



UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

**PROGRAMA ACADÉMICO DE MAESTRÍA EN
INGENIERÍA DE SISTEMAS CON MENCIÓN EN
TECNOLOGÍAS DE LA INFORMACIÓN**

**Incidencia de la tecnología data loss prevention en la
prevención de fuga de datos en un gobierno regional, Lima
2022**

AUTOR:

Olivares Zevallos, Jorge William (orcid.org/0000-0003-2155-5120)

ASESOR:

Mg. Cardeña Peña, Jorge Manuel (orcid.org/0000-0003-3176-8613)

LÍNEA DE INVESTIGACIÓN:

Infraestructura y Servicios de Redes y Comunicaciones

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA — PERÚ

2022

Dedicatoria

A mi familia, mis abuelos, mis tíos, mis hermanos y sobre todo a Dios, que me bendice para culminar la tesis para obtener el grado de Magister.

Agradecimiento

A todas las personas que me dieron la fuerza para no rendirme y seguir hasta lograr el objetivo planteado durante el transcurso del proyecto de investigación, que posteriormente se convirtió en Tesis.

Índice de contenidos

	Pág
Carátula	i
Dedicatoria	ii
Agradecimiento	iii
Índice de contenidos	iv
Índice de tablas	v
Índice de gráficos y figuras	vii
Resumen	viii
Abstract	ix
I. INTRODUCCIÓN	1
II. MARCO TEÓRICO	6
III. METODOLOGÍA	20
3.1. Tipo y diseño de investigación	20
3.2. Variables y operacionalización	20
3.3. Población, muestra y muestreo	24
3.4. Técnicas e instrumentos de recolección de datos	26
3.5. Procedimientos	29
3.6. Método de análisis de datos	29
3.7. Aspectos éticos	29
IV. RESULTADOS	31
V. DISCUSIÓN	47
VI. CONCLUSIONES	58
VII. RECOMENDACIONES	60
REFERENCIAS	62
ANEXOS	69

Índice de tablas

	Pág
Tabla 1 Matriz de operacionalización de la variable independiente: Data Loss Prevention.	22
Tabla 2 Matriz de operacionalización de la variable dependiente: Prevención de fuga de datos.	23
Tabla 3 Caracterización de la población.	25
Tabla 4 Caracterización de la muestra.	26
Tabla 5 Ficha Técnica del instrumento de medición.	27
Tabla 6 Validación del instrumento de recolección de datos.	28
Tabla 7 Resultado del análisis de confiabilidad a través del Alfa de Cronbach.	28
Tabla 8 Caracterización de la recolección de datos a través del cuestionario	31
Tabla 9 Tabla cruzada V1: Data Loss Prevention * V2: Prevención de fuga de datos.	32
Tabla 10 Tabla cruzada V1: Data Loss Prevention * V2-D1: Previene datos en uso.	33
Tabla 11 Tabla cruzada V1: Data Loss Prevention * V2-D2: Previene datos en movimiento.	34
Tabla 12 Tabla cruzada V1: Data Loss Prevention * V2-D3: Previene datos en reposo.	35
Tabla 13 Pruebas de normalidad de V1: Data Loss Prevention y V2: Prevención de fuga de datos.	36
Tabla 14 Información sobre el ajuste del modelo que explica la incidencia de la variable Data Loss Prevention en la variable prevención de fuga de datos.	37
Tabla 15 Bondad de ajuste de la incidencia de la variable Data Loss Prevention en la variable prevención de la fuga de datos.	37
Tabla 16 Pseudo R Cuadrado de la incidencia de la variable Data Loss Prevention en la variable prevención de fuga da datos.	38
Tabla 17 Estimaciones de los parámetros de incidencia de la variable Data Loss Prevention en la variable prevención de la fuga de datos.	38
Tabla 18 Información sobre el ajuste del modelo de líneas paralelas que explica la incidencia de la variable Data Loss Prevention en la dimensión previene datos en uso de la variable prevención de fuga de datos.	39

Tabla 19 Bondad de ajuste de la incidencia de la variable Data Loss Prevention en la dimensión previene datos en uso de la variable prevención de fuga de datos.	40
Tabla 20 Pseudo R Cuadrado de la incidencia de la variable Data Loss Prevention en la dimensión previene datos en uso de la variable prevención de fuga de datos.	40
Tabla 21 Estimaciones de los parámetros de incidencia de la variable Data Loss Prevention en la dimensión previene datos en uso de la variable prevención de fuga da datos.	41
Tabla 22 Información sobre el ajuste del modelo de líneas paralelas que explica la incidencia de la variable Data Loss Prevention en la dimensión previene datos en movimiento de la variable prevención de fuga de datos.	42
Tabla 23 Bondad de ajuste de la incidencia de la variable Data Loss Prevention en la dimensión previene datos en movimiento de la variable prevención de fuga de datos.	42
Tabla 24 Pseudo R Cuadrado de la incidencia de la variable Data Loss Prevention en la dimensión previene datos en movimiento de la variable prevención de fuga de datos.	43
Tabla 25 Estimaciones de los parámetros de incidencia de la variable Data Loss Prevention en la dimensión previene datos en movimiento de la variable prevención de fuga da datos.	43
Tabla 26 Información sobre el ajuste del modelo de líneas paralelas que explica la incidencia de la variable Data Loss Prevention en la dimensión previene datos en reposo de la variable prevención de fuga de datos.	44
Tabla 27 Bondad de ajuste de la incidencia de la variable Data Loss Prevention en la dimensión previene datos en reposo de la variable prevención de fuga de datos	45
Tabla 28 Pseudo R Cuadrado de la incidencia de la variable Data Loss Prevention en la dimensión previene datos en movimiento de la variable prevención de fuga de datos.	45
Tabla 29 Estimaciones de los parámetros de incidencia de la variable Data Loss Prevention en la dimensión previene datos en movimiento de la variable prevención de fuga da datos.	46

Índice de gráficos y figuras

	Pág
Figura 1 Histograma, V1: Data Loss Prevention * V2: Prevención de fuga de datos	32
Figura 2 Histograma, V1: Data Loss Prevention * V2-D1: Previene datos en uso	33
Figura 3 Histograma, V1: Data Loss Prevention * V2-D2: Previene datos en movimiento	34
Figura 4 Histograma, V1: Data Loss Prevention * V2-D3: Previene datos en reposo	35

Resumen

Con la aparición de la 4ta. Revolución Industrial o Industria 4.0, se conjugan: las tecnologías digitales, los recursos humanos y los activos físicos; con lo cual directa o indirectamente los servicios se convierten en un medio a través del cual se cocrea valor, al proporcionar los resultados que los clientes o usuarios desean obtener. Debido a ello, el principal problema que se presenta se centra en la fuga de datos - que se estima que llegan al 44%.

En el Perú se creó la Oficina Nacional de Gobierno Electrónico e Informática a cargo del Sistema Nacional de Informática. Asimismo, debido al marco legal vigente, las instituciones públicas, como los Gobiernos Regionales, tienen la obligación de diseñar e implementar un Sistema de Gestión de Seguridad de la Información, desde el año 2016. Ante el inminente riesgo latente de fuga de datos y su uso de manera intencional o no, urge la detección a tiempo para impedir que los datos sean filtrados o eliminados, mediante el uso de la tecnología Data Loss Prevention la cual mitigaría la fuga de los datos almacenados en el gobierno regional para satisfacer el interés general y el bien común a través de la función pública.

Palabras clave: DLP, Prevención de fuga de datos, descubrimiento, prevención, protección.

Abstract

With the appearance of the 4th. Industrial Revolution or Industry 4.0 are combined: digital technologies, human resources, and physical assets; with which, directly or indirectly, the services become a means through which value is co-created, by providing the results that the clients or users want to obtain. Due to this, the main problem that arises focuses on data leakage - which is estimated to reach 44%.

In Peru, the National Office of Electronic Government and Informatics was created in charge of the National Information System. Likewise, due to the current legal framework, public institutions, such as Regional Governments, have the obligation to design and implement an Information Security Management System, since 2016. Given the imminent latent risk of data leakage and its use intentionally or not, early detection is urgent to prevent data from being leaked or deleted, through the use of Data Loss Prevention technology, which would mitigate data leakage. the data stored in the Regional Government to satisfy the general interest and the common good through the public function.

Keywords: DLP, data lost prevention, discovery, prevention, protection.

I. INTRODUCCIÓN

Al aparecer la 4ta. Revolución Industrial o Industria 4.0, se conjugan: las tecnologías digitales, los recursos humanos y los activos físicos; con lo cual directa o indirectamente los servicios se convierten en un medio a través del cual se co-crea valor, al proporcionar los resultados que los clientes o usuarios desean obtener. En este sentido, son las instituciones las que tienen que estar a la vanguardia mediante el uso de tecnologías que nos permitan resguardar los datos, garantizando la seguridad de estos durante cada proceso o fase de cada servicio que se ofrece o requiere el cliente o usuario para satisfacer su demanda u oportunidad. Debido a ello, el principal problema que se presenta durante los procesos anteriormente mencionados se centra en la fuga de datos (salida no controlada de información sensible por parte de servidores públicos, ya sea por medios impresos, correos electrónicos, verbal u otros, la cual llega a personas no autorizadas) - que se estima que llegan al 44% (Sealpath, 2022).

En consecuencia, a nivel mundial dichos resultados esperados están siendo provistos por la gerencia de Tecnologías de la Información (TI) de las instituciones, sean estas públicas o privadas para lograr que se cumplan los objetivos estratégicos mediante el uso de datos, que después se transforman en información por medio de los procesos que se generan a través de los flujos de la cadena de valor. Para fines del año 2021, el 90% de las instituciones implementarán por lo menos una herramienta especializada de Data Loss Prevention (DLP), con relación al 50% que lo hizo en el año 2017 (Koenig, 2019, como se cita en Gartner, 2017).

Según Corona (2020) el fin principal del Sistema de Gestión de la Seguridad de la Información (SGSI) es la protección de los datos sensibles de las instituciones que le sirven en sus actividades primordiales. De esta manera, debemos comprender y a su vez, gestionar los riesgos inminentes para responder de manera adecuada con confidencialidad, integridad y disponibilidad; también debemos considerar dos aspectos principales: (1) la autenticación y (2) el no repudio.

Situándonos en las instituciones públicas que promueven la Inversión Privada, la cual es muy sensible y no se hará presente en donde no se controlen los datos confidenciales, y sobre todo con los que se trabajan día a día los servidores públicos de manera cotidiana, en algunos casos de manera remota debido a la pandemia que nos agobia desde el mes de marzo del 2020. La inversión privada es necesaria; motivo por el cual se debe crear un compromiso entre el beneficio lucrativo de los inversionistas y un beneficio general de mantener una parte importante de desarrollo de las residencias y los comercios manteniendo un espacio público acogedor para el ciudadano (Borja, 2009). Mondragón (2020) sostiene que, la co-creación de valor al ofrecer y proveer un servicio tecnológico, motiva el desarrollo de un enfoque que congrega el estilo de percepción de los usuarios con la entrega de los servicios, ofrecidos de cara al usuario o cliente.

En ese sentido son las instituciones públicas las llamadas a generar las condiciones que permitan una garantía, a través del fortalecimiento de las Asociaciones Público-Privadas (APP). Por otro lado, a nivel nacional, de acuerdo con ProInversión (2015) las APP se encargan de la distribución de riesgos y recursos. Tal es así, que según el artículo 8 de la Ley 28059, los gobiernos locales y regionales crearon las Agencias de Fomento de la Inversión Privada (AFIP), las cuales deben estar conformadas por: el Gobierno local o regional, el sector privado, las agrupaciones y los gremios de productores y, finalmente los emprendedores adscritos a su localidad (Ministerio de Economía y Finanzas, 2003).

Asimismo, el año 2019 se adjudicaron cuatro proyectos Asociaciones Público - Privadas en el Perú por 351,7 millones de dólares (ProInversión, 2020). Así también, se creó la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) (Presidencia del Consejo de Ministros, 2003) como la entidad reguladora y administradora del Sistema Nacional de Informática (Presidencia del Consejo de Ministros, 2004), siendo la encarga desde el año 2004 de la publicación de las pautas relativas al SGSI, ayudando a las entidades del estado en la protección de su información, fomentando el desarrollo e impulsando un SGSI. Asimismo, debido al marco legal vigente, las instituciones públicas tienen

la obligación de diseñar e implementar un SGSI, la cual fue admitida el año 2016 con la Resolución Ministerial N° 004-2016-PCM (Presidencia del Concejo de Ministros, 2016).

A nivel local, la herramienta que se utilizó para identificar la problemática de una manera sencilla fue la elaboración del árbol de problemas de la institución estatal del gobierno regional (revisar en los anexos), la cual tiene como principal propósito mejorar el servicio a los ciudadanos, a través del servicio de diseño, seguimiento de gestión, generando y fortaleciendo la capacidad institucional por medio de la gobernanza digital teniendo como aliado de esta implementación al Sistema de Gestión de la Seguridad (SGS) – ISO NTP/IEC 27001:2014 para cumplir con la Continuidad Tecnológica de esta Infraestructura, es que se tiene la necesidad de instaurar los lineamientos de la seguridad de la información referentes con la prevención, así como la recuperación ante ataques, afectando a la información que se maneja y dañando seriamente la visibilidad de la institución (Presidencia del Concejo de Ministros, 2016).

Bajo esta coyuntura, la gerencia de inversión de un gobierno regional en estos últimos años ha venido invirtiendo recursos en la prevención de la fuga de datos al cual se le considera como un activo fundamental y uno de los principales junto con el recurso humano, al igual que las diversas sedes de las unidades orgánicas de un gobierno regional, se ejecutan acciones a través de las políticas del SGSI para evitar la pérdida de datos confidenciales. Pero son insuficientes dado que algunos de los usuarios tienen acceso a información sensible, lo que provocaría la pérdida o fuga de la información por rotación o salida de los servidores públicos y por el abuso de los conocimientos informáticos por parte del área usuaria; así mismo, por el mal uso de equipos y aplicativos, dado que los datos puede ser copiados a una carpeta a través del Google Drive, para posteriormente descargarla en otro equipo y de esta manera se realiza la fuga de información (Albors, 2017).

Ante el inminente riesgo latente, urge la detección a tiempo para impedir que los datos sean filtrados, eliminados física o lógicamente, ya sea de manera intencional o no, mediante el uso de la tecnología Data Loss Prevention se

mitigaría la fuga de los datos almacenados en el gobierno regional por los servidores públicos mediante la asistencia de servicios públicos a los ciudadanos, para satisfacer el interés general y el bien común a través de la función pública.

Por lo anteriormente mencionado, se cuestionó como problema general: ¿De qué manera Data Loss Prevention incide en la prevención de fuga de datos en un gobierno regional, Lima 2022?; así mismo, se presentan los problemas específicos siguientes: (1) ¿De qué manera Data Loss Prevention incide en la dimensión de previene datos en uso en la prevención de fuga de datos en un gobierno regional, Lima 2022?; (2) ¿De qué manera Data Loss Prevention incide en la dimensión de previene datos en movimiento en la prevención de fuga de datos en un gobierno regional, Lima 2022?; (3) ¿De qué manera Data Loss Prevention incide en la dimensión de previene datos en reposo en la prevención de fuga de datos en un gobierno regional, Lima 2022?

La tesis realizada se justifica a través de distintos aspectos que se mencionan a continuación:

La justificación epistemológica, se expresa a lo largo del desarrollo de la investigación mediante las revisiones de los conceptos científicos adecuados y teorías para alcanzar una adecuada enunciación del problema al utilizar el procedimiento científico. Asimismo, según los axiomas recopilados durante el progreso del desarrollo de la investigación se validarán las hipótesis planteadas, tomando en consideración la razonabilidad y su estrecho vínculo con la verdad.

En lo concerniente con la justificación teórica, tenemos que se basa esencialmente con el fin de acrecentar el conocimiento relacionado a la tecnología Data Loss Prevention y las fases de la Promoción de la Inversión Privada (PIP). Para lograr aportar conocimientos para las investigaciones subsecuentes.

En relación con la justificación práctica, afirmo que se fundamenta en

que el uso de la implementación de la tecnología Data Loss Prevention planteada en el desarrollo de la tesis, que puede impactar en el Plan de Continuidad Operativa (PCO) y en el SGS – ISO NTP/IEC 27001:2014, nos permitirá lograr una significativa visibilidad de TI, debido a la temprana detección de la fuga de datos.

En último lugar, tenemos a la justificación metodológica, podemos mencionar que se justifica ya que el estudio puede contribuir a generar un nuevo método para darle mayor seguridad a los datos que se manejan dentro de la institución. Con el objetivo de lograr resultados fehacientes, se sostiene que a través de una adecuada recopilación de los datos será una herramienta íntegra y validada por el juicio de expertos.

En relación con el objetivo general de la tesis, se formula: Determinar la incidencia de Data Loss Prevention en la prevención de fuga de datos en un gobierno regional, Lima 2022. Como consecuencia, tenemos los objetivos específicos siguientes: (1) Determinar la incidencia de Data Loss Prevention en la dimensión de previene datos en uso de prevención de fuga de datos en un gobierno regional, Lima 2022. (2) Determinar la incidencia de Data Loss Prevention en la dimensión de previene datos en movimiento de prevención de fuga de datos en un gobierno regional, Lima 2022. (3) Determinar la incidencia de Data Loss Prevention en la dimensión de previene datos en reposo de prevención de fuga de datos en un gobierno regional, Lima 2022.

De este modo, se instituyó que la hipótesis general: Data Loss Prevention incide significativamente en la prevención de fuga de datos en un gobierno regional, Lima 2022. De modo que las hipótesis específicas son: (1) Data Loss Prevention incide significativamente la dimensión de previene datos en uso de la prevención de fuga de datos en un gobierno regional, Lima 2022; (2) Data Loss Prevention incide significativamente la dimensión de previene datos en movimiento de prevención de fuga de datos en un gobierno regional, Lima 2022; (3) Data Loss Prevention incide significativamente la dimensión de previene datos en reposo de prevención de fuga de datos en un gobierno regional, Lima 2022.

II. MARCO TEÓRICO

Para desarrollar la tesis, se tuvo por su utilidad enfatizar los siguientes estudios científicos relacionados anteriormente por su estrecha relación con el tema desarrollado, de modo que sustenten este estudio:

En cuanto a antecedentes nacionales, se encuentra a Machicao (2019), en su investigación “Análisis de riesgo y políticas de Seguridad de Información de la Oficina de Tecnologías de Información (OTI)-UNA Puno 2018”, quién planteó como objetivo el investigar los riesgos existentes en la OTI, mediante el uso de la metodología experimental para elaborar las Políticas de Seguridad de la Información (PSI), a través del estudio de riesgo según la NT ISO/IEC 27001:2014, y el Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y Comunicaciones y, de Seguridad de la Información (MAAGTICSI) a una población y tamaño de muestra de 12 personas, incluyendo a la jefa de la OTI; a través de su instrumento de recolección utilizado (cuestionario), llegó a la conclusión que, después de estudiar los peligros que agobian a la OTI y demarcando su estructura, para elaborar las PSI, en salvaguardar la información en todas sus formas, debido a que es un activo principal, al que debemos garantizarle la confidencialidad, integridad y disponibilidad, siendo administrada y almacenada en diferentes medios, físicos o virtuales.

