procedimientos de control de cambio del sistema	No	No se presenta desarrollo de software en ninguna parte del alcance
Seguridad en el proceso de desarrollo y soporte	A.14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa	No	No se presenta desarrollo de software en ninguna parte del alcance
Seguridad en el proceso de desarrollo y soporte	A.14.2.4	Restricciones sobre cambios a los paquetes de software	No	No se presenta desarrollo de software en ninguna parte del alcance
Seguridad en el proceso de desarrollo y soporte	A.14.2.5	Principios de ingeniería de sistemas seguros	No	No se presenta desarrollo de software en ninguna parte del alcance
Seguridad en el proceso de desarrollo y soporte	A.14.2.6	Ambiente de desarrollo seguro	No	No se presenta desarrollo de software en ninguna parte del alcance
Seguridad en el proceso de desarrollo y soporte	A.14.2.7	Desarrollo contratado externamente	No	No se presenta desarrollo de software en ninguna parte del alcance
Seguridad en el proceso de desarrollo y soporte	A.14.2.8	Pruebas de seguridad del sistema	No	No se presenta desarrollo de software en ninguna parte del alcance

Objetivo	Número	Nombre	Aplicabilidad	Justificación
Seguridad en el proceso de desarrollo y soporte	A.14.2.9	Pruebas de aceptación del sistema	No	No se presenta desarrollo de software en ninguna parte del alcance
Datos de prueba	A.14.3.1	Protección de los datos de prueba	No	No se presenta desarrollo de software en ninguna parte del alcance
Seguridad de la información en relaciones con el proveedor	A.15.1.1	Política de privacidad y seguridad de la información para las relaciones con los proveedores	No	No se comparte información confidencial de la institución en estudio ni datos personales con los proveedores
Seguridad de la información en relaciones con el proveedor	A.15.1.2	Abordar la seguridad dentro de los acuerdos con proveedores	No	No se comparte información confidencial de la institución en estudio ni datos personales con los proveedores
Seguridad de la información en relaciones con el proveedor	A.15.1.3	Cadena de suministro de tecnología de información y comunicación	No	No se cuenta con servicios de proveedores para la realización del proceso de evaluación
Gestión de entrega de servicios de proveedor	A.15.2.1	Monitoreo y revisión de los servicios de los proveedores	No	No se cuenta con servicios de proveedores para la realización del proceso de evaluación
Gestión de entrega de servicios de proveedor	A.15.2.2	Gestión de cambios a los servicios de proveedores	No	No se cuenta con servicios de proveedores para la realización del proceso de evaluación
Gestión de incidentes de seguridad de la información y mejoras	A.16.1.1	Responsabilidades y procedimientos	Sí	Se identificó la necesidad de establecer responsabilidades y procedimientos en las políticas de gestión de incidentes de seguridad de la información

Objetivo	Número	Nombre	Aplicabilidad	Justificación
Gestión de incidentes de seguridad de la información y mejoras	A.16.1.2	Reporte de eventos de privacidad y seguridad de la información	Sí	Es necesario elaborar periódicamente un reporte de los eventos relacionados a la privacidad y seguridad de la información dentro del proceso del alcance
Gestión de incidentes de seguridad de la información y mejoras	A.16.1.3	Reporte de debilidades de privacidad y seguridad de la información	Sí	Es necesario que un apoyo para la elaboración de un listado de acciones de mejora
Gestión de incidentes de seguridad de la información y mejoras	A.16.1.4	Evaluación y decisión sobre eventos de privacidad y seguridad de la información	Sí	
Gestión de incidentes de seguridad de la información y mejoras	A.16.1.5	Respuesta a incidentes de privacidad y seguridad de la información	Sí	Se identificó la necesidad de contar con planes de respuesta para todo tipo de incidente se seguridad de la información.
Gestión de incidentes de seguridad de la información y mejoras	A.16.1.6	Aprendizaje de los incidentes de privacidad y seguridad de la información	Sí	Se observó la necesidad de contar con una base de conocimiento adquirido durante los incidentes de seguridad, con el fin de poder afrontar dichos incidentes de manera más eficiente en el futuro
Gestión de incidentes de seguridad de la información y mejoras	A.16.1.7	Recolección de evidencia	Sí	
Continuidad de la seguridad de la información	A.17.1.1	Planificación de continuidad de privacidad y seguridad de la información	Sí	Se requiere la implementación de medidas que permita a hacer frente a las posibles interrupciones en los

Objetivo	Número	Nombre	Aplicabilidad	Justificación
				procesos de evaluación
Continuidad de la seguridad de la información	A.17.1.2	Implementación de continuidad de privacidad y seguridad de la información	Sí	Se requiere la implementación de medidas que permita a hacer frente a las posibles interrupciones en los procesos de evaluación
Continuidad de la seguridad de la información	A.17.1.3	Verificación, revisión y evaluación de continuidad de privacidad y seguridad de la información	Sí	Se requiere la implementación de medidas que permita a hacer frente a las posibles interrupciones en los procesos de evaluación
Redundancias	A.17.2.1	Instalaciones de procesamiento de la información	Sí	Debido a la necesidad de garantizar la disponibilidad de los sistemas durante el procedimiento de evaluación en línea, se determinó este control como aplicable
Cumplimiento con Requerimientos Legales y Contractuales	A.18.1.1	Identificación de requisitos contractuales y de legislación aplicables	Sí	Se debe tener en cuenta regulaciones como la Ley de Protección de Datos y similares
Cumplimiento con Requerimientos Legales y Contractuales	A.18.1.2	Derechos de propiedad intelectual	No	No corresponde al alcance del sistema de gestión de privacidad
Cumplimiento con Requerimientos Legales y Contractuales	A.18.1.3	Protección de registros	Sí	Se identificó la necesidad de proteger los registros de acuerdo a lo requerido por la ley 29733
Cumplimiento con Requerimientos Legales y Contractuales	A.18.1.4	Privacidad y protección de datos personales	Sí	Se debe tomar en cuenta a la Ley de Protección de Datos Personales