Ccesa (2017), investiga el “Diseño de un sistema de gestión de Seguridad de la Información bajo la NTP ISO/IEC 27001:2014 para la Municipalidad Provincial de Huamanga, 2016” sostuvo que, fue justo instaurar una apropiado SGSI que coadyuve a resguardar la confidencialidad, integridad y disponibilidad, debido a que las entidades públicas integrantes del SNI se les insta en la culminación de la NTP ISO/IEC 27001:2014; su población fueron los servidores públicos de la Municipalidad Provincial de Huamanga y, su muestra fue no probabilística de seis servidores públicos de la Subgerencia de Sistemas y Tecnología (SST). Utilizó una metodología no experimental – transaccional descriptivo, gestionando los peligros de Seguridad de la Información (SI), el cual dividió la investigación en tres partes: primero, se hizo el diagnóstico inicial tomando en consideración la NTP ISO/IEC 27001:2014; segundo, analizó la

institución y su argumento, se identificaron los procesos críticos y se concretó la política de seguridad, su alcance e instauración de la comisión de seguridad de la información; y tercero, identificó los elementos de configuración durante la indagación así como las amenazas latentes, se calculó el impacto del peligro y las herramientas de control requeridas para reducir los peligros encontrados al mínimo admisible; con lo cual llegó a la conclusión que gran parte de la afectación de la seguridad de la información depende del cliente o usuario, motivo por el cual se debe generar una cultura para identificar y apreciar los elementos de configuración, y las amenazas ocultas o latentes, medir su influencia en la identificación de los posibles peligros a los que están expuestos los usuarios.

Acero (2019), investigó la “Implementación de un sistema de internet de las cosas para optimizar la gestión del agua en la agricultura de la Región Tacna, 2018” quien se planteó el propósito de demostrar la certidumbre en la ejecución de Internet of Things (IOT) hacia lograr la perfeccionar en la comisión del agua a los sembríos, a una población de 14 parcelas que utilizan un pozo de agua ubicado en la Yarada-Los Palos y su muestra fue un terreno con un área aproximada de 3535 m² donde se cultiva de Olivo, que contaba con un reservorio de cerca de 600000 litros de agua y mediante una metodología aplicada, su técnica de recolección fue la aplicación del IOT al riego por goteo, mediante la utilización de un temporizador para realizar la respectiva comparación y el instrumento de recolección utilizado fue el Damla para valorar la confianza del riego por goteo. Como resultados, demostró que coexiste una necesidad en mejorar el proceso del riego de los cultivos en la optimización de la administración del recurso agua en los sembríos; con lo cual precisó que al aplicar esta solución que está basada en la industria 4.0, IOT y tecnologías de almacenamiento en la nube; esta herramienta a su vez permitirá automatizar, controlar y monitorear los datos para propulsar la sostenibilidad en la ciudad a través del uso de conectividad y servicios en entornos digitales.

Otro resultado fue el de Moscoso et al. (2018), en la tesis de nombre “Modelo de gestión de riesgos de TI que contribuye a la operación de los procesos de gestión comercial de las empresas del sector de saneamiento del

Norte del Perú” de Chiclayo, quien se planteó favorecer la mejora de los conocimientos de gestión comercial mediante un tipo de comisión de peligros de TI beneficioso para las instituciones proveedoras del servicio de saneamiento en el norte del Perú. La población utilizada en la investigación se trató de las compañías de saneamiento del norte del Perú catalogadas según la Superintendencia Nacional de Servicios de Saneamiento (SUNASS) como grandes empresas y su muestra de manera censal fue la compañía EPSEL S.A. en las técnicas comerciales y micro medición considerándose tres grupos, detectando la falta de gestión de peligros o su no implementación correcta; así mismo, estableció que los conocimientos de gestión de riesgos de TI no son considerados adecuadamente por el gerente de TI, realizando una refutación a posteriori ante escenarios desfavorables en los servicios tecnológicos ofrecidos por el área de TI, aumentando el peligro de aparición de pérdidas económicas y de la visibilidad de la empresa EPSEL S.A.. Utilizó las técnicas de recolección: encuestas y entrevistas, así como su instrumento de recolección: el cuestionario. El modelo fue validado por expertos con experiencia comprobada, aplicando la fiabilidad el Alfa de Cronbach y la correlación en base a Kendall. Obtuvo los siguientes resultados: se identificaron 165 peligros, siendo 52 catalogados de alta prioridad, se programaron tácticas de mitigación en 16 de ellas, como realizar el monitoreo y evidenciar que la comisión de riesgos contribuye en el ejercicio de los conocimientos de gestión comercial; quien afirmó que, es posible identificar los peligros que si llegaran a ocurrir afectarían la normal operatividad de cada uno de los procesos de gestión comercial institucionales y que para contrarrestarlo se tendría que tomar una decisión proactiva, utilizando los recursos y actividades para lograr una mejora continua, antes que una reactiva que conlleva los costos inherentes para corregir un riesgo materializado.

Finalmente, Ponce et al. (2019), investigaron las “Buenas prácticas en la gestión del Riesgo de Fraude Interno: Casos de tres bancos de Lima Metropolitana”, quien se planteó el propósito de detallar las buenas experiencias para lograr la mejora en la administración de los peligros de dolo interno en las principales entidades bancarias en una población que abarca a las instituciones financieras, el muestreo fue no probabilístico. Utilizaron el diseño no experimental, un enfoque cualitativo y su técnica de recolección fue entrevistas

a los funcionarios. Obtuvieron los siguientes resultados: se equiparó un acumulado de buenas prácticas implementadas en las entidades bancarias seleccionadas, encontrándose semejanza entre ellas y coincidiendo en que las pérdidas de dinero por este tipo de suceso aumentan año tras año, haciendo complicada su predicción. Concluyendo que, el uso de una herramienta de gestión permite el control de los posibles eventos de fraude interno, basado en observación de patrones inusuales automatizado, permitiendo a través de la investigación un accionar oportuno, evitándose la generación de pérdidas de dinero y reputación por fraude interno.

En el entorno de los antecedentes internacionales, tenemos a García et al. (2017), en su disertación titulada “Sistema de cifrado basado en contexto aplicado a prevención de fuga de datos” de Valencia (España) quien se planteó que el objetivo de que las herramientas DLP están aumentando, debido a que urge la necesidad de protección de los datos confidenciales. La gran mayoría de las tecnologías DLP se centran en el análisis de datos (archivos que se almacenan o que están en tránsito), la tecnología DLP analizada utiliza el cifrado basado en contexto. Quien concluyó que, la fuga de datos es considerada una amenaza emergente en las instituciones, si son principalmente realizadas por sus colaboradores y sólo se enfocan en evitar la fuga por atacantes externos y tratan a sus clientes o usuarios otorgándoles una absoluta confianza. Asimismo, indica que una herramienta DLP es sumamente necesaria porque mantiene la seguridad de la información sensible e impide de esta manera posibles filtraciones no autorizadas.

Husham et al. (2020), en su estudio “Data loss prevention by using MRSH-v2 algorithm” de Bagdad (Iraq) quien se planteó el objetivo o propósito de que las DLP’s son buenas herramientas para identificar datos confidenciales. DLP puede realizar análisis del contenido de datos y enviar comentarios a los administradores para que tomen decisiones, como filtrar, eliminar o cifrar estos datos; obtuvo los siguientes resultados: Los datos confidenciales pueden almacenarse en diferentes formas. No solo los propietarios legales, sino también las personas maliciosas son interesantes para obtener datos confidenciales. Exponer datos valiosos a otros conduce a graves consecuencias. Los clientes,

organizaciones o empresas pierden su dinero y reputación debido a violaciones de datos. Hay muchas razones para las fugas de datos. Las amenazas internas, como los errores humanos, y las amenazas externas, como los Distributed Denial Of Service (DDoS), son dos razones principales para la pérdida de datos. En general, los datos se pueden clasificar y almacenar en función de tres tipos: en uso, reposo y en movimiento. Las DLP son buenas herramientas para identificar datos importantes. Sostuvo que, es muy importante proteger los datos independientemente de lo que almacene. Los datos son importantes no solo para los propietarios legítimos, sino también para los atacantes. Concluye que hay muchos tipos de técnicas DLP, y la coincidencia de aproximación es una de ellas. Mrsh-v2 es un tipo de coincidencia de aproximación. Se implementa y evalúa mediante el uso de conjuntos de datos TS y matriz de confusión. Finalmente, Mrsh-v2 tiene una puntuación alta de verdadero positivo y sensibilidad, y tiene una puntuación baja de falso negativo.

Por su parte, Lora y Montenegro (2018), en su investigación titulada “Framework de Seguridad informática para mitigar la fuga de información ocasionada por amenazas persistentes avanzadas proveniente de correo electrónico, en los activos de información del sector hospitalario en Colombia”, la cual tuvo por objetivo demostrar que el sector salud no evidencia el uso de controles adecuados en la detección y detención de las Amenazas Persistentes Avanzadas (APT); sus resultados son: permite aminorar la fuga ocasionada por APT que se propician a través del e-mail, mediante el uso de buenas prácticas al utilizar una guía para identificar los activos en donde se almacena información sensible, que sean propensos a salida, posteriormente se identificó y modeló un acumulado de amenazas para establecer el modo en que operan las APT llegadas por e-mail. Concluyen que una estrategia de Data Loss Prevention permitirá identificar y clasificar los activos sensibles susceptibles a fuga, logrando de esta manera proteger los datos confidenciales de la institución, detectando y deteniendo las amenazas persistentes avanzadas (APT) y asegurando que se practiquen las PSI.

Por otro lado, Godínez y Olvera (2017), en su tesis “Implementación de un sistema de seguridad DLP (Data Loss Prevention)” de México, la que tuvo el

propósito de hacer hincapié en la manera de reducir la pérdida de datos y ahorrar dinero al utilizar una tecnología DLP. Su alcance se centra en la información sensible a la cual se le considera sumamente importante para la organización; recomienda que, mediante políticas creadas previamente se pueble bloquear la fuga de información por cualquier medio (CD/DVD, USB, FTP, e-mail, etc.), generando un índice de seguridad de la información óptimo; concluyendo que la herramienta DLP es la mejor opción en la prevención de la fuga de datos en cualquier institución.

Para terminar, tenemos la tesis realizada por Heinert (2018) "Implementación de una solución Data Loss Prevention (DLP) en una empresa con actividades de servicios alimenticios" en la que afronta la problemática de la fuga de datos. Tuvo por objetivo la implementación de la tecnología DLP para evadir la fuga por puertos USB o terminales electrónicos u otros medios. La población fue de 30 usuarios para identificar los tipos de anomalías detectadas y la detección de problemas. Se sostiene de manera enfática que las amenazas internas generadas por los usuarios son la principal amenaza de la organización, ya que desde su inicio se produce la pérdida, mala manipulación y fuga de información, concluye refiriendo que la herramienta DLP fue la mejor opción para impedir la fuga de Información de cualquier organización, para poder establecer una estrategia que comprenda la creación de políticas y mecanismos que controlen y eviten la fuga de la información; para lo cual la tecnología DLP abarca los tres estados de la información: reposo, movimiento y uso.

En lo referido a las teorías que se tomaron en consideración como respaldo durante esta investigación, estas serán descritas a continuación. Para empezar, tenemos a la Teoría General de Sistemas, donde Domínguez y López (2019) refieren que, si utilizamos una buena herramienta que logra un beneficio y su aplicación de manera global, para ello debemos de tener en cuenta el aporte de utilizar la destreza de divide y vencerás, generando una completa seguridad de que mientras se lleve a cabo un enfoque sistémico diligentemente, tendremos la habilidad de detectar cualquier desviación oportunamente para realizar las correcciones en el momento indicado, utilizando una visión holística y globalizada del objeto en estudio. Por otra parte, Ramírez (1989) menciona que,

al referirnos de un sistema hablamos de un grupo de elementos y si existiera la falta de una de sus partes, el sistema no funciona. De tal forma, Bertoglio (1993) indica que, un sistema es la suma de sus partes y objetos comprendidos en su delimitación, que se relacionan formando un todo influenciado de fuerzas por medio de una relación definida. Asimismo, para Arnold y Osorio (1998) afirman que, es la reunión de elementos que se corresponden entre sí, que lo mantienen indirecta o directamente fusionado de manera inalterable y que su comportamiento persigue el logro de un objetivo institucional. Otro concepto válido es el de Van (2008) que lo define como un conjunto de elementos íntimamente relacionados. Así también, Arras et al. (2008), lo conceptualiza como un todo, el cual está organizado e integrado por dos o más elementos llamados subsistemas con los que relacionan e interactúan entre sí. Finalmente, tenemos a Sommerville (2011), que lo define como una compilación intencional de elementos interconectados, de disímiles características trabajando unidos para conseguir el logro de un objetivo de la alta dirección.

Aunado a esto, se planteó la teoría del control; para empezar, Tocancipa (1976) refiere que, fue inventada por el hombre, debido a que éste tiene la idea de controlar algo a través de su historia, busca la mejor manera de inquirir y percatarse de la pretensión de indagar e instaurar los medios necesarios para vigilar los procesos de distintas maneras. Esta teoría se basa en el argumento de que cada proceso se encuentra en movimiento o trabajo ocurriendo en un tiempo explícito y por medio de etapas dentro de un sistema a través de una dinámica de alta efectividad, que tiene como base una distribución ordenada que permite seguir las actividades del proceso se basan en el conocimiento del estado anterior del sistema. Por consecuencia, otro módulo de suma importancia es el objetivo, que detalla que el cumplimiento de los requisitos previos es vital para tener un correcto control. Considerando que una distribución de control ha sido planeada satisfactoriamente si todas las etapas del proceso se alcanzan. En ese sentido, Polanía (1997) muestra que, la retroalimentación es el mecanismo más importante, debido a que la aparición de los errores durante el proceso estimula mejores resultados a futuro. Existen disímiles tipologías de controles que coadyuvan a garantizar el curso de los procesos. Así también, los controles: proporcional, integral y diferencial estuvieron instaurados para garantizar

sus conocimientos, pero se diferencian en la manera de transición hacia la mejora durante su cumplimiento. Otro punto es el de Fermín (2012) refiere que, es el mecanismo a través del cual cualquier tipo de sistemas mantiene el equilibrio. En esa misma línea se encontró a Ogata (1998) mencionando que, esta teoría propone: intervenir, medir, administrar y dirigir de manera automática las definiciones estáticas y dinámicas del ejercicio de cualquier tipo de sistemas. Finalmente, Astrom (2006), instauró lo maravilloso de retroalimentar, porque es como podemos establecer un sistema que se desempeñe correctamente, pero con componentes que trabajan pobremente; logrando de esta manera hacerlo susceptible a desviaciones y a las transiciones en los elementos que compone el sistema.

Con respecto al axioma de la variable independiente Data Loss Prevention.

Para empezar, tenemos a Fritchen (2019) definiendo que, Data Loss Prevention es el acumulado de prácticas que logran evitar que la información sensible y protegida caiga en las manos equivocadas de manera voluntaria o involuntaria.

En esa misma línea OSTECH (2015) menciona que, las Data Loss Prevention se utilizan durante el monitoreo de eventos que podrían ocasionar filtración de datos; posibilitando la prevención y mitigación de vulnerabilidades cuando se hacen presentes. También tenemos a gbadvisors (2018) quien sostiene que, Data Loss Prevention es la prevención que se aplica para impedir la pérdida de datos sensibles, ya sea de manera interna (intencionada o manipulada por personal que cuenta con el acceso privilegiado) o externa (programas malignos o virus informáticos); para ello se enfoca desde la prevención y protección, control y reducción mediante herramientas especializadas.

Mejía (2015), define a Data Loss Prevention, como las tecnologías que logran identificar, supervisar y finalmente lograr la protección de los datos en movimiento y uso, mediante la investigación del contenido y el análisis del

contexto de seguridad centralizado; las DLP están perfiladas en la detección y prevención del uso no autorizado y la transmisión de los datos confidenciales o sensibles por cualquier tipo de medio.

Por su parte Sánchez (2015) indicó que, Data Loss Prevention se trata de una solución que permite a las instituciones disponer del descubrimiento, prevención y protección de su información sensible. Asimismo, López et al. (2015) definen que, Data Loss Prevention es la solución tecnológica actual para proteger una organización de fugas de datos. La tecnología Data Loss Prevention refuerza los criterios de cómo fluirá la información dentro y fuera de la red electrónica de la empresa, incluidos los ensayos de auditoría, notificaciones y acciones de respuesta. Asimismo, es una solución capaz de inspeccionar el contenido de los datos electrónicos de la organización especializándose en buscar información sensible o valiosa, que se está moviendo sin permiso a través de la empresa.

Para finalizar Torres (2015) indica que, DLP es una expresión de la seguridad informática que vislumbra a una correlación de herramientas que principalmente evitan la remisión de datos sensible fuera de la institución, describiendo a su vez a las soluciones que la detectan, monitorean y logran evitar que los datos catalogados de confidencial sean transferidos y utilizados indebidamente.

En consideración con las dimensiones encontradas para la variable independiente Data Loss Prevention, las describo a continuación:

Como la primera dimensión se tiene a: Descubrimiento. Según Dota et al. (1999), refirieron que, el descubrimiento no es término con un significado definido, pero está de acuerdo con sus usos, pero en quehacer científico, dicha prioridad estriba principalmente por la publicidad o circulación al momento de realizar comparaciones con otros fenómenos conocidos por parte del investigador. Asimismo, Serna (2017) menciona que, epistemológicamente se trata del hallazgo de información para luego realizar la justificación del conocimiento sistematizándolo, para su posterior uso técnico, tanto para el

resultado final de una investigación como para el descubrimiento de dicho resultado. Por otro lado, Martínez (2020) refiere que, se trata del hallazgo de algo oculto y que era antes desconocido. La Real Academia Española - RAE (2019) mencionó que, se trata del conocimiento de algo oculto o que era desconocido. Según Diccionario Reverso (2018), se refiere al hallazgo de algo desconocido. Pérez y Merino (2021), lo definió como un hallazgo que antes era oculto, secreto o desconocido.

Por otro lado, como segunda dimensión tenemos la prevención. Empezando con Bunga y Rahadiyan (2020), quienes manifiestan que, ésta principalmente reside en representar los tipos de control, a través de crear las capacidades en las operaciones y en las instituciones, tecnologías de control e inclusión activa de los colaboradores. Para el Gran Diccionario de la Lengua Española (2016), es la acción que se realiza para evitar un riesgo. Según el Diccionario de la lengua española (2020), la considera como la preparación, provisión y disposición anticipada para evitar un riesgo. Asimismo, Pérez y Gardey (2021) refieren que, es la preparación anticipada a un posible daño. Finalmente, Lv Xuming et al. (2019) mencionaron que, la prevención requiere una consideración integral de los requisitos de protección en todos los niveles y el esquema de prevención de fugas de datos de terminales que se realizó a través del control de dispositivos y puertos. Aunque este método puede bloquear eficazmente la fuga de datos, también reduce la disponibilidad del sistema, porque la comunicación entre dominios es esencial para muchas aplicaciones.

Por último, como tercera dimensión se tiene la Protección. Empezamos con ICO.ORG Information Commissioner's Office (2018) quien sostuvo que, la protección es el uso justo y adecuado de la información sobre las personas. Es parte del derecho fundamental a la privacidad, pero en un nivel más práctico, realmente se trata de generar confianza entre las personas y las organizaciones. Se trata de tratar a las personas de manera justa y abierta, reconocer su derecho a tener control sobre su propia identidad y sus interacciones con los demás, y lograr un equilibrio con los intereses más amplios de la sociedad. Asimismo, refiere que la protección de datos es fundamental para la innovación. Las buenas prácticas son valiosas para avalar la confianza de la institución por parte del

público, el compromiso y el apoyo a los usos innovadores de los datos en las instituciones públicas y privadas.

Para Tamburri (2020) manifiesta que, es una regulación de un conjunto de reglas para restringir o regular el procesamiento de datos pertenecientes a una o más personas con el fin de determinar nuevos conocimientos para un propósito específico. Según Antony et al. (2017) mencionaron que, especifica la necesidad e idoneidad del procesamiento de datos y describe todas las medidas que contribuyen a la eficacia protección de los derechos personales.

Storage Networking Industry Association – SNIA (2021) refiere que, la protección se encarga de la salvaguarda de los datos sensibles a manipulación o pérdida y provee la capacidad de restauración de ellos a un estado anterior, permitiendo la funcionalidad ante la ocurrencia algún incidente que los convierta en inutilizables o inaccesibles; a su vez, se debe de garantizar que no se dañen, solo usados para los fines provistos con confidencialidad, con cumplimiento de las normas o disposiciones legales. Los datos que se protegen deben tener la disponibilidad correspondiente de ser requeridos y serán utilizados bajo su propósito conocido.

Finalmente, Emotiv (2021) menciona que, la protección es un subconjunto de la privacidad. Esto se debe a que proteger los datos del usuario y la información confidencial es un primer paso para mantener la privacidad de los datos del usuario.

De otra parte, en lo que se refiere pertinentemente al axioma de la variable dependiente Prevención de Fuga de Datos, las describo a continuación:

Según Kelsey (2002) menciona que, es la evasión no examinada de información que llega a manos equivocadas, así como la pérdida de su resguardo; a su vez refiere que la fuga se presenta cuando un sistema presenta brechas en su seguridad o integridad, permitiendo a los agresores la interceptación de los datos.

Por su parte Patrizio y Kranz (2021) refiere que, es una estrategia para impedir que los clientes o usuarios accedan a datos sensibles que no necesitan, garantizando que el personal no la envíe fuera de la red de la institución de manera accidental o maliciosamente por una infiltración, principalmente de hackers informáticos, mientras están en uso (acciones de terminales), en movimiento (tráfico de red) y en reposo (almacenamiento de datos).

En esa misma línea tenemos a Fearn y Tuner (2021) mencionan que, proporciona una forma eficaz de evitar la pérdida de datos a través de almacenamiento no seguro o mediante exfiltración maliciosa por parte de terceros. Según García et al. (2017) sostienen que, la prevención de fuga de datos es útil porque ayuda a mantener segura la información sensible; de esta manera evitaremos filtraciones.

Tujab (2017) manifiesta que, se trata de toda aquella gestión enfocada en evitar cualquier riesgo que vulnere la confiabilidad, integridad y disponibilidad. Al ocurrir una fuga, se genera un impacto y consecuencias negativas, que es la que mayor preocupación despierta en las instituciones, pues la filtración de información daña su imagen y además genera desconfianza e inseguridad, sobre todo si la información filtrada pone en riesgo a los usuarios o clientes de la institución.

Como acápite Torres (2015) manifiesta que, ayuda para detectar y prevenir en tiempo real una posible fuga que se pueda originar, ya sea de manera no intencional o con algún objetivo específico. Así también, permite instruir y comunicar a los usuarios sobre la forma más adecuada del tratamiento de la información confidencial, obteniéndose un progreso sustancial al inferir la Seguridad de la Información en toda empresa. Esta prevención utiliza unas herramientas desarrolladas especialmente para impedir el envío de datos sensibles fuera del ambiente institucional; adicionalmente, detalla a las soluciones que encargan de la detección, monitoreo y evitan que los datos confidenciales sean utilizados indebidamente fuera de las instituciones. Finalmente, Rayami (2020) refiere que, debemos estar enfocados en el resguardo y gobernanza de datos es sumamente crítica, no sólo para cumplir con la normativa vigente y la

privacidad; asimismo mitiga la fuga de datos confidenciales y el riesgo que se acarrea. Asimismo, provee la atención de políticas basadas en el análisis situacional de los datos en los estados de: reposo, uso y movimiento, para los datos almacenados on premise como cloud.

En correlación a las dimensiones encontradas para la variable dependiente, éstas se relatan seguidamente:

Para la primera, se expone a: Previene datos en uso. Empezamos con Fitzgibbons (2019) lo conceptualizó como los datos que se están actualizando, procesando, borrando, accediendo o leyendo en un sistema. Este tipo de datos no se almacenan pasivamente, sino que se mueven activamente a través de partes de una infraestructura de TI. Asimismo, menciona que, a través del cifrado, autenticación del usuario, gestión de la identidad y permisos bien mantenidos dentro de la institución para protegerlos. Tenemos también a Froehlich (2020) que para proteger los datos en uso es necesario proporcionar una visibilidad adecuada para la detección de infracciones. Asimismo, menciona que a mejor manera de proteger los datos en uso es restringir el acceso por función de usuario, limitando el acceso al sistema solo a aquellos que lo necesitan. Aún mejor sería ser más granular y restringir el acceso a los datos en sí.

De eso se desprende, como segunda dimensión se tiene a previene datos en movimiento. Para iniciar con su definición tenemos a Allen (2016) que nos dice que los datos en movimiento se encuentran en su punto más vulnerable y es donde se deben centrar la atención de la protección porque es donde lidiamos con errores humanos, fallas en la red, intercambio de archivos inseguro, acciones maliciosas entre otras. También tenemos a Neha y Rashmi (2018), quienes lo definen como los datos que están en comunicación o que se intercambian durante una comunicación. Para Froehlich (2020), para prevenir los datos en movimiento, se debe proporcionar una visibilidad adecuada para la detección de infracciones. Los avances en las herramientas de seguridad de inteligencia artificial que ingieren datos de telemetría de red y luego los analizan para detectar anomalías en el comportamiento de acceso a los datos pueden identificar amenazas, determinar el alcance del daño y proporcionar información

procesable sobre cómo detener una mayor pérdida de datos. Las herramientas modernas de análisis de seguridad e inteligencia artificial, como la detección y respuesta de redes y la inteligencia artificial para las plataformas de operaciones de TI, son excelentes formas de obtener el nivel adecuado de visibilidad sin requerir una gran cantidad de tiempo desde una perspectiva administrativa.

Finalmente, como tercera dimensión se tiene a previene datos en reposo. Según Neha y Rashmi (2018) sostienen que, son los datos que se han vaciado de la memoria y se han escrito en el disco. Para Mantis Net (2021), son los datos inactivos que se almacenan físicamente en cualquier forma digital. Finalmente, Froehlich (2020) menciona que, para proteger mejor los datos en reposo, las organizaciones deben saber dónde residen todos los datos confidenciales y cómo clasificarlos. Las empresas necesitan procesos para limitar las ubicaciones donde se almacenan los datos confidenciales, pero eso no puede suceder si no pueden identificar adecuadamente la naturaleza crítica de sus datos. Asimismo, refiere que, los datos en reposo son tan seguros como la infraestructura que los respalda. Monitorear continuamente las amenazas internas y externas que intentan acceder a los datos en reposo es otra excelente manera de vigilar la infraestructura y proporcionar una visibilidad adecuada para la detección de infracciones.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

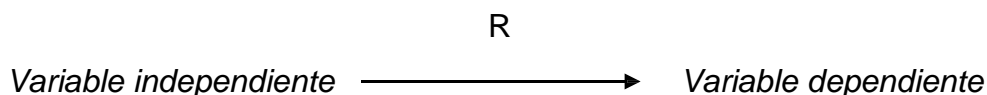
3.1.1 Tipo de investigación

En cuanto al tipo de investigación de la investigación, fue **básica** (Concytec 2018), con un enfoque cuantitativo. quienes afirmaron que, es aquella investigación científica que cumple el propósito de promover conocimiento y presunciones.

3.1.2 Diseño de investigación

Por otra parte, el diseño de investigación fue el **no experimental**. Según analiza Hernández y Mendoza (2018), es aquella en la cual no se modifican de forma premeditada las variables independientes. Ahondando en el diseño, se clasifica como una publicación **transversal** denominado transaccional porque esgrime una recolección de datos en un determinado momento, periodo o lugar específicos de nivel **correlacional-causal**, ya que se puede limitar a dos variables: independiente y dependiente.

Esquema:



Del esquema anterior, se infiere que la variable independiente Data Loss Prevention se relaciona de manera correlacional causal con la variable dependiente prevención de fuga de datos.

3.2. Variables y operacionalización

Según Hernández y Mendoza (2018) refieren que, al utilizar este enfoque estudiaremos los fenómenos de manera sistémica proporcionando profundidad a los datos, a través del cual el investigador examina los hechos y revisa las investigaciones previas simultáneamente, para crear una teoría consistente con lo realidad problemática observada.

Durante el desarrollo de la tesis, la variable independiente tiene como premisa a Data Loss Prevention, y previene datos en uso, movimiento y reposo como parte de la variable dependiente prevención de fuga de datos que se aplicará para el descubrimiento, prevención y protección de la información que es trabajada por los servidores públicos en el gobierno regional.

Variable independiente: Data Loss Prevention

La variable independiente Data Loss Prevention es del Tipo Cuantitativa, según la idea subjetiva del investigador; utilizando en la medición la escala de Likert no forzada de cinco puntos, mediante la valoración del cuestionario desarrollado para tal fin, en el cual se logró identificar sus tres dimensiones y sus indicadores por cada dimensión.

La **definición conceptual** de Data Loss Prevention según refiere Sánchez (2015) indica que Data Loss Prevention se trata de una solución que permite a las instituciones disponer del descubrimiento, prevención y protección de su información sensible.

Para la **definición operacional** de Data Loss Prevention, se logró identificar las dimensiones descubrimiento, prevención y protección provenientes de la definición conceptual de la variable independiente Data Loss Prevention, la cual fue utilizada como punto de partida para racionalizar y llegar a inferir los indicadores que se identificaron por cada una de las tres dimensiones: (1) para descubrimiento (identificación, clasificación y trazabilidad); (2) para prevención (capacitación, supervisión y control de acceso); y (3), para protección (monitoreo, control de los repositorios y confiabilidad). Posteriormente, redacté dos preguntas por cada uno de los indicadores encontrados y para su mejor entendimiento por los servidores públicos del gobierno regional, que se tuvo a bien utilizar un cuestionario con dieciocho ítems (1-18) utilizando la escala de Likert no forzada de 5 puntos. Paso seguido, se construyeron los niveles no óptimo, medio y óptimo para el resultado. Para finalizar, se infirieron los rangos para cada nivel: (1) para no óptimo (18-42); (2) para medio (43-67); y (3) para óptimo (68-90). Cabe mencionar, que las dimensiones, indicadores y ítems del cuestionario elaborado por el investigador en la tesis para la variable

independiente Data Loss Prevention fueron validados con la calificación de suficiencia, por el juicio de tres expertos, los cuales se mencionan más adelante a través de la Tabla 6. Para ello, se elaboró la matriz de operacionalización de la variable independiente en Tabla 1, la cual se muestra a continuación.

Tabla 1

Matriz de operacionalización de la variable independiente: Data Loss Prevention.

Dimensiones	Indicadores	Ítems	Escala de Valores	Niveles	Rangos
Descubrimiento	Identificación	1-2			
	Clasificación	3-4			
	Trazabilidad	5-6	1) Totalmente en desacuerdo	No óptimo	18-42
Prevención	Capacitación	7-8			
	Supervisión	9-10	2) En desacuerdo		
	Control de acceso	11-12	3) Ni de acuerdo ni en desacuerdo	Medio	43-67
Protección	Monitoreo	13-14	4) De acuerdo	Óptimo	68-90
	Control de los repositorios	15-16	5) Totalmente de acuerdo		
	Confiabilidad	17-18			

Los **indicadores** que se infieren para la dimensión descubrimiento son identificación, clasificación y trazabilidad; para prevención son capacitación, supervisión y control de acceso; y protección son monitoreo, control de los repositorios y confiabilidad. Todos ellos fueron necesarios para la aplicación de la tecnología Data Loss Prevention en el gobierno regional.

La **escala de medición** utilizada para el desarrollo de la tesis fue la de Likert no forzada de 5 puntos, tanto para las dimensiones e indicadores: descubrimiento (identificación, clasificación, trazabilidad), prevención (capacitación, supervisión, control de acceso) y protección (monitoreo, control de los repositorios, confiabilidad) de la variable independiente.

Variable dependiente: Prevención de fuga de datos

La variable dependiente prevención de fuga de datos es del Tipo Cuantitativo, según la idea subjetiva del investigador; utilizándose la escala de Likert no forzada de cinco puntos, mediante la valoración del cuestionario desarrollado

para tal fin en el cual se logró identificar sus tres dimensiones y sus respectivos tres indicadores por dimensión.

La **definición conceptual** de prevención de fuga de datos, según Patrizio y Kranz (2021) refirieron que, es una estrategia para impedir que los clientes o usuarios accedan a datos sensibles que no necesitan, garantizando que el personal no la envíe fuera de la red de la institución de manera accidental o maliciosamente por una infiltración, principalmente de hackers informáticos.

Para la **definición operacional** de prevención de fuga de datos, se logró identificar las dimensiones previene datos en uso, previene datos en movimiento y previene datos en reposo provenientes de la definición conceptual de la variable dependiente prevención de fuga de datos, la cual fue utilizada como punto de partida para racionalizar y llegar a inferir los indicadores que se identificaron por cada una de las tres dimensiones: (1) para previene datos en uso (monitoreo de actividades, evaluar almacenamiento y detección de fuga); (2) para previene datos en movimiento (análisis de tráfico de red, monitoreo de violaciones y salida de datos no autorizada); y (3), para previene datos en reposo (monitoreo de los activos, retención y cifrado de datos). Posteriormente, redacté dos preguntas por cada uno de los indicadores encontrados y para su mejor entendimiento por los servidores públicos del gobierno regional, que se tuvo a bien utilizar un cuestionario con dieciocho ítems (19-26 utilizando la escala de Likert no forzada de 5 puntos. Paso seguido, se construyeron los niveles malo, regular y bueno para el resultado. Para finalizar, se infirieron los rangos para cada nivel: (1) para malo (18-42); (2) para regular (43-67); y (3) para bueno (68-90). Cabe mencionar, que las dimensiones, indicadores y ítems del cuestionario elaborado por el investigador en la tesis para la variable dependiente prevención de fuga de datos fueron validados con la calificación de suficiencia, por el juicio de tres expertos, los cuales se mencionan más adelante a través de la Tabla 6. Para ello, se elaboró la matriz de operacionalización de la variable independiente en Tabla 2, la cual se muestra a continuación.

Tabla 2

Matriz de operacionalización de la variable dependiente: Prevención de fuga de datos.

Dimensiones	Indicadores	Ítems	Escala de Valores	Niveles	Rangos
	Monitoreo de actividades	19-20			
Previene datos en uso	Evaluar almacenamiento	21-22			
	Detección de fuga	23-24	1) Totalmente en desacuerdo	Malo	18-42
Previene datos en movimiento	Análisis de tráfico de la red	25-26	2) En desacuerdo	Regular	43-67
	Monitoreo de violaciones	27-28	3) Ni de acuerdo ni en desacuerdo		
	Salida de datos no autorizada	29-30	4) De acuerdo	Bueno	68-90
Previene datos en reposo	Monitoreo de los activos	31-32	5) Totalmente de acuerdo		
	Retención	33-34			
	Cifrado de datos	35-36			

Los **indicadores** que se infieren para previene datos en uso son monitoreo de actividades, evaluar almacenamiento y detección de fuga; para previene datos en movimiento son análisis de tráfico de la red, monitoreo de violaciones y salida de datos no autorizada; y para previene datos en reposo son monitoreo de los activos, retención y cifrado de datos. Todos ellos fueron necesarios para la aplicación de la prevención de fuga de datos en el gobierno regional.

La **escala de medición** utilizada para el desarrollo de la tesis fue la de Likert no forzada de 5 puntos, tanto para las dimensiones e indicadores: previene datos en uso (monitoreo de actividades, evaluar almacenamiento, detección de fuga), previene datos en movimiento (análisis de tráfico de la red, monitoreo de violaciones, salida de datos no autorizada) y previene datos en reposo (monitoreo de los activos, retención, cifrado de datos) de la variable dependiente.

3.3. Población, muestra y muestreo

3.3.1 Población

Según Hernández y Mendoza (2018), es la reunión de las cuestiones de acorde con una sarta de relaciones planteadas por el investigador para delimitar su desarrollo en el proyecto. De esta manera, para la elaboración de la investigación a desarrollar se consideró a la población constituida por 65 colaboradores del gobierno regional. Los que se definen en la Tabla 3.

Tabla 3

Caracterización de la población.

Población	Cantidad
Gerentes y subgerentes	4
Administrador	1
Servidores públicos	60
Total	65

Criterios de inclusión

Las características de inclusión como parte de la población fueron: los servidores públicos, a los que se les asignaron y hacen uso de los equipos informáticos de la institución y, que cuentan con acceso a la red, al correo electrónico y a las carpetas compartidas que laboran durante su turno asignado de lunes a viernes, de manera presencial, virtual o mixta.