Objetivo	Número	Nombre	Aplicabilidad	Justificación
Cumplimiento con Requerimientos Legales y Contractuales	A.18.1.5	Regulación de los controles criptográficos	No	No se cuenta en el Perú con regulaciones sobre criptografía relevantes para el caso de la institución en estudio
Revisiones de seguridad de la información	A.18.2.1	Revisión independiente de la privacidad y seguridad de la información	Sí	Se identificó la necesidad de implementar procedimientos adicionales de revisión periódica al sistema de gestión
Revisiones de seguridad de la información	A.18.2.2	Cumplimiento de las políticas y normas de privacidad y seguridad de la información	Sí	Es necesario proponer mecanismos para dar seguimiento al cumplimiento de la política interna de privacidad y seguridad de la información
Revisiones de seguridad de la información	A.18.2.3	Revisión del cumplimiento técnico	Sí	Se contempla la necesidad de estas revisiones para los equipos utilizados por la institución en estudio durante el desarrollo de las pruebas

- **Controles para controladores de datos personales según el Anexo A de ISO/IEC 27701:2019**

Número	Nombre	Aplicabilidad	Justificación
A.07.2.1	Identificar y documentar propósito	Sí	Por cumplimiento de la Ley 29733
A.07.2.2	Identificar la base legal	Sí	Es necesario estar al día en cuanto a las regulaciones relacionadas a la protección de datos personales

Número	Nombre	Aplicabilidad	Justificación
A.07.2.3	Determinar cuándo y cómo obtener el consentimiento	Sí	Por cumplimiento de la ley 29733
A.07.2.4	Obtener y registrar el consentimiento	Sí	Por cumplimiento de la ley 29733
A.07.2.5	Evaluación de impactos de privacidad	Sí	Durante la gestión de riesgos, es necesario identificar y evaluar aquellos escenarios que tengan un impacto sobre la privacidad de los titulares de datos personales
A.07.2.6	Contratos con procesadores de datos personales	No	No existen procesadores de datos personales externos en ninguno de los procesos
A.07.2.7	Controlador de datos personales conjunto	No	No existen acuerdos con entidades externas en los que se establezca el rol de controlador de datos personales conjunto
A.07.2.8	Registros relacionados al procesamiento de datos personales	Sí	Por cumplimiento de la Ley 29733
A.07.3.1	Determinación y cumplimiento de obligaciones con los titulares de datos personales	Sí	Por cumplimiento de la Ley 29733
A.07.3.2	Determinación de la información para los titulares de datos personales	Sí	Por cumplimiento de la Ley 29733
A.07.3.3	Provisión de información a los titulares de datos personales	Sí	Por cumplimiento de la Ley 29733
A.07.3.4	Provisión de mecanismos para modificar o retirar el consentimiento	Sí	Por cumplimiento de la Ley 29733
A.07.3.5	Provisión de mecanismos para oponerse al procesamiento de datos personales	Sí	Por cumplimiento de la Ley 29733
A.07.3.6	Acceso, corrección y eliminación	Sí	Por cumplimiento de la Ley 29733

Número	Nombre	Aplicabilidad	Justificación
A.07.3.7	Obligaciones de los controladores de datos personales de informar a terceros	No	No se comparten los datos personales con terceros
A.07.3.8	Provisión de copias de datos personales procesados	Sí	Por cumplimiento de la Ley 29733
A.07.3.9	Manejo de solicitudes	Sí	Por cumplimiento de la Ley 29733
A.07.3.10	Toma de decisiones automatizada	No	No se lleva a cabo ningún procesamiento automatizado de datos personales
A.07.4.1	Limitar la recopilación	Sí	Por cumplimiento de la política interna de privacidad y seguridad de la información
A.07.4.2	Limitar el procesamiento	Sí	Por cumplimiento de la política interna de privacidad y seguridad de la información
A.07.4.3	Precisión y calidad	Sí	Por cumplimiento de la Ley 29733
A.07.4.4	Objetivos de minimización de datos personales	Sí	Por cumplimiento de la política interna de privacidad y seguridad de la información
A.07.4.5	Desidentificación y eliminación de los datos personales culminado el procesamiento	Sí	Es necesario asegurar la eliminación de los datos personales de los participantes de las pruebas una vez concluido el proceso de evaluación
A.07.4.6	Archivos temporales	Sí	Es necesario asegurar la eliminación de los datos personales de los participantes de las pruebas una vez concluido el proceso de evaluación

Número	Nombre	Aplicabilidad	Justificación
A.07.4.7	Retención	Sí	Es necesario asegurar la eliminación de los datos personales de los participantes de las pruebas una vez concluido el proceso de evaluación
A.07.4.8	Eliminación	Sí	Es necesario contar con procedimientos para que lo datos personales sean eliminados cuando ya no van a ser utilizados
A.07.4.9	Controles de transmisión de datos personales	No	Ningún dato personal es divulgado a terceros
A.07.5.1	Identificar la base para la transferencia de datos personales entre jurisdicciones	No	El flujo transfronterizo de datos personales no forma parte del alcance del sistema de gestión
A.07.5.2	Países y organizaciones internacionales a las que se puede transferir datos personales	No	El flujo transfronterizo de datos personales no forma parte del alcance del sistema de gestión
A.07.5.3	Registros de transferencia de datos personales	No	El flujo transfronterizo de datos personales no forma parte del alcance del sistema de gestión
A.07.5.4	Registros de divulgación de datos personales a terceros	No	Ningún dato personal es divulgado a terceros

- **Controles para procesadores de datos personales según el Anexo B de ISO/IEC 27701:2019**

Número	Nombre	Aplicabilidad	Justificación
B.08.2.1	Acuerdo del cliente	No	El procesamiento de datos personales se da bajo el nombre de la institución en estudio
B.08.2.2	Propósito de la organización	Sí	Por exigencia de la ley 29733
B.08.2.3	Uso para publicidad y marketing	No	No se utiliza ningún dato personal para propósitos de marketing y publicidad

Número	Nombre	Aplicabilidad	Justificación
B.08.2.4	Instrucciones infractoras	No	El procesamiento de datos personales se da bajo el nombre de la institución en estudio
B.08.2.5	Obligaciones del cliente	No	El procesamiento de datos personales se da bajo el nombre de la institución en estudio
B.08.2.6	Registros relacionados al procesamiento de datos personales	Sí	Por exigencia de la ley 29733
B.08.3.1	Obligaciones hacia los titulares de datos personales	Sí	Por exigencia de la ley 29733
B.08.4.1	Archivos temporales	Sí	Es necesario asegurar la eliminación de los datos personales de los participantes de las pruebas una vez concluido el proceso de evaluación
B.08.4.2	Retorno, transferencia y eliminación de datos personales	Sí	Es necesario asegurar la eliminación de los datos personales de los participantes de las pruebas una vez concluido el proceso de evaluación
B.08.4.3	Controles para la transmisión de datos personales	No	No se divulgan datos personales a terceros
B.08.5.1	Base para la transferencia de datos personales entre jurisdicciones	No	El flujo transfronterizo de datos personales no forma parte del alcance del sistema de gestión
B.08.5.2	Países y organizaciones internacionales a las que se puede transferir datos personales	No	El flujo transfronterizo de datos personales no forma parte del alcance del sistema de gestión
B.08.5.3	Registros de divulgación de datos personales a terceros	No	No se divulgan datos personales a terceros
B.08.5.4	Notificación de solicitudes de divulgación de datos personales	Sí	Es necesario notificar a los clientes respecto a solicitudes de divulgación de datos personales por parte de las autoridades
B.08.5.5	Divulgación de datos personales jurídicamente vinculante	Sí	Se tiene que declarar en las políticas de privacidad que la institución en

Número	Nombre	Aplicabilidad	Justificación
			estudio solo aceptará solicitudes de divulgación de datos personales por parte de las autoridades
B.08.5.6	Divulgación de subcontratistas procesadores de datos personales	No	La institución en estudio se encarga en la totalidad del manejo de los datos personales
B.08.5.7	Compromiso de subcontratistas para procesar datos personales	No	La institución en estudio se encarga en la totalidad del manejo de los datos personales
B.08.5.8	Cambio de subcontratistas de procesamiento de datos personales	No	La institución en estudio se encarga en la totalidad del manejo de los datos personales

Anexo K: Matriz de comunicación

Proceso	¿Qué se comunica?	Requisito según ISO	Emisor	Receptor	¿Cuándo se comunica?	¿Cómo se comunica?
Determinación de los procesos del alcance del SGP	Alcance y contexto del sistema de gestión de privacidad	27001 - 4.3	Administrador del sistema de gestión	Alta dirección	Durante el diseño del sistema de gestión	Reunión
Establecimiento de las políticas de privacidad y seguridad de la información	Políticas de privacidad y seguridad de la información	27001 - 5.2	Administrador del sistema de gestión	Alta dirección	Durante el diseño del sistema de gestión	Documento digital
Establecimiento de la metodología de gestión de riesgos para el sistema de gestión	Metodología de gestión de riesgos de privacidad y seguridad de la información	27001 - 6.1	Administrador del sistema de gestión	Comité de gestión de riesgos	Luego de la aprobación de la metodología de gestión de riesgos	Documento digital
Determinación de objetivos de privacidad y seguridad de la información	Objetivos de privacidad seguridad de la información	27001 - 6.2	Administrador del sistema de gestión	Comité de privacidad y seguridad de la información	Durante el diseño del sistema de gestión	En el documento de políticas del sistema de gestión
Establecimiento de la gestión documental	Estándar de gestión documental para el sistema de gestión de privacidad	27001 - 7.5	Administrador del sistema de gestión	Comité de privacidad y seguridad de la información	Durante el diseño del sistema de gestión	Documento digital
Gestión de riesgos	Resultados de la evaluación de riesgos	27001 - 8.2	Comité de gestión de riesgos	Alta dirección	Luego de llevar a cabo la evaluación de los riesgos	Presentación de análisis y evaluación en hojas de cálculo
Gestión de riesgos	Resultados del tratamiento de riesgos	27001 - 8.3	Comité de gestión de riesgos	Alta dirección	Luego de llevar a cabo el tratamiento de los riesgos	Presentación de informe de gestión de riesgos
Monitoreo y revisión	Cuadro de control del sistema de gestión	27001 - 9.1	Administrador del sistema de gestión	Alta dirección	Durante el diseño del sistema de gestión	Documento digital
Monitoreo y revisión	Resultados del monitoreo y medición	27001 - 9.1	Administrador del sistema de gestión	Alta dirección	Luego de llevar a cabo el monitoreo del sistema ges gestión	Reunión
Establecimiento del programa de auditorías internas	Programa de auditoría interna	27001 - 9.2	Administrador del sistema de gestión	Auditores internos	Durante el diseño del sistema de gestión	Documento digital
Auditoría interna	Informe de resultados de auditorías internas	27001 - 9.2	Auditores internos	Alta dirección	Luego de culminar la auditoría interna	Documento digital
Revisión por alta dirección	Resultados de la revisión por alta dirección	27001 - 9.3	Alta dirección	Entidades reguladoras	Luego de culminar la revisión por la alta dirección	Documento digital
Auditoría interna	No conformidades	27001 - 10.1	Auditores internos	Alta dirección	Durante el reporte de resultados de la auditoría interna	Reunión y documento digital
Revisión por alta dirección	Acciones correctivas	27001 - 10.1	Administrador del sistema de gestión	Comité de privacidad y seguridad de la información	Durante la reunión para la revisión por alta dirección	Reunión y documento digital