Criterios de exclusión

Las condiciones de exclusión como parte de la población fueron: los servidores públicos que no se les asignaron y no hacen uso de los equipos informáticos de la institución, y, que no cuentan con acceso a la red, al correo electrónico y a las carpetas compartidas que laboran durante su turno asignado de manera presencial de lunes a viernes (tales como los choferes, personal de vacaciones o que por tener una enfermedad persistente, tienen licencia con goce de haber por ser personas vulnerables o de alto riesgo de infección por la enfermedad COVID-19).

3.3.2 Muestra

Según Hernández y Mendoza (2018) indicaron que, depende de cómo comprendemos el fenómeno en investigación, se determina tomando en

consideración al contexto y necesidades para la evolución de uno o más propósitos del proceso inductivo. Por consiguiente, para efectuar el cómputo de la muestra se trajo a consideración el aplicativo Decision Analyst STATS v. 2.0.0.2, considerándose lo siguiente: población, 65 servidores públicos; un máximo de error aceptable, 5%; porcentaje estimado, 50%; y, nivel de confianza deseado, 95%. Es así como, se realizó el ingreso de los parámetros anteriormente mencionados, dando como resultado de la muestra 56 servidores públicos. Por consiguiente, el detalle de la muestra se define en la Tabla 4.

Tabla 4

Caracterización de la muestra.

Muestra	Cantidad
Gerentes y subgerentes	2
Administrador	1
Servidores públicos	53
Total	56

3.3.3 Muestreo

Se optó por un muestreo no probabilístico, en referencia con Hernández y Mendoza (2018) indican que, se trata de seleccionar casos por uno o varios motivos dirigidos para el cumplimiento del propósito del desarrollo de la tesis.

3.4. Técnicas e instrumentos de recolección de datos

En cuanto a la **técnica de recolección de datos** fue la encuesta. Según Hernández y Mendoza (2018) indican que, son los instrumentos que nos permiten afinar y uniformizar la investigación paulatinamente.

Con respecto al **instrumento de recolección de datos** fue el cuestionario. Para González et al. (2017) infieren que, nos sirve de guía y señala al investigador la manera de cómo se deben interpretar los datos recolectados; a su vez, permite pasar de los conocimientos abstractos hacia los indicadores empíricos por medio de la operacionalización de la variable y que esta etapa sea fácil para su observación en la institución. La escala de Likert se utilizó para

valorar la estimación, debido a que nos permitió nivelar las opiniones recogidas. De esta manera, las tipologías del instrumento se definen en la Tabla 5.

Tabla 5

Ficha Técnica del instrumento de medición.

Nombre del Instrumento			Cuestionario para los colaboradores del gobierno regional		
Autor			Olivares Zevallos Jorge William		
Año			2022		
Tipo de Instrumento			Cuestionario		
Objetivo			Determinar la incidencia de Data Loss Prevention en la prevención de fuga de datos en un gobierno regional, Lima 2022		
Población			Gerentes y subgerentes, Administrador y Servidores públicos		
Número de Ítems			36		
Aplicación			En línea		
Tiempo de administración			5 a 7 minutos		
Normas de aplicación			El servidor público debe seleccionar una de las opciones que a su parecer sea la correcta por cada ítem, dependiendo de su apreciación y según su propia opinión.		
Escala			Likert no forzada de 5 puntos		
Descripción			Valor		
Totalmente en desacuerdo			1		
En desacuerdo			2		
Ni de acuerdo ni en desacuerdo			3		
De acuerdo			4		
Totalmente de acuerdo			5		
Niveles de rango:					
Variable: Data Loss Prevention			Variable: Prevención de Fuga de Datos		
Nivel	Valor	Rango	Nivel	Valor	Rango
No óptimo	1	18-42	Malo	1	18-42
Medio	2	43-67	Regular	2	43-67
Óptimo	3	68-90	Bueno	3	68-90

Validez

El grado de validez de esta investigación se fundamenta y alcanza su plena concepción al alcanzar la pertinencia, relevancia y claridad del cuestionario por cada ítem. En ese sentido, se definió a bien usar el método de juicio de expertos en esta investigación con el fin de salvaguardar la correcta validez del instrumento en cuestión. En relación con esto último señalado, Hernández et al. (2018) señalan que, provee que la herramienta tenga la capacidad necesaria para llevar a cabo la métrica de la característica vinculante de la investigación.

Para contar con la validez respectiva, se contó con la validación acertada del juicio de los tres expertos que se definen en la Tabla 6.

Tabla 6

Validación del instrumento de recolección de datos.

DNI	Grado académico, apellidos y nombres	Institución donde labora	Calificación
09468263	Mag. Ramírez Pacheco, Luis Enrique	Universidad César Vallejo	Suficiencia
17930425	Mag. Tejada Ruiz, Roberto Juan	Universidad César Vallejo	Suficiencia
10251980	Mag. Matos Guerrero, César David	SUNAT	Suficiencia

Confiabilidad

Según Ñaupas et al. (2018) se entiende por confiabilidad a la no variación significativa de resultados provenientes de la aplicación del instrumento indicado en circunstancias de semejanza o de isomorfismos en la naturaleza propia en donde se desarrolla la investigación. En ese sentido, se utilizó el programa informático IBM SPSS Statistics 25 para validar la fiabilidad del Alfa de Cronbach de la recolección de los datos, según Hernández y Mendoza (2018), utilizado para garantizar la confiabilidad de los resultados logrados al aplicar el instrumento cuestionario, siempre y cuando el referido estadístico esté muy cerca de la unidad. Finalmente, se consideró a la muestra alcanzando el 0.994 de fiabilidad Alfa de Cronbach, un resultado confiable. Ñaupas et al. (2018) señalan que, el resultado obtenido de la fiabilidad del Alfa de Cronbach oscila de 0 a 1, y se consideran el nivel nulo con 0% de confiabilidad y perfecta con el 100% de confiabilidad. Con lo cual se demostró que esta cifra obtenida satisface la consistencia descrita líneas arriba, para afianzar el resultado obtenido de la recolección de datos a través del análisis que se define en la Tabla 7.

Tabla 7

Resultado del análisis de confiabilidad a través del Alfa de Cronbach.

Tipo de Aplicación	N° de encuestas	N° de ítems	Alfa de Cronbach
General	56	36	0.994

Nota: Se detalla la cifra obtenida de la fiabilidad del Alfa de Cronbach después de la recolección de datos.

3.5. Procedimientos

En este proyecto de investigación primero se manejó la ejecución del cuestionario que constó de 36 ítems a la población que se considera como

muestra representativa a juicio del investigador a la población del gobierno regional, continuamos con la validación del instrumento por 3 expertos para obtener el nivel de suficiencia y conseguir datos suficientemente confiables en la investigación. Para seguido, se trasladan los 36 ítems de los datos recolectados del cuestionario que se realizó a muestra, utilizando el Microsoft Excel y como parte final, se procesaron estos datos utilizando IBM SPSS Statistics 25, obteniéndose derivaciones inferenciales esgrimidas como acápite de esta tesis.

3.6. Método de análisis de datos

En relación con el método de análisis de datos, fue el IBM SPSS Statistics 25, durante la investigación de los datos recolectados mediante el cuestionario para los usuarios del gobierno regional realizado a través del Microsoft Forms mediante el enlace: <https://forms.office.com/r/xNEC7EsfU>, por medio del método de regresión, para la variable independiente y dependiente, considerando las encuestas realizadas a la población objetivo del gobierno regional. Esta investigación y análisis recopilatorio nos permitirá demostrar la correlación de Data Loss Prevention sobre la prevención de fuga de datos. En tal sentido, durante el estudio descriptivo se empleará el Alfa de Cronbach para cada uno de los 36 ítems, previa transferencia inicial al MS Excel para poder realizar la interpretación de resultados obtenidos para validar la fiabilidad estadística en el IBM SPSS Statistics 25 del instrumento utilizado. Para el estudio inferencial, se tuvo en cuenta el procedimiento no paramétrico para confirmar que las hipótesis planteadas son verificables y repetibles, para establecer la relación causal que existe entre la variable Data Loss Prevention y la variable prevención de fuga de datos.

3.7. Aspectos éticos

Conviene subrayar, que la investigación de esta tesis es integra, porque se desempeñó de manera honesta con las normas éticas establecidas por la Universidad César Vallejo, según la Resolución de Consejo Universitario N°0262-2020/UCV, que sustenta la limpieza y autenticidad con la que se realizó esta investigación científica.

Se tuvo a bien, considerar a la Ley sobre el Derecho de Autor, respetando la posesión del autor en las investigaciones científicas que se citaron y referenciaron en la tesis. Finalmente, se consideró también la Ley de Protección de Datos Personales, que impide compilar información personal a través de cualquier medio engañoso, desleal o ilícito; debido a ello, durante el desarrollo de esta investigación se recogió la información con sumo respeto considerando el correcto anonimato y la anuencia informada de los servidores públicos contemplados como población objetivo del gobierno regional.

IV. RESULTADOS

4.1 Análisis descriptivos

En referencia a la edad: la mínima fue 20 y la máxima 67, la frecuencia de mayor recuento fue la de 31 a 40 años, que equivalió al 41.1% del total; en referencia al sexo de la muestra: el masculino fue el de mayor porcentaje, equivalió al 55.4%, mientras que el femenino al 44.6% restante; en referencia a la ocupación: Tercero se situó en el primer lugar con 50.0%, seguido del CAS con 37.5%, siendo los más representativos; en referencia al grado de estudio: Posgrado se situó en el primer lugar con el 48.2%, seguido del superior universitaria con el 39.3%, siendo los más representativos; en referencia a gerencia o subgerencia: la principal fue contratos con un 44.6%, seguido de operaciones con un 30.4%, siendo los más representativos. Los resultados obtenidos se definen en la Tabla 8.

Tabla 8

Caracterización de la recolección de datos a través del cuestionario

Dato recolectado		Recuento	% de N tablas
Edad	de 20 a 30	11	19,6%
	de 31 a 40	23	41,1%
	de 41 a 50	14	25,0%
	de 51 a 60	6	10,7%
	de 61 a 67	2	3,6%
Sexo	Femenino	25	44,6%
	Masculino	31	55,4%
Ocupación	CAS	21	37,5%
	F3	2	3,6%
	Nombrado	1	1,8%
	SP	4	7,1%
	Tercero	28	50,0%
Grado de estudio	Posgrado	27	48,2%
	Secundaria	1	1,8%
	Superior Técnica	6	10,7%
	Superior Universitaria	22	39,3%
Gerencia o Subgerencia	Contratos	25	44,6%
	Gerencia	4	7,1%
	Operaciones	17	30,4%
	Promociones	10	17,9%

Análisis descriptivo de la variable Data Loss Prevention y la variable prevención de fuga de datos

Tabla 9

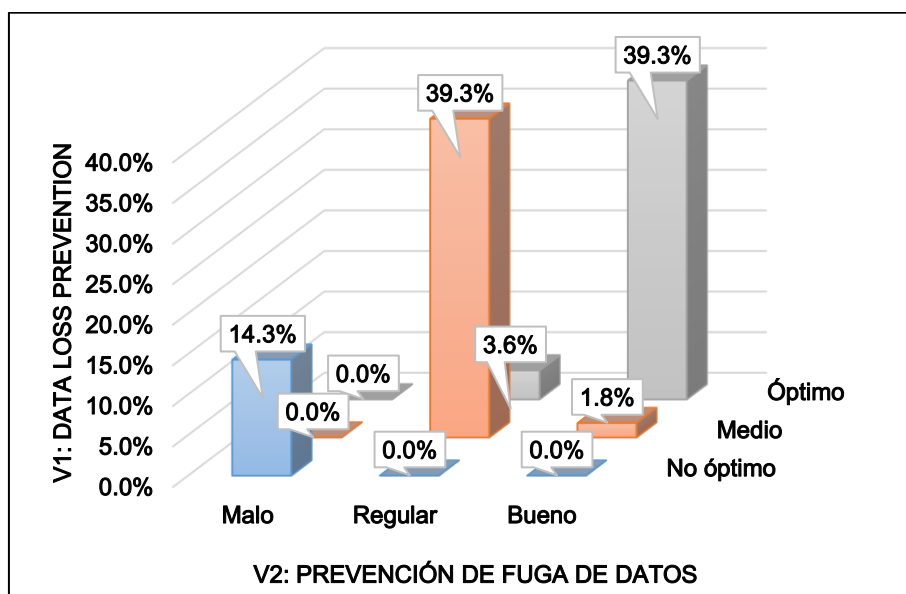
Tabla cruzada V1: Data Loss Prevention * V2: Prevención de fuga de datos.

		V2: Prevención de fuga de datos			
		Malo	Regular	Bueno	Total
V1: Data Loss Prevention	No óptimo	8 (14.3%)	0 (0.0%)	0 (0.0%)	8 (14.3%)
	Medio	0 (0.0%)	22 (39.3%)	1 (1.8%)	24 (42.9%)
	Óptimo	0 (0.0%)	2 (3.6%)	22 (39.3%)	24 (42.9%)
	Total	8 (14.3%)	24 (42.9%)	23 (41.1%)	56 (100.0%)

Nota: Elaborado por el investigador, tomando el resultado obtenido del cruce de las variables V1 y V2, a través del análisis factorial procesado en el IBM SPSS Statistics 25.

Figura 1

Histograma, V1: Data Loss Prevention * V2: Prevención de fuga de datos



A través de la tabla 9 y figura 1 de manera gráfica, se comprobó que las mayores frecuencias de aprobación se presentaron en el encuentro de los niveles: regular para la variable dependiente prevención de fuga de datos, con el nivel medio de la variable Data Loss Prevention; y bueno para la variable prevención de fuga de datos, con el nivel óptimo para la variable independiente. En ambos casos, se tuvo un total de 22 encuestados que equivalen al 39.3% de la muestra.

Análisis descriptivo de la variable Data Loss Prevention y la dimensión Previene datos en uso de la variable Prevención de fuga de datos

Tabla 10

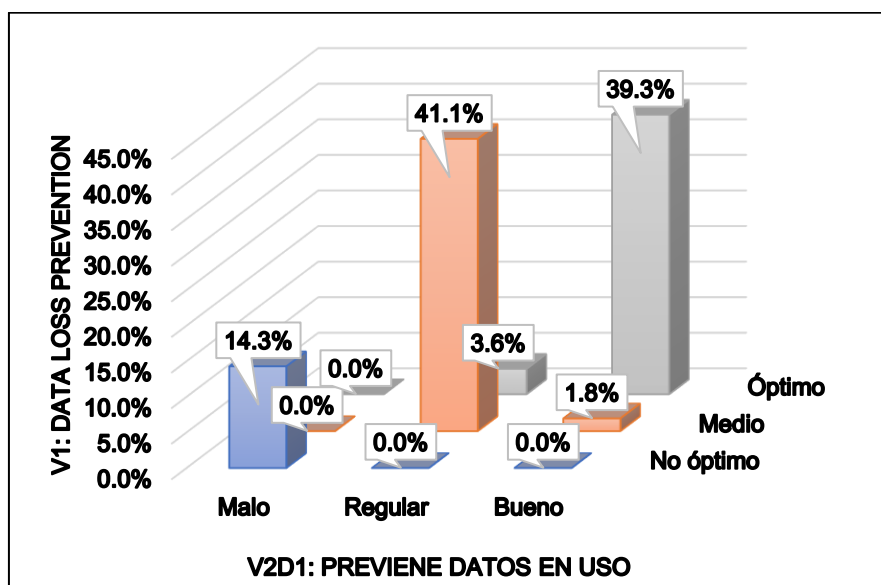
*Tabla cruzada V1: Data Loss Prevention * V2-D1: Previene datos en uso.*

		V2-D1: Previene datos en uso			
		Malo	Regular	Bueno	Total
V1: Data Loss Prevention	No óptimo	8 (14.3%)	0 (0.0%)	0 (0.0%)	8 (14.3%)
	Medio	0 (0.0%)	23 (41.1%)	1 (1.8%)	24 (42.9%)
	Óptimo	0 (0.0%)	2 (3.6%)	22 (39.3%)	24 (42.9%)
	Total	8 (14.3%)	25 (44.6%)	23 (41.1%)	56 (100.0%)

Nota: Elaborada por el investigador, tomando el resultado obtenido del cruce de las variables V1 y V2-D1: previene datos en uso, a través del análisis factorial procesado en el IBM SPSS Statistics 25.

Figura 2

*Histograma, V1: Data Loss Prevention * V2-D1: Previene datos en uso*



A través de tabla 10 y figura 2 de manera gráfica, se comprobó que la frecuencia de mayor aprobación se presentó en el encuentro del nivel regular para la dimensión previene datos en uso de la variable prevención de fuga de datos, con el nivel medio para la variable Data Loss Prevention. En este caso, se tuvo un total de 23 encuestados que equivalen al 41.1% de la muestra.

Análisis descriptivo de la variable Data Loss Prevention y la dimensión Previene datos en movimiento de la variable Prevención de fuga de datos

Tabla 11

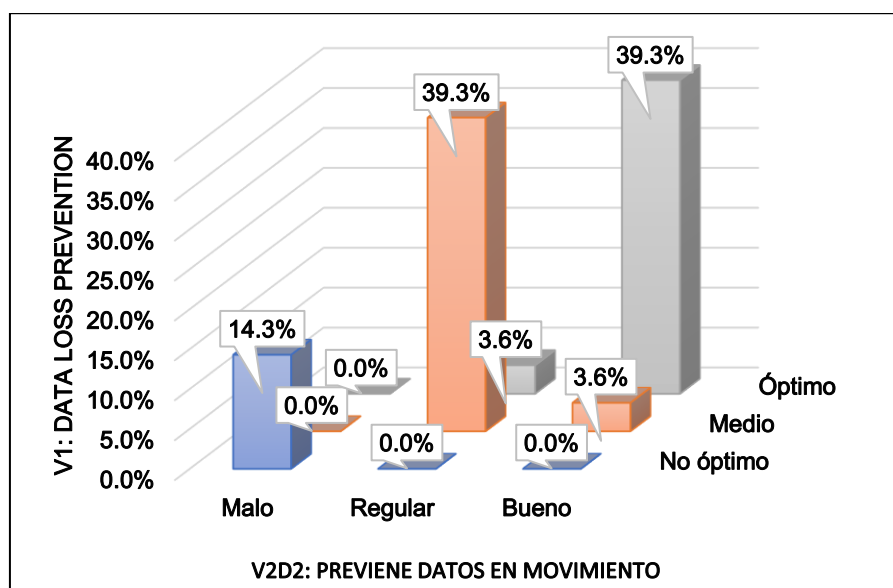
*Tabla cruzada V1: Data Loss Prevention * V2-D2: Previene datos en movimiento.*

		V2-D2: Previene datos en movimiento			
		Malo	Regular	Bueno	Total
V1: Data Loss Prevention	No óptimo	8 (14.3%)	0 (0.0%)	0 (0.0%)	8 (14.3%)
	Medio	0 (0.0%)	22 (39.3%)	2 (3.6%)	24 (42.9%)
	Óptimo	0 (0.0%)	2 (3.6%)	22 (39.3%)	24 (42.9%)
	Total	8 (14.3%)	24 (42.9%)	24 (42.9%)	56 (100.0%)

Nota: Elaborado por el investigador, tomando el resultado obtenido del cruce de las variables V1 y V2-D2: previene datos en movimiento, a través del análisis factorial procesado en el IBM SPSS Statistics 25.