Proceso	¿Qué se comunica?	Requisito según ISO	Emisor	Receptor	¿Cuándo se comunica?	¿Cómo se comunica?
Establecimiento del marco de gestión de privacidad y seguridad de la información	Funciones y responsabilidades de privacidad y seguridad de la información	27001 - A.6.1.1	Alta dirección	Comité de privacidad y seguridad de la información	Durante el diseño del sistema de gestión	Reunión
Identificación de activos e implementación de controles sobre estos	Políticas del uso aceptable de los activos de información	27001 - A.8.1.3	Administrador del sistema de gestión	Propietarios de los activos de información	Durante la implementación de las políticas específicas de privacidad y seguridad de la información	Documento digital
Implementación de controles para la gestión de accesos	Políticas para las bóvedas de la institución en estudio	27001 - A.9.1.1	Comité de privacidad y seguridad de la información	Personal que hace uso de la bóveda	Durante la implementación de las políticas específicas de privacidad y seguridad de la información	Documento digital
Implementación de controles para la transferencia de información	Acuerdos de confidencialidad o no divulgación	27001 - A.13.2.4	Administrador del sistema de gestión	Diagramadores de instrumentos de evaluación y diseñadores de ítems	Al contratar el servicio de los diagramadores o diseñadores de ítems	Documento físico
Gestión de incidentes	Procedimiento para gestión de incidentes de privacidad y seguridad de la información	27001 - A.16.1.5	Administrador del sistema de gestión	Comité de privacidad y seguridad de la información	Durante el diseño del sistema de gestión	Reunión
Gestión de incidentes	Incidentes de privacidad y seguridad de la información	27001 - A.16.1.5	Comité de privacidad y seguridad de la información	Alta dirección	Cada dos meses después de establecer el procedimiento para la gestión de incidentes	Reunión
Implementación de controles para la continuidad de la privacidad y seguridad de la información	Planes para la continuidad de la privacidad y seguridad de la información	27001 - A.17.1.2	Administrador del sistema de gestión	Comité de privacidad y seguridad de la información	Luego de la aprobación del documento	Reunión
Identificación de la base legal y contractual	Requisitos legales, normativos y contractuales	27001 - A.18.1.1	Administrador del sistema de gestión	Comité de privacidad y seguridad de la información	Durante el diseño del sistema de gestión	Reunión
Obtención del consentimiento de los titulares de datos personales	Propósito del procesamiento de datos personales	27701 - A.7.3.3	Relaciones públicas	Titulares de datos personales	Previo a la inscripción de los participantes	Correo electrónico

Anexo L: Estándar de gestión documental del sistema de gestión

- **Proceso de gestión de información documentada del sistema de gestión de protección de datos personales**

Elaboración, revisión y aprobación:

- El gestor del sistema de gestión de protección de datos personales propone la información documentada del sistema de gestión de protección de datos personales y coordina su elaboración con los actores del sistema de gestión de acuerdo con sus responsabilidades.
- La alta dirección, en coordinación con el gestor del sistema de gestión de protección de datos personales, es responsable de la elaboración de los procedimientos específicos para la operación del sistema de gestión, incluyendo los registros correspondientes.
- Para el cumplimiento de lo indicado se debe coordinar con el gestor del sistema de gestión.
- Toda información documentada debe contar con la revisión y aprobación por parte de la alta dirección

Control de cambios:

- Todo documento del sistema de gestión de protección de datos personales debe contener un cuadro de control de cambios, en el que se contenga una descripción breve de todos los cambios por los que pasó el documento

Difusión, uso y protección de la integridad:

- Sólo tiene validez la información documentada del sistema de gestión de protección de datos personales que sea comunicada por cualquier medio establecido en la matriz de comunicaciones del sistema de gestión de protección de datos personales.

- El copiado e impresión de los documentos del sistema de gestión de protección de datos personales se realiza con la autorización escrita del gestor del sistema de gestión, a fin de asegurar el uso de la última versión de los documentos.
- Los colaboradores deben contar con la autorización y los permisos de los responsables respectivos para consultar y utilizar la información documentada que está clasificada como confidencial.

Seguimiento de la información documentada:

- La información documentada establecida por el sistema de gestión de protección de datos personales debe ser revisada como mínimo una vez al año (o según indique el propio documento) o cuando ocurran cambios estratégicos, organizacionales, operativos, tecnológicos o incidentes críticos de privacidad o seguridad de la información.

Retención y disposición final:

- La retención o tiempo de conservación de la información documentada fuera de vigencia debe ser al menos de 5 años, para efectos de revisión del sistema de gestión de seguridad de la información
- La disposición final tras el periodo de retención de toda información documentada del SGSI consiste en su eliminación digital y, donde aplique, a nivel físico.

Anexo M: Guía de implementación de controles de ISO/IEC 27001:2013 e ISO/IEC 27701:2019

- **Introducción**

En este documento se brindan las directrices para la implementación de los siguientes controles:

ISO/IEC 27001:2013 – Anexo A: 5.1.1, 5.1.2, 6.2.2, 7.2.3, 7.3.1, 8.1.3, 8.1.4, 8.3.1, 9.1.1, 10.1.1, 11, 13.2.1, 13.2.2, 13.2.3, 13.2.4, 15.1.1, 15.1.2, 15.1.3, 16, 18.1.4

ISO/IEC 27701:2019 – Anexo A: 7.2.1, 7.2.3, 7.4.9, 7.4.9, 7.4.9, 7.4.9, 7.4.9, 7.4.9

ISO/IEC 27701:2019 – Anexo B: 8.8.2.6, 8.8.4.1

La documentación elaborada como parte de la implementación de los controles, así como todo otro documento del sistema de gestión de protección de datos personales, debe incluirse en un listado maestro de información documentada, indicando la frecuencia de revisión para cada uno de estos documentos, según lo establecido en el estándar de gestión documental del sistema de gestión.