Figura 3

*Histograma, V1: Data Loss Prevention * V2-D2: Previene datos en movimiento*



A través de la información de la tabla 11 y figura 3 de manera gráfica, se comprobó que las mayores frecuencias de aprobación se presentaron en el encuentro de los niveles regular para la dimensión previene datos en movimiento de la variable prevención de fuga de datos, con el nivel medio para la variable Data Loss Prevention; y bueno de la dimensión previene datos en movimiento para la variable dependiente prevención de fuga de datos, con el nivel óptimo

para la variable Data Loss Prevention. En ambos casos, se tuvo un total de 22 encuestados que equivalen al 39.3% de la muestra.

Análisis descriptivo de la variable Data Loss Prevention y la dimensión Previene datos en reposo de la variable Prevención de fuga de datos

Tabla 12

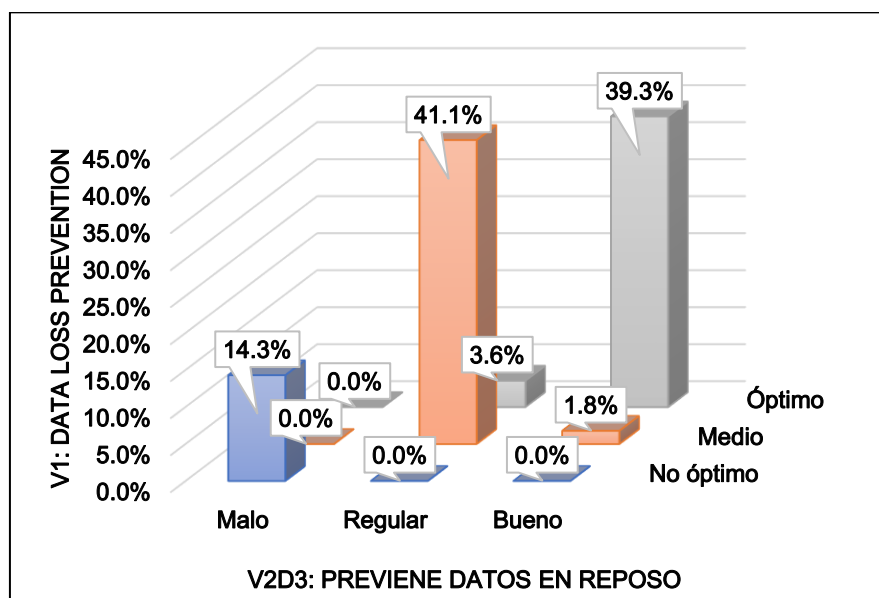
*Tabla cruzada V1: Data Loss Prevention * V2-D3: Previene datos en reposo.*

		V2-D3: Previene datos en reposo			
		Malo	Regular	Bueno	Total
V1: Data Loss Prevention	No óptimo	8 (14.3%)	0 (0.0%)	0 (0.0%)	8 (14.3%)
	Medio	0 (0.0%)	22 (39.3%)	1 (1.8%)	24 (42.9%)
	Óptimo	0 (0.0%)	2 (3.6%)	22 (39.3%)	24 (42.9%)
	Total	8 (14.3%)	24 (42.9%)	23 (41.1%)	56 (100.0%)

Nota: Elaborado por el investigador, tomando el resultado obtenido del cruce de las variables V1 y V2-D3: previene datos en movimiento, a través del análisis factorial procesado en el IBM SPSS Statistics 25.

Figura 4

*Histograma, V1: Data Loss Prevention * V2-D3: Previene datos en reposo*



A través de la información de la tabla 12 y figura 4 de manera gráfica, se comprobó que la frecuencia de mayor aprobación se presentó en el encuentro del nivel regular intersección de los niveles regular para la dimensión previene datos en reposo de la variable Prevención de fuga de datos, con el nivel medio

para la variable Data Loss Prevention. En este caso, se tuvo un total de 23 encuestados que equivalen al 41.1% de la muestra.

4.2 Prueba de normalidad

Conviene subrayar, que la muestra que se consideró para el desarrollo de esta tesis fue de 56 colaboradores del gobierno regional, por lo cual, se utilizó la prueba de normalidad Kolmogorov–Smirnov; a través del registro de los datos recolectados migrados del MS Excel al software estadístico IBM SPSS Statistics 25, debido a que la muestra es mayor a 50, con una confianza del 0.95, un margen de error del 0.05 y para criterio de decisión: Si Sig. < 0.05 se refuta la H0; Si Sig. >= 0.05 se admite la H0 y se rechaza la H1. Por ello, se refuta la H0 y se acepta la H1 = Los datos no siguen una distribución normal. Para ello se muestra el resultado obtenido en la tabla 13:

Tabla 13

Pruebas de normalidad de V1: Data Loss Prevention y V2: Prevención de fuga de datos.

	Kolmogorov-Smirnov			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
V1: Data Loss Prevention	0.273	56	0.000	0.781	56	0.000
V2: Prevención de fuga de datos	0.263	56	0.000	0.784	56	0.000

Nota: Elaborado por el investigador, procesado en el IBM SPSS Statistics 25.

4.3 Análisis inferencial

Se utilizó el método no paramétrico, debido al resultado obtenido de la prueba de normalidad de Kolmogorov-Smirnov; paso seguido, tuve a bien utilizar el factor de análisis de Regresión Logística Ordinal (RLO), dicho método nos permitió precisar si concurre una correspondencia correlacional causal indicadora de la relación entre la variable independiente y la variable dependiente estudiadas. Koletsy y Pandis (2018) indican que, la RLO se recomienda al querer pronosticar la conducta de la variable dependiente con categorías ordinales en escalas que se transforman en un determinado número de contestaciones predestinadas. Por lo tanto, se esgrimió el modelo de RLO para validar las hipótesis planteadas y se instauró el desempeño de los datos estadísticos utilizados en la tesis, a través de la prueba de Wald.

Prueba de Hipótesis

Prueba de hipótesis general

Para empezar, se enunciaron las siguientes hipótesis estadísticas:

H1: Data Loss Prevention incide significativamente en la prevención de fuga de datos en un gobierno regional, Lima 2022.

H0: Data Loss Prevention no incide significativamente en la prevención de fuga de datos en un gobierno regional, Lima 2022.

Contrastación de hipótesis estadística:

Tabla 14

Información sobre el ajuste del modelo que explica la incidencia de la variable Data Loss Prevention en la variable prevención de fuga de datos.

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	94.795			
Final	7.068	87.727	1	0.000

Nota: Elaborado por el investigador, procesado en el IBM SPSS Statistics 25.

Se analizó el valor de significancia final de 0.000 de la tabla 14, el cual tiene un valor menor a 0.05; por consiguiente, se dio por aceptada la hipótesis alterna H1 de la prueba de hipótesis general, confirmándose de esta manera que la incidencia de la variable Data Loss Prevention se ajusta al modelo de RLO.

Tabla 15

Bondad de ajuste de la incidencia de la variable Data Loss Prevention en la variable prevención de la fuga de datos.

	Chi-cuadrado	gl	Sig.
Pearson	1.720	3	0.633
Desvianza	2.583	3	0.461

Nota: Elaborado por el investigador, procesado en el IBM SPSS Statistics 25.

Se analizó el resultado del ajuste del modelo Chi-cuadrado siendo este

de 87.727 en la tabla 15. Asimismo, en la tabla 13 se reveló el resultado de la prueba de independencia Chi-cuadrado-Pearson de 1.720. Así también, si sabemos que $87.727 < 1.720$ es incorrecta, se debe rechazar que la variable Data Loss Prevention y prevención de fuga de datos son independientes y, por consiguiente, se asumió que la variable Data Loss Prevention incide significativamente en la variable prevención de fuga de datos. Por último, el nivel de significancia indicado en la tabla 15 fue de 0.633, resultado que es mayor que 0.05, por ende, se logra justificar el uso del modelo RLO.

Tabla 16

Pseudo R Cuadrado de la incidencia de la variable Data Loss Prevention en la variable prevención de fuga da datos.

Coeficiente R ²	Valor
Cox y Snell	0.791
Nagelkerke	0.914
McFadden	0.781

Nota: Elaborado por el investigador, procesado en el IBM SPSS Statistics 25.

Se observó que el coeficiente Pseudo R Cuadrado de Nagelkerke en la tabla 16 dio la valoración 0.914, siendo a nivel de porcentaje el 91.4%. Es decir, se demuestra que existe una adecuada predicción de la variable independiente Data Loss Prevention en relación con la variable dependiente prevención de fuga de datos; probándose que el 91.4% de la varianza es revelada por la variable independiente sobre la variable dependiente.

Tabla 17

Estimaciones de los parámetros de incidencia de la variable Data Loss Prevention en la variable prevención de la fuga de datos.

		Estimación	Desv. Error	Wald	gl	Sig.	Intervalo de confianza al 95%	
							Límite inferior	Límite superior
Umbral	[V2 = 1]	9.286	2.206	17.725	1	0.000	4.963	13.609
	[V2 = 2]	16.990	3.588	22.425	1	0.000	9.958	24.021
Ubicación	V1	6.564	1.282	26.229	1	0.000	4.052	9.077

Nota: Elaborado por el investigador, procesado en el IBM SPSS Statistics 25.

Se observó que el valor de la estimación de la variable independiente

Data Loss Prevention tuvo un resultado de 6.564 en la tabla 17, un resultado de significancia para la prueba de Wald de 0.000; asimismo, se interpretó que el coeficiente de RLO dio como resultado un P valor de 0.000, menor al margen de error de 0.05, por lo cual, se rechazó la hipótesis nula sustentando fehacientemente y con la suficiente evidencia estadística, la existencia de la incidencia significativa entre la variable independiente y la variable dependiente de un gobierno regional, 2022.

Prueba de hipótesis específica 1:

Para continuar, se enunciaron las siguientes hipótesis estadísticas:

H1¹: Existe incidencia significativa entre la variable Data Loss Prevention y la dimensión previene datos en uso de la variable prevención de fuga de datos en un gobierno regional, Lima 2022.

H0¹: No existe incidencia significativa entre la variable Data Loss Prevention y la dimensión previene datos en uso de la variable prevención de fuga de datos en un gobierno regional, Lima 2022.

Contrastación de hipótesis estadística:

Tabla 18

Información sobre el ajuste del modelo de líneas paralelas que explica la incidencia de la variable Data Loss Prevention en la dimensión previene datos en uso de la variable prevención de fuga de datos.

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	112.392			
Final	0.000	112.392	1	0.000

Nota: Elaborado por el investigador, procesado en el IBM SPSS Statistics 25.

Se nos presentó el resultado de significancia final de 1 y siendo este resultado mayor a 0.05 en la tabla 18, se rechaza la hipótesis alterna H1¹ de la prueba de hipótesis específica 1, confirmándose la presencia del modelo RLO que se planteó; sustentando fehacientemente y con la suficiente evidencia estadística, la existencia de la incidencia significativa entre la variable

independiente y la dimensión previene datos en uso de la variable dependiente de un gobierno regional, 2022.

Tabla 19

Bondad de ajuste de la incidencia de la variable Data Loss Prevention en la dimensión previene datos en uso de la variable prevención de fuga de datos.

	Chi-cuadrado	gl	Sig.
Pearson	0.000	3	1.000
Desvianza	0.001	3	1.000

Nota: Elaborado por el investigador, procesado en el IBM SPSS Statistics 25.

Se aprecia el resultado final del ajuste del modelo Chi-cuadrado, siendo el valor obtenido 0.000 en la tabla 19. Asimismo, se aprecia el resultado de la prueba de independencia Chi-cuadrado-Pearson, siendo el valor obtenido 0.000. Por lo tanto, sabemos que $112.392 < 0.000$ es incorrecta, se acepta la dimensión previene datos en uso de la variable prevención de fuga de datos. Para finalizar, el nivel de significancia en la tabla 19 dio como resultado 1.000, valor superior a 0.05, confirmándose la presencia del modelo RLO que se planteó.

Tabla 20

Pseudo R Cuadrado de la incidencia de la variable Data Loss Prevention en la dimensión previene datos en uso de la variable prevención de fuga de datos.

Coeficiente R²	Valor
Cox y Snell	0.866
Nagelkerke	1.000
McFadden	1.000

Nota: Elaborado por el investigador, procesado en el IBM SPSS Statistics 25.

Se comprobó que para el coeficiente Pseudo R Cuadrado de Nagelkerke se obtuvo 1.000 en la tabla 20, cuya expresión porcentual del 100.00% recae en el supuesto de que cuando este valor se acerca más a uno, quiere decir que el modelo es mucho más preciso y que representa un correcto pronóstico de la variable Data Loss Prevention en correlación con la dimensión previene datos en uso de la variable prevención de fuga de datos. Así mismo, se puede probar que el 100.00% de la varianza es revelada por la variable Data Loss Prevention en

relación con la dimensión previene datos en uso de la variable prevención de fuga de datos.

Tabla 21

Estimaciones de los parámetros de incidencia de la variable Data Loss Prevention en la dimensión previene datos en uso de la variable prevención de fuga da datos.

		Intervalo de confianza al 95%						
		Estimación	Desv. Error	Wald	gl	Sig.	Límite inferior	Límite superior
Umbral	[VAR2 = 1]						38.037	259.991
	[VAR2 = 2]	62.669	321.638	0.038	1	0.846	-567.729	693.068
Ubicación	V1D2V2	25.174	132.915	0.036	1	0.850	-235.334	285.683

Nota: Elaborado por el investigador, procesado en el IBM SPSS Statistics 25.

Se observó que el valor de la estimación de la dimensión previene datos en uso de la variable prevención de fuga de datos registró un valor de 25.174 en la tabla 21, obteniéndose una significancia de 0.000 para la prueba de Wald. Por lo cual, se dedujo que después de emplear el coeficiente estadístico de RLO se logró un P valor de 0.000, menor al error significativo de 0.05, por lo tanto, se rechaza la hipótesis nula (H_0^1) sustentando fehacientemente y con la suficiente evidencia estadística, la existencia de la incidencia significativa entre la variable independiente y la dimensión previene datos en uso de la variable dependiente de un gobierno regional, 2022.

Prueba de hipótesis específica 2:

Para continuar, se enunciaron las siguientes hipótesis estadísticas:

H1²: Existe incidencia significativa entre la variable Data Loss Prevention y la dimensión previene datos en movimiento de la variable prevención de fuga de datos en un gobierno regional, Lima 2022.

H0²: No existe incidencia significativa entre la variable Data Loss Prevention y la dimensión previene datos en movimiento de la variable prevención de fuga de datos en un gobierno regional, Lima 2022.

Contrastación de hipótesis estadística:

Tabla 22

Información sobre el ajuste del modelo de líneas paralelas que explica la incidencia de la variable Data Loss Prevention en la dimensión previene datos en movimiento de la variable prevención de fuga de datos.

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	94.795			
Final	7.068 ^b	87.727	1	0.000

Nota: Elaborado por el investigador, procesado en el IBM SPSS Statistics 25.

Se nos presentó el resultado de significancia final de 0.108 y siendo este resultado mayor a 0.05 en la tabla 22, se rechaza la hipótesis alterna H1² de la prueba de hipótesis específica 2, confirmándose la presencia del modelo RLO aplicado y sustentando fehacientemente y con la suficiente evidencia estadística, la existencia de la incidencia significativa entre la variable independiente y la dimensión previene datos en movimiento de la variable dependiente de un gobierno regional, 2022.

Tabla 23

Bondad de ajuste de la incidencia de la variable Data Loss Prevention en la dimensión previene datos en movimiento de la variable prevención de fuga de datos.

	Chi-cuadrado	gl	Sig.
Pearson	1.720	3	0.633
Desviación	2.583	3	0.461

Nota: Elaborado por el investigador, procesado en el IBM SPSS Statistics 25.

Se aprecia el resultado final del ajuste del modelo Chi-cuadrado, siendo el valor obtenido 0.000 en la tabla 23. Asimismo, en la tabla 17 se aprecia el resultado de la prueba Chi-cuadrado-Pearson, siendo el valor obtenido 1.720. Por lo tanto, sabemos que $87.727 < 1.720$ es incorrecta, se acepta la dimensión previene datos en movimiento de la variable prevención de fuga de datos. Para finalizar, el nivel de significancia en la tabla 23 dio como resultado 0.633,

resultado que es mayor a 0.05, confirmándose la presencia del modelo RLO aplicado.

Tabla 24

Pseudo R Cuadrado de la incidencia de la variable Data Loss Prevention en la dimensión previene datos en movimiento de la variable prevención de fuga de datos.

Coefficiente R²	Valor
Cox y Snell	0.791
Nagelkerke	0.914
McFadden	0.781

Nota: Elaborado por el investigador, procesado en el IBM SPSS Statistics 25.

Se comprobó un valor de 0.914 para el coeficiente Pseudo R Cuadrado de Nagelkerke en la tabla 24, cuya expresión porcentual del 91.4% incurre en el supuesto de que cuando este valor se acerca a uno, quiere decir que el modelo es mucho más ajustado y que describe un correcto pronóstico de la variable Data Loss Prevention en relación con la dimensión previene datos en movimiento de la variable prevención de fuga de datos; también se validó que el 91.4% de la varianza es revelada por la variable Data Loss Prevention en relación con la dimensión previene datos en movimiento de la variable prevención de fuga de datos.

Tabla 25

Estimaciones de los parámetros de incidencia de la variable Data Loss Prevention en la dimensión previene datos en movimiento de la variable prevención de fuga da datos.

		Intervalo de confianza al 95%						
		Estimación	Desv. Error	Wald	gl	Sig.	Límite inferior	Límite superior
Umbral	[VAR2 = 1]	9.286	2.206	17.725	1	0.000	4.963	13.609
	[VAR2 = 2]	16.990	3.588	22.425	1	0.000	9.958	24.021
Ubicación	V1D3V2	6.564	1.282	26.229	1	0.000	4.052	9.077

Nota: Elaborado por el investigador, procesado en el IBM SPSS Statistics 25.