- **Políticas específicas**

Visión general

Con el objetivo de implementar gran parte de los controles del anexo A de ISO 27001 y los anexos A y B de ISO 27701 se propone la elaboración de los siguientes documentos:

- Políticas de privacidad y seguridad de la información para el teletrabajo
- Políticas de privacidad y seguridad de la información para la gestión de recursos humanos

- Políticas para el uso aceptable de los activos
- Políticas de control de accesos
- Políticas para el uso de controles criptográficos
- Políticas de seguridad física y ambiental
- Políticas de relaciones con proveedores
- Políticas de control de datos personales
- Políticas para el procesamiento de datos personales

Políticas de privacidad y seguridad de la información para el teletrabajo

En este documento, se detallarán los siguientes puntos:

- Cómo se llevarán a cabo los procesos de comunicación interna en un entorno de teletrabajo
- Cómo se llevarán a cabo los procesos del alcance del sistema de gestión de protección de datos personales y seguridad de la información (diseño de ítems, diagramación de instrumentos de evaluación, y aplicación de las pruebas)

Políticas de privacidad y seguridad de la información para la gestión de recursos humanos

En este documento, se detallarán los siguientes puntos:

- Qué políticas debe conocer el personal
- Qué conocimientos debe tener el gestor del sistema de gestión
- La realización de las actividades de concientización y capacitación

Políticas para el uso aceptable de los activos

En este documento, se detallarán los siguientes puntos:

- Cuál será el procedimiento para inventariar los activos de información adquiridos

- Asignación de responsables para los activos
- Quién está a cargo de supervisar la baja o reasignación de equipos de cómputo o dispositivos de almacenamiento
- Cuál será el procedimiento para el retorno de activos de información en caso de cese de empleo
- Cómo se manejarán los medios de almacenamiento removibles durante el proceso de impresión de las pruebas
- Quién se encarga de clasificar los activos de información
- Con qué criterios se clasificará la información (Elaborado en la metodología de gestión de riesgos)

Políticas de control de accesos

En este documento, se detallarán los siguientes puntos:

- Se debe especificar que los usuarios solo tendrán acceso a los activos que requieran para el desarrollo de sus funciones.
- Cuáles serán las excepciones al punto anterior
- Cómo se procesarán las solicitudes de acceso a información personal

Políticas para el uso de controles criptográficos

En este documento, se detallarán los siguientes puntos:

- Qué estándares y regulaciones deben cumplir los controles criptográficos a implementar
- Qué sistemas requieren de la aplicación de controles criptográficos
- Quién se encargará de implementar y dar mantenimiento a los controles criptográficos

Políticas de seguridad física y ambiental

En este documento, se detallarán los siguientes puntos:

- Qué áreas requieren de especial atención en cuanto a seguridad física
- Quienes pueden acceder a las bóvedas
- Qué objetos se pueden introducir a las bóvedas y cuales no
- Cuál es el procedimiento para el acceso a las bóvedas
- Por cuanto tiempo se almacenarán los registros de del control biométrico de las bóvedas
- Por cuanto tiempo se almacenarán las grabaciones de las cámaras de seguridad de las bóvedas
- Bajo qué circunstancias se revisarán las grabaciones de las cámaras de seguridad de las bóvedas
- Cuál será la frecuencia de actualización de los códigos de alarmas de las bóvedas
- Cuáles serán las políticas de pantalla limpia y escritorio limpio (por ejemplo, bloquear la pantalla al abandonar el lugar de trabajo)
- Quién se encargará del mantenimiento preventivo de los equipos
- Frecuencia del mantenimiento preventivo de equipos

Políticas de relaciones con proveedores

En este documento, se detallarán los siguientes puntos:

- Qué información será compartida con los proveedores
- Qué certificados deben tener los proveedores en cuanto a seguridad de la información
- Qué certificados de privacidad deben tener los proveedores en caso de que estos ofrezcan servicios de procesamiento de datos personales

Políticas para el tratamiento de datos personales

En este documento, se detallarán los siguientes puntos:

- Cómo se determinará y comunicará el propósito de la recopilación y procesamiento de datos personales

- Cuáles son las leyes y regulaciones de privacidad a las que se encuentra sujeta la institución en estudio
- Cuál será el procedimiento para la obtención y registro del consentimiento por parte de los participantes de las pruebas, los diseñadores de ítems, los diagramadores de las pruebas y los aplicadores de estas (por ejemplo, mediante correo electrónico o formularios en un sitio web)
- Cómo se almacenará el consentimiento de los titulares de datos personales
- Qué otra información se considera necesaria de comunicar a los titulares de datos personales (por ejemplo, notificación de fin de procesamiento de datos personales)
- Cómo se llevará a cabo la comunicación con los titulares de datos personales (por ejemplo, mediante correo electrónico)
- Cuál será el procedimiento para modificar o retirar el consentimiento de los titulares de datos personales
- Cuál será el procedimiento para la modificación o eliminación de datos personales
- Cuál es la mínima información privada (como campos o propiedades) necesaria para el proceso de evaluación
- Qué mecanismos se utilizarán para minimizar la recopilación y procesamiento de datos personales
- Cuál será el procedimiento para eliminar los archivos temporales generados (como tablas de Excel o bases de datos) por el procesamiento de datos personales
- Cuál será el periodo durante el cual se retendrán los datos personales luego de terminar el procesamiento de estos
- Qué datos personales serán procesados
- Cómo se llevará a cabo el procesamiento de datos personales
- Cómo se registrará el procesamiento de datos personales

- Qué archivos temporales serán creados durante el procesamiento de datos personales

- **Controles de seguridad física**

Bóvedas:

Las bóvedas son las zonas dentro de las instalaciones de la universidad privada a la que pertenece la institución en estudio, en las que se llevan a cabo los procesos de diseño de ítems y diagramación de instrumentos de evaluación. Dado que se trata de áreas en las que se procesa información sensible, las bóvedas son la principal prioridad en la implementación de controles de seguridad física.