Se observó que el valor de la estimación de la dimensión previene datos en movimiento de la variable prevención de fuga de datos registró un valor de 6.564 en la tabla 25, obteniéndose una significancia de 0.000 para la prueba de Wald. Por lo cual, se dedujo que después de emplear el coeficiente estadístico de RLO se logró un P valor de 0.000, menor al error significativo de 0.05, por ello, se rechaza la hipótesis nula (H_0^2) sustentando fehacientemente y con la suficiente evidencia estadística, la existencia de la incidencia significativa entre la variable independiente y la dimensión previene datos en movimiento de la variable dependiente de un gobierno regional, 2022.

Prueba de hipótesis específica 3:

Para continuar, se enunciaron las siguientes hipótesis estadísticas:

H_1^3 : Existe incidencia significativa entre la variable Data Loss Prevention y la dimensión previene datos en reposo de la variable prevención de fuga de datos en un gobierno regional, Lima 2022.

H_0^3 : No existe incidencia significativa entre la variable Data Loss Prevention y la dimensión previene datos en reposo de la variable prevención de fuga de datos en un gobierno regional, Lima 2022.

Contrastación de hipótesis estadística:

Tabla 26

Información sobre el ajuste del modelo de líneas paralelas que explica la incidencia de la variable Data Loss Prevention en la dimensión previene datos en reposo de la variable prevención de fuga de datos.

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	112.392			
Final	0.000	112.392	1	0.000

Nota: Elaborado por el investigador, procesado en el IBM SPSS Statistics 25.

Se nos presentó el resultado de significancia final de 1 y siendo este resultado mayor a 0.05 en la tabla 26, se rechaza la hipótesis alterna H_1^3 de la prueba de hipótesis específica 1, aplicado y sustentando fehacientemente y con la

suficiente evidencia estadística, la existencia de la incidencia significativa entre la variable independiente y la dimensión previene datos en reposo de la variable dependiente de un gobierno regional, 2022.

Tabla 27

Bondad de ajuste de la incidencia de la variable Data Loss Prevention en la dimensión previene datos en reposo de la variable prevención de fuga de datos

	Chi-cuadrado	gl	Sig.
Pearson	0.000	3	1.000
Desviación	0.001	3	1.000

Nota: Elaborado por el investigador, procesado en el IBM SPSS Statistics 25.

Se aprecia el resultado final del ajuste del modelo Chi-cuadrado, siendo el valor obtenido 0.000 en la tabla 27. Asimismo, se aprecia el resultado de la prueba Chi-cuadrado-Pearson, siendo el valor obtenido 0.000. Por lo tanto, sabemos que $112.392 < 0.000$ es incorrecta, se acepta la dimensión previene datos en reposo de la variable prevención de fuga de datos. Para finalizar, el nivel de significancia en la tabla 27 dio como resultado 0.633, resultado mayor a 0.05, justificándose que los datos investigados son estables con el modelo indicado.

Tabla 28

Pseudo R Cuadrado de la incidencia de la variable Data Loss Prevention en la dimensión previene datos en movimiento de la variable prevención de fuga de datos.

Coefficiente R²	Valor
Cox y Snell	0.866
Nagelkerke	1.000
McFadden	1.000

Nota: Elaborado por el investigador, procesado en el IBM SPSS Statistics 25.

Se comprobó un valor de 1.000 para el coeficiente Pseudo R Cuadrado de Nagelkerke en la tabla 28, cuya expresión porcentual del 100.0% recae en el supuesto de que cuando este valor se acerca más a uno, quiere decir que el modelo es mucho más preciso y que representa un correcto pronóstico, el cual se confirma al probarse que el 100.0% de la varianza es explicada por la variable

Data Loss Prevention en relación con la dimensión previene datos en reposo de la variable prevención de fuga de datos.

Tabla 29

Estimaciones de los parámetros de incidencia de la variable Data Loss Prevention en la dimensión previene datos en movimiento de la variable prevención de fuga de datos.

		Intervalo de confianza al 95%						
		Estimación	Desv. Error	Wald	gl	Sig.	Límite inferior	Límite superior
Umbral	[VAR2 = 1]						38.037	259.991
	[VAR2 = 2]	62.669	321.638	0.038	1	0.846	-567.729	693.068
Ubicación	V1D3V2	25.174	132.915	0.036	1	0.850	-235.334	285.683

Nota: Elaborado por el investigador, procesado en el IBM SPSS Statistics 25.

Se observó que el valor de la estimación de la dimensión previene datos en reposo de la variable prevención de fuga de datos registró un valor de 6.564 en la tabla 29. Asimismo, logró una significancia de 0.850 para la prueba de Wald. Por lo cual, se dedujo que después de emplear el coeficiente estadístico de RLO se logró un P valor de 0.000, menor al error significativo de 0.05, por ello, se rechaza la hipótesis nula (H_0^3) sustentando fehacientemente y con la suficiente evidencia estadística, la existencia de la incidencia significativa entre la variable independiente y la dimensión previene datos en reposo de la variable dependiente de un gobierno regional, 2022.

V. DISCUSIÓN

Como consecuencia de los resultados, donde se evaluó la incidencia de la tecnología Data Loss Prevention en la prevención de fuga de datos en un gobierno regional en Lima 2022, procederé con la discusión respecto a la hipótesis general y las hipótesis específicas.

Respecto a la hipótesis general: para empezar, tomando en referencia los resultados que se obtuvieron para validar si la tecnología Data Loss Prevention incide significativamente en la prevención de fuga de datos en un gobierno regional en Lima 2022.

En primera instancia, después de realizar el análisis descriptivo, se puede mencionar que el resultado de las respuestas de los servidores públicos del gobierno regional se situó en el nivel no óptimo fueron 8 respuestas que se relacionan con el 14.3% del nivel malo de la variable prevención de fuga de datos. Así mismo, se validó que el nivel medio de la variable independiente Data Loss Prevention fueron 22 respuestas que se relacionaron con el 39.3% del nivel regular de la variable prevención de fuga de datos. Por otro lado, se verificó que el nivel óptimo de la variable independiente Data Loss Prevention fue de 22 respuestas que hacen plena referencia de 39.3% con el nivel bueno de la variable dependiente prevención de fuga de datos respectivamente. De este análisis se desprende, que los niveles regular y bueno y, medio y óptimo se relacionan con un 39.3% del total de los servidores públicos del gobierno regional respectivamente.

En segunda instancia, se analizó el análisis inferencial donde se puede mencionar que el uso del modelo de RLO es sumamente importante para el desarrollo de la tesis, en la prueba de ajuste aparece el resultado de significancia de 0.000, valor inferior a 0.05. Aunado a esto, se logró determinar que los datos analizados tienen una consistencia con la RLO, donde la prueba Chi-cuadrado de Pearson da como resultado 1.720, valor superior a 0.05. Asimismo, el resultado del Pseudo R Cuadrado de Nagelkerke fue de 0.914, el cual equivale al 91.4% de la variable independiente Data Loss Prevention sobre la variable dependiente prevención de fuga de datos. Para finalizar, se justifica el

coeficiente de la RLO para la estimación de la incidencia a través del resultado 6.584, que confirma la congruencia con tendencia a 0.000, siendo un valor menor a 0.05, confirmando que sí existe una incidencia significativa de la variable independiente Data Loss Prevention sobre la variable dependiente prevención de fuga de datos. Al respecto, los resultados esgrimidos en el párrafo anterior concuerdan con el hallazgo de García et al. (2017), donde mencionan de manera concluyente que una herramienta DLP es sumamente necesaria para mantener la seguridad aplicando el cifrado basado en el contexto a la información sensible, e impide de esta manera la posible fuga de datos no sólo por atacantes externos, sino también por internos; siendo la lectura de un archivo en promedio entre 120 a 130ms adicionales para validar el acceso al mismo. En tal sentido, Husham et al. (2020) manifestaron que las amenazas internas y externas son las dos razones principales para la pérdida de datos, siendo las DLP's las tecnologías que se encargan de proteger los datos importantes y si utilizan el algoritmo Mrsh-v2 mediante el conjunto de datos TS se obtiene una alta tasa de verdadero positivo y, una sensibilidad de 0.85 de 1, infiriéndose que existe un gran conjunto de tipos de archivos descubiertos correctamente por este algoritmo. Por otra parte, Lora y Montenegro (2018) sostuvieron que una estrategia de DLP permite proteger los datos confidenciales de la institución, detectando y deteniendo las amenazas persistentes avanzadas, siempre y cuando se practiquen las políticas de seguridad de la información aunadas a los sistemas de detección (IDS) y prevención de intrusos (IPS) sobre todo en los equipos tecnológicos que tienen un nivel de fuga medio, alto y superior; según se plasma al analizar los riesgos con la metodología Magerit y el modelo Kill Chain para coadyubar en la detección de amenazas, a través de los controles adecuados para obtener una apropiada gestión de la seguridad de los datos. En ese mismo contexto, Godínez y Olvera (2017) concluyen que la tecnología DLP es la mejor opción hacia la prevención de la fuga de datos en los equipos tecnológicos de cualquier institución ahorrando costos y tiempo, concientizando a los usuarios en el uso de los datos (sensibles) y el mensaje que recae en la seguridad de la información, que es tarea de todos. Asimismo, Heinert (2018) reafirma que la tecnología DLP es la mejor opción para impedir la fuga de datos de cualquier organización; pero para que se consiga este resultado, se debe crear una estrategia que comprende la creación

de políticas y mecanismos que controlen y, eviten la fuga de los datos durante los tres estados de los datos: uso, movimiento y reposo, al encontrarse las evidencias de manipulación y extracción necesarias hacia la revisión constante de las políticas de seguridad de la información y los informes que genera la herramienta, dando un seguimiento adecuado para prevenir la fuga de los datos.

Respecto a la hipótesis específica 1: paso seguido, se muestra la cuestión de los resultados obtenidos en la tesis, en relación con la incidencia de la variable Data Loss Prevention en la dimensión de previene datos en uso de la prevención de fuga de datos en un gobierno regional, Lima 2022.

En primera instancia, después de realizar el análisis descriptivo, se puede mencionar que el número de respuestas de los servidores públicos del gobierno regional se situaron en el nivel no óptimo fueron 8 respuestas que se relacionan con el 14.3% del nivel malo de la variable prevención de fuga de datos. Así mismo, se validó que el nivel medio de la variable independiente Data Loss Prevention fueron 23 respuestas que se relacionaron con el 41.1% del nivel regular de la variable prevención de fuga de datos. Por ello, se comprobó que el nivel óptimo de la variable independiente Data Loss Prevention fue de 22 respuestas que hacen plena referencia de 39.3% con el nivel bueno de la variable dependiente prevención de fuga de datos respectivamente. De este análisis se desprende, que los niveles regular y bueno y, medio y óptimo se relacionan con un 41.1% y 39.3% del total de los servidores públicos del gobierno regional respectivamente.

En segunda instancia, se analizó el análisis inferencial concluyendo que el uso del modelo de RLO es fuertemente significativo para el progreso de la tesis, dado que en el ensayo del ajuste aparece el resultado de significancia de 0.000, valor superior a 0.05. Aunado a esto, se determinó que los datos analizados gozan de consistencia con la RLO, donde la prueba Chi-cuadrado de Pearson da como resultado 0.000, valor superior a 0.05. el Pseudo R Cuadrado de Nagelkerke involucra que el 100.0% de la varianza es aplicada por la variable independiente Data Loss Prevention sobre la dimensión previene datos en uso de la variable dependiente prevención de fuga de datos. Para finalizar, se

justifica y confirma el coeficiente de la RLO para demostrar fehacientemente que, existe una incidencia reveladora de la variable independiente Data Loss Prevention sobre la dimensión previene datos en uso de la variable dependiente prevención de fuga de datos. Al respecto, los resultados coinciden con Fritchen (2019) al definir a la variable Data Loss Prevention como el acumulado de prácticas y técnicas, que evitan que la información sensible y protegida caiga en manos equivocadas de manera voluntaria o involuntaria, teniendo medidas de prevención de datos en capas con un nivel de seguridad alto, permitiendo muchas más posibilidades de éxito para lograr su objetivo primordial. De manera similar, OSTEC (2015) sostiene que, Data Loss Prevention se utiliza durante el monitoreo de eventos que podrían ocasionar filtración de datos; posibilitando la prevención y mitigación de vulnerabilidades evidenciadas cuando se hacen presentes; mostrando como establecer las soluciones para lograr el cumplimiento de las políticas de seguridad de la información. Así también, tenemos a gbadvisors (2018) quien nos dice que, Data Loss Prevention es la prevención que se aplica para impedir la pérdida de datos sensibles, ya sea de manera interna (intencionada o manipulada por personal que cuenta con el acceso privilegiado) o externa (programas malignos o virus informáticos); para ello se enfoca desde la prevención y protección, control y reducción mediante herramientas especializadas, a través de la adquisición de hardware y software potenciando la seguridad de la información desde la falta de pericia, hasta la información y negligencia por parte de los usuarios. Asimismo, López et al. (2015) definen que, Data Loss Prevention es la solución tecnológica actual para proteger una organización de fugas de datos y refuerza los criterios de cómo fluirá la información dentro y fuera de la red electrónica de la empresa; es una solución capaz de inspeccionar el contenido de los datos electrónicos de la organización en los formatos de datos más comunes, evitando la evasión de los filtros (tales como los archivos de imágenes, iso, archivos comprimidos y encriptados) para lograr la detección de las infracciones de las políticas de seguridad de la información. En suma, para Torres (2015), es una expresión de la seguridad informática que vislumbra a una correlación de herramientas (principalmente DLP, firewall, IDS e IPS), que evitan la remisión de datos sensible fuera de la institución, describiendo a su vez a las soluciones que la detectan, monitorean y logran evitar que los datos catalogados de confidencial

sean transferidos y, utilizados indebidamente; donde se logra el éxito al realizar el análisis del flujo de los datos y su clasificación, riesgos y la configuración que se realiza en la herramienta para el cumplimiento de las políticas de seguridad de la información. Al respecto, Kelsey (2002) menciona que, la prevención de fuga de datos es la evasión no examinada de información que llega a manos equivocadas, así como la pérdida de su resguardo; a su vez refiere que la fuga se presenta cuando un sistema presenta brechas en su seguridad o integridad, permitiendo a los agresores la interceptación de los datos basándose únicamente en el tamaño de la salida del compresor cuando se utilizan los algoritmos de compresión sin pérdidas; dando como resultado que se debe comprimir la información antes de cifrarla para aumentar la seguridad del sistema, ahorrando ancho de banda y almacenamiento. Por su parte, para Patrizio y Kranz (2021), la prevención de fuga de datos es una estrategia para impedir que los usuarios accedan a datos sensibles que no necesitan, garantizando que el personal no la envíe fuera de la red de la institución de manera accidental o maliciosamente por una infiltración; afirmando, que ha aumentado del 50% al 90% la implementación de por lo menos una tecnología DLP, para evitar mayormente que las fugas de datos sean realizadas por el personal interno cuando cometa un error sin mala intención a través de bloqueos establecidos por el equipo de seguridad de la información. Fitzgibbons (2019), conceptualizó a previene datos en uso como los datos que se están actualizando, procesando, borrando, accediendo o leyendo en un sistema y que no se almacenan pasivamente, sino que se mueven activamente a través de los componentes de una infraestructura de TI. Asimismo, menciona que, a través del cifrado, autenticación del usuario, gestión de la identidad y permisos bien mantenidos dentro de la institución para proteger los datos poniendo en práctica las recomendaciones recibidas por el grupo de profesionales en seguridad de la información para la institución. Al respecto, tenemos también a Froehlich (2020) quien sostuvo que, para proteger los datos en uso es necesario proporcionar una visibilidad adecuada para la detección de infracciones y la mejor manera de proteger los datos en uso es restringir el acceso por función de usuario, limitando el acceso al sistema solo a aquellos que lo necesitan; siendo las organizaciones medianas y pequeñas las más vulnerables porque a menudo no cuentan con herramientas por su costo y la aplicación de políticas de seguridad de la

información adecuadas, teniendo el apoyo de la gerencia dotando del presupuesto y personal necesario para proteger los datos del riesgo de una gran pérdida por fuga.

Respecto a la hipótesis específica 2

Paso seguido, se muestra la cuestión de los resultados obtenidos en la tesis, en relación con la incidencia de la variable Data Loss Prevention en la dimensión de previene datos en movimiento de la prevención de fuga de datos en un gobierno regional, Lima 2022.

En primera instancia, después de realizar el análisis descriptivo, se puede mencionar que el número de respuestas de los servidores públicos del gobierno regional se situaron en el nivel no óptimo fueron 8 respuestas que se relacionan con el 14.3% del nivel malo de la variable prevención de fuga de datos. Así mismo, se validó que el nivel medio de la variable independiente Data Loss Prevention fueron 22 respuestas que se relacionaron con el 39.3% del nivel regular de la variable prevención de fuga de datos. Asimismo, se verificó que el nivel óptimo de la variable independiente Data Loss Prevention fue de 22 respuestas que hacen plena referencia de 39.3% con el nivel bueno de la variable dependiente prevención de fuga de datos respectivamente. De este análisis se desprende, que los niveles regular y bueno y, medio y óptimo se relacionan con un 39.3% del total de los servidores públicos del gobierno regional respectivamente.

En segunda instancia, se analizó el análisis inferencial concluyendo que el uso del modelo de RLO es fuertemente significativo para el progreso de la tesis, dado que en el ensayo del ajuste aparece el resultado de significancia de 0.000, valor superior a 0.05. Aunado a esto, se determinó que los datos analizados gozan de consistencia con la RLO, donde la prueba Chi-cuadrado de Pearson da como resultado 1.720, valor superior a 0.05. el valor registrado para el Pseudo R Cuadrado de Nagelkerke involucra que el 91.4% de la varianza es aplicada por la variable independiente Data Loss Prevention sobre la dimensión previene datos en reposo de la variable dependiente prevención de fuga de datos. Para finalizar, se justifica y confirma el coeficiente de la RLO para

demostrar fehacientemente que, sí existe una incidencia significativa de la variable independiente Data Loss Prevention sobre la dimensión previene datos en reposo de la variable dependiente prevención de fuga da datos.

Al respecto, los resultados esgrimidos en el párrafo anterior concuerdan con Mejía (2015) que define Data Loss Prevention, como las tecnologías que logran identificar, supervisar y finalmente lograr la protección de los datos en movimiento y uso, mediante la investigación del contenido y el análisis del contexto de seguridad centralizado; las DLP están perfiladas en la detección y prevención del uso no autorizado y la transmisión de los datos confidenciales o sensibles por cualquier tipo de medio; para lo cual, plantea la implementación de un DLP de network y un DLP para los file servers, para monitorear el cumplimiento de las políticas de seguridad de la información por los usuarios. Por su parte Sánchez (2015) indicó que, Data Loss Prevention se trata de una solución que permite a las instituciones disponer del descubrimiento, prevención y protección de su información sensible; para ello, se identifican las brechas de seguridad, se analiza el problema de fuga, los incidentes detectados y mejora de procesos, en donde se identifican sus limitaciones de monitoreo de tráfico cifrado, módulo de monitoreo de red y maduración constante. Asimismo, tenemos a Fearn y Tuner (2021) mencionan que, la prevención de fuga de datos proporciona una forma eficaz de evitar la pérdida de datos a través de almacenamiento no seguro o mediante exfiltración maliciosa por parte de terceros. Para García et al. (2017) sostienen que, la prevención de fuga de datos es útil porque ayuda a mantener segura la información sensible; de esta manera evitaremos filtraciones; por lo cual, recomiendan el uso del cifrado basado en contexto con el algoritmo de cifrado asimétrico, porque es el que tiene mejor rendimiento. Para iniciar con previene datos en movimiento se tiene a Allen (2016) que nos dice que los datos en movimiento se encuentran en su punto más vulnerable y es donde se deben centrar la atención de la protección porque es donde lidiamos con errores humanos, fallas en la red, intercambio de archivos inseguro, acciones maliciosas entre otras; por ello, debemos tomar medidas proactivas para lograr la visibilidad, integración y automatización para evitar la fuga de datos, su costo acarreado y pérdida de reputación añadida. Para finalizar, Froehlich (2020) para prevenir los datos en movimiento, se debe

proporcionar una visibilidad adecuada para la detección de infracciones; debido a los avances en las herramientas de seguridad de inteligencia artificial que ingieren datos de telemetría de red y luego los analizan para detectar anomalías en el comportamiento de acceso a los datos pueden identificar amenazas, determinar el alcance del daño y, proporcionar información procesable sobre cómo detener una mayor pérdida de datos; logrando de esta manera, evitar el fraude de identidad y espionaje, siempre teniendo en cuenta que se deben reevaluar constantemente los niveles y reajustarlos a las políticas de seguridad de la información.

Respecto a la hipótesis específica 3

Paso seguido, se muestra la cuestión de los resultados obtenidos en la tesis, en relación con la incidencia de la variable Data Loss Prevention en la dimensión de previene datos en reposo de la prevención de fuga de datos en un gobierno regional, Lima 2022.

En primera instancia, después de realizar el análisis descriptivo, se puede mencionar que el número de respuestas de los servidores públicos del gobierno regional se situaron en el nivel no óptimo fueron 8 respuestas que se relacionan con el 14.3% del nivel malo de la variable prevención de fuga de datos. Así mismo, se validó que el nivel medio de la variable independiente Data Loss Prevention fueron 22 respuestas que se relacionaron con el 39.3% del nivel regular de la variable prevención de fuga de datos. Así también, se verificó que el nivel óptimo de la variable independiente Data Loss Prevention fue de 22 respuestas que hacen plena referencia de 39.3% con el nivel bueno de la variable dependiente prevención de fuga de datos respectivamente. De este análisis se desprende, que los niveles regular y bueno y, medio y óptimo se relacionan con un 39.3% del total de los servidores públicos del gobierno regional respectivamente.

En segunda instancia, se analizó el análisis inferencial concluyendo que el uso del modelo de RLO fuertemente significativo para el progreso de la tesis, dado que en el ensayo del ajuste aparece el resultado de significancia de 0.000, valor superior a 0.05. Aunado a esto, se determinó que los datos examinados

tienen consistencia con la RLO, donde la prueba Chi-cuadrado de Pearson da como resultado 0.000, el valor registrado para el Pseudo R Cuadrado de Nagelkerke involucra que el 100.0% de la varianza es aplicada por la variable independiente Data Loss Prevention sobre la dimensión previene datos en reposo de la variable dependiente prevención de fuga de datos. Para finalizar, se justifica y confirma el coeficiente de la RLO para demostrar fehacientemente que, sí existe una incidencia significativa de la variable independiente Data Loss Prevention sobre la dimensión previene datos en reposo de la variable dependiente prevención de fuga de datos.

Al respecto, Tujab (2017) manifiesta que, la prevención de fuga de datos se trata de toda aquella gestión enfocada en evitar cualquier riesgo que vulnere la confiabilidad, integridad y disponibilidad. Al ocurrir una fuga, se genera un impacto y consecuencias negativas, que es la que mayor preocupación despierta en las instituciones, pues la filtración de información daña su imagen y además genera desconfianza e inseguridad, sobre todo si la información filtrada pone en riesgo a los usuarios o clientes de la institución; dando como resultado, que es completamente necesario el establecimiento de métodos específicos de detección y fortalecer la prevención a tiempo de una fuga de datos, sin olvidarse de la capacitación continua en seguridad de la información y la concientización de las políticas de seguridad de la información. Asimismo, Neha y Rashmi (2018) quienes sostuvieron que, son los datos que se han vaciado de la memoria y se han escrito en el disco. Para Mantis Net (2021), son los datos inactivos que se almacenan físicamente en cualquier forma digital. Finalmente, Froehlich (2020) menciona que, para proteger mejor los datos en reposo, las organizaciones deben saber dónde residen todos los datos confidenciales y cómo clasificarlos. Asimismo, refiere que, los datos en reposo son tan seguros como la infraestructura que los respalda. Monitorear continuamente las amenazas internas y externas que intentan acceder a los datos en reposo es otra excelente manera de vigilar la infraestructura y proporcionar una visibilidad adecuada para la detección de infracciones.

Respecto a la metodología de investigación

Para empezar, en esta tesis se recolectaron los datos referentes a la incidencia de Data Loss Prevention en la prevención de fuga de datos en un gobierno regional, para el año 2022. Concretamente, se demostró la incidencia de la tecnología Data Loss Prevention en la prevención de la fuga de datos a través de la aplicación de la regresión logística ordinal; no sin antes, verificar la fiabilidad del Alfa de Cronbach y para ello, se utilizó el IBM SPSS Statistics 25 con un error del 5% y una confianza del 95%.

Al haberse utilizado el tipo de investigación básica, con diseño no experimental, investigación transversal, nivel correlación causal y enfoque cuantitativo, debido a que la muestra de la unidad de análisis de 56 es superior de 50, se tuvo que realizar la prueba de normalidad Kolmogorov – Smirnov, resultando que no existe normalidad. Por lo tanto, se tuvo que realizar el análisis estadístico no paramétrico. Paso seguido, se realizaron las tablas cruzadas de la variable independiente con la variable dependiente, la variable independiente con la dimensión uno de la variable dependiente, la variable independiente con la dimensión dos de la variable dependiente, la variable independiente con la dimensión tres de la variable dependiente.

Finalmente, para realizar la estadística inferencial se escogió la regresión logística ordinal para confirmar la validez de la hipótesis general y específicas, demostrando que sí existe correlación causal entre ellas, mediante el análisis estadístico inferencial a través del valor de significancia, Chi-cuadrado-Pearson, Pseudo R Cuadrado de Nagelkerke, la evaluación de los parámetros para la prueba de Wald. Demostrando de manera contundente, con la suficiente evidencia estadística descriptiva e inferencial y congruentes que: (1) sí existe incidencia significativa entre la variable Data Loss Prevention y la variable prevención de fuga de datos de un gobierno regional, 2022; (2) incidencia significativa entre la variable Data Loss Prevention y la dimensión previene datos en uso de la variable prevención de fuga de datos de un gobierno regional, 2022; (3) incidencia significativa entre la variable Data Loss Prevention y la dimensión previene datos en movimiento de la variable prevención de fuga de datos de un gobierno regional, 2022; y, (4) incidencia significativa entre la variable Data Loss

Prevention y la dimensión previene datos en reposo de la variable prevención de fuga de datos de un gobierno regional, 2022.

VI. CONCLUSIONES

Primero Para la variable Data Loss Prevention dio como resultado de la estimación un valor de 6.584 y una significancia de 0.000 con la prueba de Wald; por consiguiente, se concluyó que existe incidencia significativa sobre la variable independiente prevención de fuga de datos en un gobierno regional, Lima 2022. De esta manera, se dio por alcanzada la hipótesis general y por consecuencia, se cumple con el objetivo general de la tesis. Al mismo tiempo, se pudo establecer que el 39.3% de la muestra consideró que para la variable dependiente prevención de fuga de datos posee un nivel regular o bueno para la incidencia medio y óptimo de la variable independiente Data Loss Prevention.

Segundo Para la dimensión previene datos en uso de la variable prevención de fuga de datos dio como resultado de estimación un valor de 25.174 y una significancia de 0.850 con la prueba de Wald; por consiguiente, se concluyó que existe incidencia de la variable independiente Data Loss Prevention sobre la dimensión previene datos en uso de la variable dependiente prevención de fuga de datos en un gobierno regional, Lima 2022. De esta manera, se dio por alcanzada la hipótesis específica 1 y por consecuencia, se cumple con el objetivo específico 1. Al mismo tiempo, se pudo establecer que el 41.1% de la muestra consideró que para la variable dependiente prevención de fuga de datos posee un nivel regular ante la incidencia medio y óptimo para la dimensión previene datos en uso de la variable independiente Data Loss Prevention.

Tercero Para la dimensión previene datos en movimiento de la variable prevención de fuga de datos dio como resultado de estimación un valor de 6.564 y una significancia de 0.000 con la prueba de

Wald; por consiguiente, se concluyó que existe incidencia de la variable independiente Data Loss Prevention sobre la dimensión previene datos en movimiento de la variable dependiente prevención de fuga de datos en un gobierno regional, Lima 2022. De esta manera, se dio por alcanzada la hipótesis específica 2 y por consecuencia, se cumple con el objetivo específico 2. Al mismo tiempo, se pudo establecer que el 39.3% de la muestra consideró que para la variable dependiente prevención de fuga de datos posee un nivel regular o bueno para la incidencia medio y óptimo para la dimensión previene datos en movimiento de la variable independiente Data Loss Prevention.

Cuarto

Para la dimensión previene datos en uso de la variable prevención de fuga de datos dio como resultado de estimación un valor de 6.584 y una significancia de 0.000 con la prueba de Wald; por consiguiente, se concluyó que existe incidencia de la variable independiente Data Loss Prevention sobre la dimensión previene datos en movimiento de la variable dependiente prevención de fuga de datos en un gobierno regional, Lima 2022. De esta manera, se dio por alcanzada la se dio por alcanzada la hipótesis específica 3 y por consecuencia, se cumple con el objetivo específico 3. Al mismo tiempo, se pudo establecer que el 41.1% de la muestra consideró que para la variable dependiente prevención de fuga de datos posee un nivel regular para la incidencia medio y óptimo para la dimensión previene datos en reposo de la variable independiente Data Loss Prevention.

VII. RECOMENDACIONES

- Primero** Se recomienda como área usuaria a la gerencia del gobierno regional realizar un requerimiento dirigido a la subgerencia de tecnologías de la información a fin de capacitar y sensibilizar a los servidores públicos sobre la tecnología Data Loss Prevention en el descubrimiento, prevención y protección de los datos sensibles durante su uso, movimiento y reposo en la institución.
- Segundo** Se recomienda como área usuaria a la gerencia del gobierno regional realizar un requerimiento dirigido a la subgerencia de tecnologías de la información para concientizar vía correos electrónicos, capacitaciones y entrega física de la documentación a los servidores públicos de las políticas generales de seguridad de la información, basados en Cobit e ITIL 4 reduciendo los riesgos tecnológicos y los delitos informáticos en la institución para no perder la confidencialidad.
- Tercero** Se recomienda como área usuaria a la gerencia del gobierno regional realizar un requerimiento dirigido a la subgerencia de tecnologías de la información para que el jefe de redes y comunicaciones realice el control y, monitorear la infraestructura tecnológica con la herramienta ProactiveNet 9.6 o BPPM 10 del fabricante BMC para la prevención del uso de los datos en movimiento para no perder la disponibilidad de los servicios tecnológicos.
- Cuarto** Se recomienda como área usuaria a la gerencia del gobierno regional realizar un requerimiento dirigido a la subgerencia de tecnologías de la información para realizar webinarios vía Zoom o Google Meet a los usuarios de manera permanente, referente a los niveles de protección de fuga de datos cuando se almacenan mostrando algunos cuadros o gráficos para lograr el

cumplimiento del objetivo principal de la institución que es mejorar el servicio al ciudadano.

REFERENCIAS

- Acero, C. (2019). Implementación de un Sistema de Internet de las Cosas para Optimizar la Gestión del Agua en la Agricultura de la Región Tacna, 2018. (U. P. Tacna, Ed.) Tacna, Perú. <https://doi.org/http://hdl.handle.net/20.500.12969/1304>
- Albors, J. (2017). ¿Es seguro guardar información corporativa en Google Drive (o servicios similares)? *Welivesecurity by ESET*. Obtenido de <https://www.welivesecurity.com/la-es/2017/07/10/google-drive-informacion-corporativa/>
- Allen, R. (2016). Securing data in motion. (H. N. Security, Ed.) Obtenido de <https://www.helpnetsecurity.com/2016/10/25/securing-data-in-motion/>
- Antony et al. (2017). Manual for writing a data protection concept. *TMF - Technologie - und Methodenplattform für die vernetzte medizinische Forschung e. V.* Obtenido de http://www.tmf-ev.de/DesktopModules/Bring2mind/DMX/Download.aspx?Method=attachment&Command=Core_Download&EntryId=32356&PortalId=0
- Arnold, M. y. (1998). Introducción a los Conceptos Básicos de la Teoría General de Sistemas. (U. d. Chile, Ed.) *Sistema de Información Científica Redalyc*. Obtenido de <https://www.redalyc.org/articulo.oa?id=10100306>
- Arras et al. (2008). Comunicación y cambio organizacional. *Revista Latina de Comunicación Social* (Núm. 63), 418-434. Obtenido de http://www.ull.es/publicaciones/latina/08/35_792_51_Chihuahua/Ana_Maria_Arraz.html
- Astrom, K. (21-23 de June de 2006). *Challenges in Control Education*. Obtenido de Symposium on Advances in Control Education: <http://archive.control.lth.se/media/Staff/KarlJohanAstrom/Lectures/ControlEducationMadrid2006.pdf>
- Bertoglio, O. (1993). Introducción a la Teoría General de Sistemas. En G. N. Editores (Ed.). México: Editorial Limusa S.A. Obtenido de https://camilos03.files.wordpress.com/2015/08/1-_introduccion_a_la_teor%C3%ADa_general_de_sistemas_-_oscar_johansen2-libre.pdf
- Borja, J. (2009). El Centro Refleja El Proceso Democrático. *Km. cero, diciembre 2009*(17), 10-11. Obtenido de <https://issuu.com/kmcerorevista/docs/km0-17>
- Bunga, I. y. (15 de September de 2020). The influence of internal control on fraud prevention (Case study at Bank BRI of Cimahi City). *International Journal of Financial, Accounting, and Management*, Vol. 2(Núm. 3), 199-211. <https://doi.org/https://doi.org/10.35912/ijfam.v2i2.165>

- Ccesa, M. (2017). Diseño de un sistema de gestión de Seguridad de la Información bajo la NTP ISO/IEC 27001:2014 para la Municipalidad Provincial de Huamanga, 2016. (U. N. Huamanga, Ed.) Huamanga, Ayacucho, Perú. Obtenido de <http://repositorio.unsch.edu.pe/handle/UNSCH/1751>
- Corona, M. (2020). ITIL 4 y Information Security Management Practice. Best Practice Gurus - IT Service Management Republic Dominican. Obtenido de <https://www.youtube.com/watch?v=Qewg616QAYs>
- Diccionario de la lengua española. (2020). Prevención. (Edición del Tricentenario). (R. A. Española, Ed.) Madrid, España. Obtenido de <https://dle.rae.es/prevenci%C3%B3n>
- Diccionario Reverso. (2018). Definición descubrimiento. (K. D. Español-Definiciones, Ed.) Obtenido de <https://mobile-dictionary.reverso.net/es/espanol-definiciones/descubrimiento>
- Domínguez, V. y. (2019). Teoría General de Sistemas, un enfoque práctico. *Tecnociencia Chihuahua, Revista de ciencia y tecnología, Vol. X(Núm. 3)*, 125-132. Obtenido de <https://vocero.uach.mx/index.php/tecnociencia/article/view/174/137>
- Dota et al. (1999). Epistemología e Historia de la Ciencia. (U. N. Córdoba, Ed.) *Selección de Trabajos de las IX Jornadas, Vol. 5(Núm. 5)*, 282-285. Obtenido de <https://rdu.unc.edu.ar/bitstream/handle/11086/3383/45%20-%20Que%20es%20el%20descubrimiento.pdf?sequence=1&isAllowed=y>
- Emotiv. (2021). What is Data Privacy? USA. Obtenido de <https://www.emotiv.com/glossary/data-privacy/>
- Fearn, N. y. (2021). Best data loss prevention service of 2021. (TechRadar, Ed.) United Kingdom. Obtenido de <https://www.techradar.com/uk/best/best-data-loss-prevention>
- Fermín, F. (2012). La Teoría de Control y la Gestión Autónoma de Servidores Web. (C. 2012, Ed.) *IV Congreso Internacional de Computación y Telecomunicaciones*, 73-78. Obtenido de http://repositorio.uigv.edu.pe/bitstream/handle/20.500.11818/859/Paper_servidoresweb.pdf?sequence=1&isAllowed=y
- Fitzgibbons, L. (2019). Definition data in use. (TechTarget, Ed.) USA. Obtenido de <https://whatis.techtarget.com/definition/data-in-use>
- Fritchen, K. (2019). How to prevent data loss. (M. Methods, Ed.) USA. Obtenido de <https://managedmethods.com/blog/how-to-prevent-data-loss/>
- Froehlich, A. (2020). How to secure data at rest, in use and in motion. With internal and external cyberthreats on the rise, check out these tips to best protect and secure data at rest and in motion. (TechTarget, Ed.) USA. Obtenido de <https://searchsecurity.techtarget.com/feature/Best-practices-to-secure-data-at-rest-in-use-and-in-motion>