Entre los controles que se deben implementar y mantener, se encuentran los siguientes:

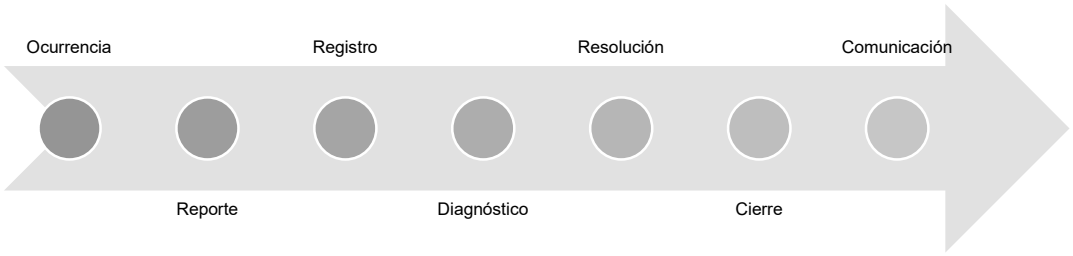
- Cámaras de seguridad hacia los exteriores de la bóveda
- Cámaras de seguridad hacia los interiores de la bóveda
- Personal de seguridad estacionado en la entrada de la bóveda
- Lector de huella digital para acceso a la bóveda
- Emplazamiento de equipos dentro de la bóveda

Las políticas alineadas a estos controles para la seguridad de la información de la bóveda se deben detallar en el documento de políticas de seguridad física y ambiental.

- **Gestión de incidentes de privacidad y seguridad de la información**

Ciclo de vida de los incidentes:

El gráfico a continuación muestra los procesos por los que han de pasar los incidentes de privacidad y seguridad de la información que se presenten en la institución en estudio.



Responsabilidades:

Todo colaborador ha de reportar los incidentes y vulnerabilidades de privacidad y seguridad de la información cuando estas sean identificadas. Esto es reportado al gestor del sistema de gestión de protección de datos personales, quien se encarga de registrar los incidentes y proponer los controles necesarios en colaboración con el comité de privacidad y seguridad de la información. La resolución del incidente estará a cargo de las personas que sean asignadas para cada incidente por el comité de privacidad y seguridad de la información. Finalmente, la comunicación de los resultados estará a cargo del gestor del sistema de gestión.

Gestión del conocimiento:

Se debe de mantener un repositorio de “Lecciones aprendidas”, el cual contendrá los resultados y conclusiones de incidentes previos. Este documento será comunicado según lo establecido en la matriz de comunicaciones. El propósito de este documento será el de ser la base para las mejoras propuestas en el futuro para el sistema de gestión de protección de datos.

Anexo N: Políticas específicas del Sistema de gestión

- **Políticas de privacidad y seguridad de la información para el teletrabajo**
    - El área técnica, en coordinación con el gestor del sistema de gestión de protección de datos personales, se encarga de definir que medios serán utilizados para la comunicación de cada uno de los puntos detallados en la matriz de comunicaciones del sistema de gestión
    - Los servicios de teletrabajo son usados estrictamente para las funciones asignadas al personal
    - Los accesos a los sistemas utilizados para el teletrabajo deben ser autorizados por el área técnica considerando las evaluaciones de riesgos de privacidad y seguridad de la información.
    - Para el acceso al teletrabajo se deben tener en cuenta las necesidades técnicas y tecnológicas que garanticen que el personal cuente con las herramientas necesarias para poder realizar su trabajo, así como las configuraciones de acceso seguro a los sistemas.
    - Todo dispositivo utilizado para las actividades de teletrabajo deberá cumplir con los requisitos mínimos de seguridad de la información establecidos por el área técnica
    - Las conexiones a servicios de teletrabajo deben permanecer encriptadas utilizando conexiones seguras o redes privadas entre el lugar dónde se realiza el teletrabajo
    - Todo el personal es responsable de reportar inmediatamente la pérdida o hurto de los equipos utilizados para el teletrabajo que se encuentren bajo su responsabilidad
    - No se permite la modificación de los controles de seguridad de la información implementados en los equipos autorizados para las actividades de teletrabajo

- No se permite brindar acceso a información, servicios o sistemas de información mediante los sistemas de teletrabajo a personal que no haya recibido la autorización por parte del área técnica
- El coordinador del área técnica se encarga de gestionar la implementación de controles de seguridad en los equipos empleados para el teletrabajo, según se establezca en los resultados de gestión de riesgos.

- **Políticas de privacidad y seguridad de la información para la gestión de recursos humanos**
  - El personal de diagramación de ítems, así como el personal encargado de la aplicación de las pruebas, deberá firmar un acuerdo de confidencialidad respecto al proceso de evaluación que se detalló como alcance del sistema de gestión
  - Todo el personal debe recibir capacitaciones sobre protección de datos personales y seguridad de la información periódicamente
  - En caso de cese de sus labores, el personal deberá seguir los procedimientos definidos por el área técnica para entregar su cuenta de usuario y accesos a servicios informáticos brindados.
  - No se permite el envío, descarga o visualización de información que no forma parte de las tareas asignadas al usuario de un sistema particular
  - El área de coordinación se encarga de solicitar la creación, modificación o cancelación de las cuentas de usuario para personal nuevo
  - Todo personal es responsable del cumplimiento y seguimiento de esta política y de velar por el cumplimiento de las políticas específicas.
- **Políticas para el uso aceptable de los activos**

- Se debe mantener en todo momento un catálogo de activos de información, el cual formará parte del proceso de gestión de riesgos de privacidad y seguridad de la información.
- Los activos de información serán etiquetados según su criticidad, tal como se establece en la metodología de gestión de riesgos.
- Todo activo que contenga datos personales sensibles debe ser etiquetado como tal y tratado con la mayor prioridad
- Todo el personal es responsable de la administración de controles de seguridad de la información sobre los activos tecnológicos que se le asigna
- El personal se compromete a cumplir las leyes y regulaciones relevantes a seguridad de la información y protección de datos personales que apliquen.
- Está prohibido utilizar los activos de información para fines diferentes al cumplimiento de las funciones asignadas
- El área técnica es encargada de llevar a cabo la revisión periódica de los privilegios de acceso otorgados a los usuarios de los activos de información.
- El coordinador del área técnica se encarga de supervisar la baja o reasignación de equipos de cómputo o dispositivos de almacenamiento
- En caso de cese de empleo, los activos de información asignados serán devueltos y se firmará un acta de devolución de activos.

- **Políticas de control de acceso**
  - El personal tendrá acceso únicamente a aquellos activos que se le hayan sido asignados para el desarrollo de sus funciones
  - Todo acceso a los sistemas de información debe ser autorizado por el área técnica.
  - Todo acceso a la información debe considerar el nivel de clasificación definido en la metodología de gestión de riesgos

- Todo acceso a la información debe cumplir con los requisitos legales y normativos relacionados a seguridad de la información y protección de datos personales.
- Solo se brindará acceso a sistemas con información personal a terceros, cuando este acceso haya sido explícitamente autorizado por los titulares de datos personales
- El acceso a los sistemas con información personal solo se brindará luego de la firma de una solicitud de acceso en la que se mencione y justifique explícitamente el motivo de la solicitud.

- **Políticas de controles criptográficos**
  - Toda información de carácter reservado o que contenga datos personales clasificados como sensibles se debe cifrar.
  - Se requiere el uso de algoritmos de cifrado asimétricos para la encriptación de la información sensible
  - Las laptops utilizadas para el proceso de impresión de pruebas, así como los dispositivos externos de almacenamiento también usados en este proceso, deben ser sometidas a procesos de encriptación.
  - El área técnica se encarga de la implementación de los controles criptográficos en los activos de información de la organización.
  - Periódicamente, el área técnica se encargará de la revisión de los controles criptográficos implementados
  - Luego de los procesos de encriptación, el área técnica mantendrá una copia de las claves de encriptación en lugar seguro.
  - Las claves utilizadas para la encriptación de la información se deben gestionar y proteger de acuerdo a las mejores prácticas, las cuales son promovidas por el área técnica.
  - Está prohibido revelar las claves privadas de encriptación a personal no autorizado.

- **Políticas de seguridad física y ambiental**
    - Solo se permite el acceso a las bóvedas para el personal encargado de la diagramación de las pruebas
    - Se debe mantener registros del ingreso a las bóvedas, indicando nombre de la persona que ingresa, documento nacional de identificación, fecha, hora de entrada y salida, y motivo de la visita.
    - No se permite el ingreso de computadoras portátiles, cámaras o dispositivos móviles a las bóvedas.
    - Los datos registrados para el acceso a las bóvedas se almacenarán por un periodo de seis meses.
    - Cada mes o ante la ocurrencia de incidentes de filtración de información se llevará a cabo una revisión de las grabaciones de las cámaras de seguridad de las bóvedas.
    - Los códigos de alarma de las bóvedas de actualizarán cada tres meses.
    - Todo personal debe bloquear la pantalla de los computadores a su cargo en caso de ausentarse.
    - Del mismo modo, los documentos físicos deben ser almacenados en lugares seguros durante periodos de ausencia del personal.
    - Periódicamente, el área técnica se encargará de realizar actividades de mantenimiento preventivo a los equipos tecnológicos.
    - El personal debe ser contantemente capacitado en temas de seguridad ocupacional y protocolos ante situaciones de desastres.
- **Política de relaciones con proveedores**
    - Los proveedores solo tendrán acceso a los sistemas de información que son indispensables para el cumplimiento de sus requisitos contractuales.

- Se establecerán los requerimientos de seguridad de la información y protección de datos personales que debe cumplir el proveedor al momento de elaborarse el contrato.
- Para los proveedores de sistemas en los que se procese información crítica, se requerirá que cuenten con un sistema de gestión de seguridad de la información certificado.
- Del mismo modo, los proveedores de servicios que procesen datos personales, requerirán demostrar que cuentan con medidas de cumplimiento de la ley de protección de datos personales.

- **Políticas de tratamiento de datos personales**
  - Todo personal es responsable del cumplimiento de estas políticas con el fin de garantizar el cumplimiento con la ley de protección de datos personales
  - El tratamiento de datos personales se rige por los principios establecidos en la Ley 29733 – Ley de protección de datos personales
  - Antes de registrar la información de los participantes de las pruebas, se les informará sobre sus derechos de acuerdo a la ley de protección de datos personales, así como el propósito del tratamiento de los datos y las formas en los que estos serán tratados.
  - Se obtendrá el expreso consentimiento por parte de los titulares de datos personales para el tratamiento de estos datos, luego de haberles brindado la información requerida por la ley.
  - Se debe contar con procedimientos para que los titulares de datos personales, puedan hacer uso de los derechos ARCO (Acceso, rectificación, cancelación y oposición). Para esto, el área de coordinación mantendrá un formato de formulario

de solicitud de acceso a los derechos ARCO, el cual los titulares deberán llenar para hacer uso de estos derechos.

- Ante cualquier incidente que ponga en riesgo la confidencialidad de los datos personales recopilados, se informará a los titulares mediante correos electrónicos y llamadas telefónicas, en la mayor brevedad posible.
- Solo se recopilarán aquellos datos personales que sean estrictamente necesarios para el desarrollo del proceso de evaluación.
- Los datos personales recopilados se mantendrán por un periodo máximo de seis meses.
- Se mantendrá un formato de solicitud de cesión de datos personales para casos en los que terceros necesiten acceder a estos datos. Para la cesión de estos datos, será necesario obtener el consentimiento expreso de los titulares de datos personales.

Anexo O: Cuadro de control del sistema de gestión

- **Indicadores para los objetivos del sistema de gestión**

Objetivo	Indicador	Valor objetivo	Responsable de la medición	Frecuencia de medición
Asegurar el cumplimiento con el marco legal para privacidad y seguridad de la información	Porcentaje de puntos de la ley de protección de datos personales cubiertos en la documentación del sistema de gestión	> 90%	Gestor del sistema de gestión	Trimestral
Garantizar la disponibilidad del proceso de evaluación en todo momento	Número de días en los que el proceso de evaluación no está disponible	< 2 días	Gestor del sistema de gestión	Trimestral
Garantizar la confidencialidad e integridad del contenido de instrumentos de evaluación	Porcentaje de incidentes de seguridad de la información correspondientes a los instrumentos de evaluación que han sido resueltos	> 90%	Gestor del sistema de gestión	Trimestral
Garantizar la confidencialidad e integridad de los datos personales de los	Porcentaje de controles de ISO 27002 adaptados para la protección de datos personales	> 95%	Gestor del sistema de gestión	Trimestral

participantes de las evaluaciones				

- **Indicadores para los procesos del sistema de gestión**

Objetivo	Indicador	Valor objetivo	Responsable de la medición	Frecuencia de medición
Gestión de riesgos	Porcentaje de activos de información con vulnerabilidades identificadas	> 90%	Gestor del sistema de gestión	Trimestral
	Porcentaje de escenarios de riesgos con tratamientos propuestos	> 90%	Gestor del sistema de gestión	Trimestral
	Porcentaje de controles propuestos que han sido implementados	> 90%	Gestor del sistema de gestión	Trimestral
Auditoría interna	Porcentaje de no conformidades identificadas que fueron levantadas	100%	Gestor del sistema de gestión	Trimestral
	Porcentaje de acciones de mejora implementadas	> 90%	Gestor del sistema de gestión	Trimestral
Diseño del sistema de gestión	Porcentaje de requisitos de ISO 27001 y 27701 implementados	100%	Alta dirección	Mensual

	Porcentaje de personal con roles asignados en el sistema de gestión	> 90%	Alta dirección	Mensual
Comunicación	Porcentaje de procesos mapeados en la matriz de comunicaciones	> 80%	Gestor del sistema de gestión	Trimestral
Concientización y capacitación	Porcentaje de asistencias a las charlas sobre privacidad y seguridad de la información	> 80%	Gestor del sistema de gestión	Trimestral
	Promedio obtenido en los test de privacidad y seguridad de la información	> 7/10	Gestor del sistema de gestión	Trimestral

- **Indicadores para los controles de ISO/IEC 27001:2013 e ISO/IEC 27701:2019**

Objetivo	**Indicador**	**Valor objetivo**	**Responsable de la medición**	**Frecuencia de medición**
27001.A.5.1.1	Porcentaje de políticas aprobadas por la alta dirección	> 95%	Gestor del sistema de gestión	Trimestral
	Número de incidentes de incumplimiento de políticas reportado	< 10	Gestor del sistema de gestión	Mensual
27001.A.7.2.3	Porcentaje de incidentes de incumplimiento de políticas que fueron	> 95%	Gestor del sistema de gestión	Trimestral

	sancionados según lo establecido en las políticas del sistema de gestión			
27001.A.8.2.2	Porcentaje de documentos que han sido debidamente etiquetados	> 95%	Gestor del sistema de gestión	Trimestral
27001.A.10.1.1	Porcentaje de sistemas con información sensible en los que se aplicaron controles criptográficos	> 95%	Gestor del sistema de gestión	Trimestral
27001.A.12.2.1	Número de incidentes relacionados a malware identificados en un mes	< 5	Gestor del sistema de gestión	Mensual

Anexo P: Cuadro de validación de entregables

A continuación, se muestra una tabla que contiene los acuerdos establecidos en las actas de reunión con la institución en estudio. Para mayor detalle sobre cada una de las actas de reunión, enviar un correo a cgirbau@pucp.pe.

N°	Fecha	Acuerdos
1	11/05/2020	1. Se aprueba el Diagrama del Proceso en BPMN. 2. Se aprueba el Informe del Análisis del Contexto. 3. La institución en estudio enviará los documentos presentados en la reunión, con sus comentarios: Metodología de Gestión de Riesgos, Inventario de Activos, Evaluación de Riesgos (verificará los valores propuestos para la probabilidad e impacto) y Plan de Tratamiento de Riesgos.
2	21/05/2020	1. Se aprueba la Metodología de gestión riesgos de privacidad y seguridad para el SG 2. Se aprueba el Inventario de activos (incluyendo aspectos de datos personales y datos sensibles) 3. Se aprueba el documento de Evaluación de Riesgos y Plan de tratamiento de riesgos. 4. La institución en estudio enviará los documentos presentados en la reunión, con sus comentarios: Declaración de Aplicabilidad y Matriz de Comunicaciones.
3	01/06/2020	1. Se aprueba la Declaración de Aplicabilidad para el SG. 2. Se aprueba la Matriz de Comunicaciones para el SG. 3. La institución en estudio enviará los documentos presentados en la reunión, con sus comentarios: Política del SGP y Gestión documentaria para el SGP
4	01/07/2020	1. La institución en estudio da conformidad a los entregables finales del proyecto de Diseño de un Sistema de Gestión de la Privacidad según ISO 27701:2019. 2. Se envió el compilado de todos los entregables (y sus versiones editables) a la institución en estudio.