- García et al. (27-29 de septiembre de 2017). Sistema de cifrado basado en contexto aplicado a prevención de fuga de datos. (U. P. Madrid, Ed.) *XIII Jornadas de Ingeniería telemática (JITEL 2017)*, 93-100. <https://doi.org/https://doi.org/10.4995/JITEL2017.2017.6576>
- gbadvisors. (11 de JUNE de 2018). All you need to know about Data Leak Prevention (DLP) and Compliance to protect your digital assets. (Tech-Blog, Ed.) USA. Obtenido de <https://www.gb-advisors.com/data-leak-prevention-dlp/>
- Godínez, A. y. (2017). Implementación de un sistema de seguridad DLP (Data Loss Prevention). (U. A. México, Ed.) México. <https://doi.org/http://132.248.9.195/ptd2017/febrero/0756317/Index.html>
- González et al. (diciembre de 2017). Diseño y Validación de una Encuesta para la Caracterización de Unidades de Producción Caprina. (U. C. Venezuela, Ed.) *Revista de la Facultad de Ciencias Veterinarias*, Vol. 52(Núm. 2), 68-74. https://doi.org/http://ve.scielo.org/scielo.php?script=sci_arttext&pid=S0258-65762017000200003
- Gran Diccionario de la Lengua Española. (2016). prevención. (n.d.) . (T. F. Farlex, Ed.) Obtenido de <https://es.thefreedictionary.com/prevenci%c3%b3>
- Heinert, L. (08 de junio de 2018). Implementación de una solución Data Loss Prevention (DLP) en una empresa con actividades de servicios alimenticios. (E. S. Litoral, Ed.) Guayaquil, Ecuador. Obtenido de <http://www.dspace.espol.edu.ec/xmlui/handle/123456789/43610>
- Hernández, R. y. (2018). *Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta* (Primera edición ed.). México: Mc Graw Hill Education.
- Husham et al. (August de 2020). Data loss prevention (DLP) by using MRSH-v2 algorithm. *International Journal of Electrical and Computer Engineering (IJECE)*, Vol.10(No. 4), 3615-3622. <https://doi.org/http://doi.org/10.11591/ijece.v10i4.pp3615-3622>
- ICO.ORG Information Commissioner's Office. (2018). Some basic concepts. Obtenido de <https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/some-basic-concepts/#:~:text=Data%20protection%20is%20about%20ensuring,purposes%2C%20you%20need%20to%20comply>
- Kelsey, J. (2002). Compression and Information Leakage of Plaintext. (F. S. Encryption, Ed.) Obtenido de <http://www.iacr.org/cryptodb/archive/2002/FSE/3091/3091.pdf>
- Koenig, S. (2019). What Happened to the Gartner DLP Magic Quadrant? Obtenido de <https://www.zscaler.com/blogs/product-insights/what-happened-gartner-dlp-magic-quadrant>

- Koletsj, D. y. (2018). Ordinal logistic regression. *American Journal of Orthodontics and Dentofacial Orthopedics*, Vol. 153(Núm. 1), 157-158. <https://doi.org/https://doi.org/10.1016/j.ajodo.2017.11.011>
- López et al. (30 de septiembre de 2015). Methodology for Data Loss Prevention Technology Evaluation for Protecting Sensitive Information. *Revista Politécnica*, Vol. 36(Núm. 3), 1-10. Obtenido de https://revistapolitecnica.epn.edu.ec/ojs2/index.php/revista_politecnica2/article/view/582
- Lora, G. y. (2018). Framework de Seguridad informática para mitigar la fuga de información ocasionada por amenazas persistentes avanzadas proveniente de correo electrónico, en los activos de información del sector hospitalario en Colombia. Colombia. <https://doi.org/http://hdl.handle.net/20.500.12622/300>.
- Lv et al. (2019). Current status and future prospects of data leakage prevention technology: A brief review. (C. 2019, Ed.) *Journal of Physics: Conference Series*, Vol. 1345(Núm, 2). <https://doi.org/https://10.1088/1742-6596/1345/2/022010>
- Machicao, S. (2019). Análisis de riesgo y políticas de seguridad de información de la Oficina de Tecnologías de Información (OTI) – UNA Puno 2018. (U. N. Altiplano, Ed., & M. E. Informática, Recopilador) Puno, Perú. Obtenido de <http://repositorio.unap.edu.pe/handle/UNAP/13958>
- Mantis Net. (2021). The Ultimate Cyber Security Strategy Is Data in Motion-The Answer. Obtenido de <https://www.mantisnet.com/blog/the-ultimate-cyber-security-strategy-is-data-in-motion-the-answer>
- Martínez, J. (2020). Descubrimiento diccionario.leyderecho.org. Obtenido de <https://diccionario.leyderecho.org/descubrimiento/>
- Mejía, M. (2015). Propuesta de un modelo de seguridad para el tratamiento de documentos confidenciales en entidades del estado ecuatoriano que se encuentren sujetas al cumplimiento del acuerdo 166 emitido por la secretaria nacional de Administración Pública, caso de estudi. (P. U. Ecuador, Ed.) Quito, Ecuador. Obtenido de <http://repositorio.puce.edu.ec/handle/22000/9695>
- Ministerio de Economía y Finanzas. (2003). LEY Nº 28059 - Ministerio de Economía y Finanzas. Lima, Perú. Obtenido de <https://www.mef.gob.pe/es/normatividad/por-temas/descentralizacion/6843-ley-n-28059-2/file#:~:text=El%20Estado%20garantiza%20la%20libre,la%20Constituci%C3%B3n%20y%20las%20leyes>
- Mondragón, D. (2020). ¿SLA o XLA?, midiendo el nivel de experiencia con el servicio. *Revista Contacto de Unión Empresarial*. Obtenido de <https://revistacontacto.com.mx/sla-o-xla-midiendo-el-nivel-de-experiencia-con-el-servicio/>

- Moscoso et al. (2018). Modelo de gestión de riesgos de TI que contribuye a la operación de los procesos de gestión comercial de las empresas del sector de saneamiento del Norte del Perú. (U. C. Mogrovejo, Ed.) Chiclayo, Perú. <https://doi.org/http://hdl.handle.net/20.500.12423/1409>
- Neha, G. y. (2018). A Deep Dive into NoSQL Databases: The Use Cases and Applications. (G. C. Edited by Pethuru Raj, Ed.) *Advances in Computers* – Elsevier BV, Vol. 109, 101-132. <https://doi.org/https://doi.org/10.1016/bs.adcom.2018.01.003>
- Ñaupas et al. (2018). *Metodología de la investigación cuantitativa-cualitativa y redacción de la tesis*. Ediciones de la U.
- Ogata, K. (1998). Ingeniería de control moderna. En P. E. S.A. (Ed.). España: Prentice Hall Hispanoamericana S.A. Obtenido de <https://biblioteca.cio.mx/ebooks/e0213.pdf>
- OSTEC. (2015). DLP: O que é e como funciona? (S. d. resultados, Ed.) Tubarão, Brasil. Obtenido de <https://ostec.blog/seguranca-perimetro/dlp-o-que-e-e-como-funciona/>
- Patrizio, A. y Kranz, G. (2021). What is data loss prevention (DLP)? (TechTarget, Ed.) USA. Obtenido de <https://www.techtarget.com/whatis/definition/data-loss-prevention-DLP>
- Pérez, J. y. (2021). Definicion.de: Definición de descubrimiento. Obtenido de <https://definicion.de/descubrimiento/>
- Pérez, J. y. (2021). Definicion.de: Definición de prevención. Obtenido de <https://definicion.de/prevencion/>
- Polanía, L. (1997). Teoría del Control. *Revista Paideia Surcolombiana* (Núm. 6), 77-81. <https://doi.org/https://doi.org/10.25054/01240307.985>
- Ponce et al. (2019). Buenas prácticas en la gestión del Riesgo de Fraude Interno: Casos de tres bancos de Lima Metropolitana. (P. U. Perú, Ed.) Lima, Perú. <https://doi.org/http://hdl.handle.net/20.500.12404/15152>
- Presidencia del Consejo de Ministros. (28 de junio de 2003). Decreto Supremo N° 066-2003-PCM. *El Peruano*, pág. 246806. Obtenido de https://cdn.www.gob.pe/uploads/document/file/357114/N%C2%BA_066-2003-PCM.pdf
- Presidencia del Consejo de Ministros. (6 de julio de 2004). Resolución Ministerial N° 206-2004-PCM. Lima, Perú. Obtenido de https://cdn.www.gob.pe/uploads/document/file/357354/RM_206-2004-PCM.pdf
- Presidencia del Consejo de Ministros. (2016). 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". (e. t. Informática, Ed.) Lima,

- Perú. Obtenido de <https://busquedas.elperuano.pe/download/url/aprueban-el-uso-obligatorio-de-la-norma-tecnica-peruana-ntp-resolucion-ministerial-no-004-2016-pcm-1333015-1>
- Presidencia del Consejo de Ministros. (8 de enero de 2016). Resolución Ministerial N° 004-2016-PCM. Lima, Perú. Obtenido de https://cdn.www.gob.pe/uploads/document/file/357224/Resoluci%C3%B3n_Ministerial_N__004-2016-PCM20190902-25578-19siyuu.pdf
- ProInversión. (2015). Las Asociaciones Público Privadas en el Perú. En A. d. Privada. Lima, Perú.
- ProInversión. (2020). Memoria Anual de Pro Inversión 2019. *Agencia de Promoción de la Inversión Privada*. Lima, Perú. Obtenido de <https://cdn.www.gob.pe/uploads/document/file/1894729/Memoria-2019.pdf.pdf>
- Ramírez, C. (28 de abril de 1989). La escuela de sistemas y sus aplicaciones a la administración. (U. EAN, Ed.) *Revista Escuela de Administración de Negocios (EAN)*(Núm. 9), 14-20. Obtenido de <https://journal.universidadean.edu.co/index.php/Revista/article/view/1010>
- Rayami, A. (21 de julio de 2020). Prevenir la pérdida de datos y mitigar los riesgos en el entorno actual de trabajo remoto. (N. C. Latinoamérica, Ed.) Obtenido de <https://news.microsoft.com/es-xl/prevenir-la-perdida-de-datos-y-mitigar-los-riesgos-en-el-entorno-actual-de-trabajo-remoto/>
- Real Academia Española - RAE. (2019). Diccionario panhispánico del español jurídico. España. Obtenido de <https://dpej.rae.es/lema/descubrimiento>
- Sánchez, D. (6 de junio de 2015). Implementación de una solución de prevención de fuga de información en una empresa de telecomunicaciones. (E. S. ESPOL, Ed.) Guayaquil, Ecuador. Obtenido de <https://www.dspace.espol.edu.ec/handle/123456789/31559>
- Sealpath. (2022). How to calculate the cost of a data breach - A Case Study. Cybersecurity Compliance. Retrieved from <https://www.sealpath.com/blog/how-to-quantify-the-cost-of-a-data-breach-a-case-study/>
- Serna, E. (2017). Descubrimiento, innovación y objetividad: Schopenhauer y su repercusión en la epistemología Signos Filosóficos. (S. Filosóficos, Ed.) *Redalyc.org Red de Revistas de América Latina, el Caribe, España y Portugal, Vol. XIX* (Núm. 38), 62-89. Obtenido de <http://www.redalyc.org/articulo.oa?id=34353146002>
- Sommerville, I. (2011). Ingeniería de Software. México: Pearson Educación México. Obtenido de https://sistemamid.com/panel/uploads/biblioteca/2018-06-11_03-37-12144643.pdf

- Storage Networking Industry Association - SNIA. (2021). What is Data Protection? USA. Obtenido de <https://www.snia.org/education/what-is-data-protection>
- Tamburri, D. (2020). Design principles for the General Data Protection Regulation (GDPR): A formal concept analysis and its evaluation. (T. U. Eindhoven, Ed.) *Information Systems*, Vol. 91, 1-14. <https://doi.org/https://doi.org/10.1016/j.is.2019.101469>
- Tocancipa, A. (01 de enero de 1976). Teoría del Control. *Boletín de Matemáticas*, Vol. X, 28-47. Obtenido de <https://revistas.unal.edu.co/index.php/bolma/article/view/34818>
- Torres, M. (2015). DLP: Prevención de Fuga de Información (Data Loss Prevention). (U. P. Colombia, Ed.) Colombia. Obtenido de <http://polux.unipiloto.edu.co:8080/00002325.pdf>
- Tujab, J. (2017). Fuga de información ministerial; procedimientos de detección y enlace de responsables. (U. R. Landívar, Ed.) Guatemala. Obtenido de <http://recursosbiblio.url.edu.gt/tesiseortiz/2017/07/03/Tujab-Jelderzon.pdf>
- Van, J. (2008). Teoría General de Sistemas. México: Editorial Trillas. Obtenido de <https://etikhe.files.wordpress.com/2013/10/306-lectura3-2.pdf>

ANEXOS

Anexo 1: Matriz de Consistencia

TÍTULO: Incidencia de la tecnología Data Loss Prevention en la Prevención de Fuga de Datos en un gobierno regional, Lima 2022.							
AUTOR: Olivares Zevallos, Jorge William							
PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES E INDICADORES				
<p>Problema principal: ¿De qué manera Data Loss Prevention incide en prevención de fuga de datos en un gobierno regional, Lima 2022?</p> <p>Problemas específicos: PE1: ¿De qué manera Data Loss Prevention incide en la dimensión de previene datos en uso de prevención de fuga de datos en un gobierno regional, Lima 2022?</p> <p>PE2: ¿De qué manera Data Loss Prevention incide en la dimensión de previene datos en movimiento de la</p>	<p>Objetivo principal: Determinar la incidencia de Data Loss Prevention en la prevención de fuga de datos en un gobierno regional, Lima 2022.</p> <p>Objetivos específicos: OE1: Determinar la incidencia de Data Loss Prevention en la dimensión de previene datos en uso de prevención de fuga de datos en un gobierno regional, Lima 2022.</p> <p>OE2: Determinar la incidencia de Data Loss Prevention en la dimensión de previene datos en movimiento de prevención</p>	<p>Hipótesis principal: Data Loss Prevention incide significativamente en la prevención de fuga de datos en un gobierno regional, Lima 2022.</p> <p>Hipótesis específicas: HE1: Data Loss Prevention incide significativamente la dimensión de previene datos en uso de la prevención de fuga de datos en un gobierno regional, Lima 2022.</p> <p>HE2: Data Loss Prevention incide significativamente la dimensión de previene datos en movimiento de prevención de fuga de</p>	Variable - 1: Data Loss Prevention				
			Dimensiones	Indicadores	Ítems	Niveles	
			Descubrimiento	Identificación	1-2	Óptimo Medio No óptimo	
				Clasificación	3-4		
				Trazabilidad	5-6		
			Prevención	Capacitación	7-8		
				Supervisión	9-10		
				Control de acceso	11-12		
			Protección	Monitoreo	13-14		
				Control de los repositorios	15-16		
				Confiability	17-18		
			Variable - 2: Prevención de fuga de datos				
			Dimensiones	Indicadores	Ítems	Niveles	
			Previene datos en uso	Monitoreo de actividades	19-20	Bueno Regular Malo	
Evaluar almacenamiento	21-22						
Detección de fuga	23-24						
Previene datos en movimiento	Análisis de tráfico de red	25-26					
	Monitoreo de violaciones	27-28					

TÍTULO: Incidencia de la tecnología Data Loss Prevention en la Prevención de Fuga de Datos en un gobierno regional, Lima 2022.						
AUTOR: Olivares Zevallos, Jorge William						
PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES E INDICADORES			
prevención de fuga de datos en un gobierno regional, Lima 2022? PE3: ¿De qué manera Data Loss Prevention incide en la dimensión de previene datos en reposo de prevención de fuga de datos en un gobierno regional, Lima 2022?	de fuga de datos en un gobierno regional, Lima 2022. OE3: Determinar la incidencia de Data Loss Prevention en la dimensión de previene datos en reposo de prevención de fuga de datos en un gobierno regional, Lima 2022.	datos en un gobierno regional, Lima 2022. HE3: Data Loss Prevention incide significativamente la dimensión de previene datos en reposo de prevención de fuga de datos en un gobierno regional, Lima 2022.		Salida de datos no autorizada	29-30	
			Previene datos en reposo	Monitoreo de los activos	31-32	
				Retención	33-34	
				Cifrado de datos	35-36	

Metodología

TIPO Y DISEÑO	POBLACIÓN Y MUESTRA	TÉCNICAS E INSTRUMENTOS	ESTADÍSTICA POR UTILIZAR
Tipo: Básica Diseño: No Experimental, Transversal, Correlacional-causal.	Población: 65 colaboradores de un gobierno regional Tamaño de muestra: 56 colaboradores de un gobierno regional Muestreo: No probabilístico intencional - dirigido	Técnicas: Encuesta Instrumentos: Cuestionario	Descriptiva: Se utilizó para describir e interpretar los datos alzados en forma ordenada, mediante el uso de histogramas y tablas con la información, a través de una hoja electrónica y el programa estadístico. Inferencial: Se utilizó para realizar el análisis estadístico no paramétrico, las tablas cruzadas de las variables con coeficientes de regresión logística ordinal para confirmar la validez de la hipótesis general y específicas; para ello, se validaron: valor de significancia, Chi-cuadrado-Pearson, Pseudo R Cuadrado de Nagelkerke y la estimación de los parámetros para la prueba de Wald.

Anexo 2: Matriz de Operacionalización de Variables

TÍTULO: Incidencia de la tecnología Data Loss Prevention en la Prevención de Fuga de Datos en un Gobierno Regional, Lima 2022.					
AUTOR: Olivares Zevallos, Jorge William					
Variables	Dimensiones	Indicadores	No.	Ítems (Preguntas)	Niveles
Variable - 1: Data Loss Prevention Sánchez (2015) indica que Data Loss Prevention se trata de una solución que permite a las instituciones disponer del descubrimiento, prevención y protección de su información sensible.	Descubrimiento Serna (2017), epistemológicamente se trata del hallazgo de información para luego realizar la justificación del conocimiento sistematizándolo, para su posterior uso técnico, tanto para el resultado final de una investigación como para el proceso mediante el cual se descubrió dicho resultado.	Identificación	1	¿Los datos de la institución deben protegerse?	Óptimo Medio No óptimo
			2	¿Le parece que los datos están identificados?	
		Clasificación	3	¿Los datos sensibles deben estar clasificados?	
			4	¿Considera que los datos sensibles están clasificados?	
		Trazabilidad	5	¿Se debe tener una adecuada autenticación y autorización para acceder a los datos sensibles?	
			6	¿Considera que se debe tener una trazabilidad en el acceso a los datos sensibles?	
	Prevención Bunga y Rahadiyan (2020) indican que consiste en describir varios medios de control mediante la creación de políticas de procedimientos y de organización, técnicas de control e incluir la participación de los empleados.	Capacitación	7	¿Todos los usuarios de la institución deben estar capacitados en el uso de los datos?	
			8	¿Considera que las capacitaciones son útiles para los servidores públicos de la institución?	
		Supervisión	9	¿Para que los datos no sufran alteraciones se debe tener una adecuada detección?	
			10	¿Considera que se deben cumplir las políticas de seguridad de la información de la institución?	
		Control de acceso	11	¿Sólo los usuarios autorizados deben acceder a los datos sensibles?	
			12	¿Se deben controlar todos los dispositivos mediante los cuales se utilizan los datos sensibles?	

TÍTULO: Incidencia de la tecnología Data Loss Prevention en la Prevención de Fuga de Datos en un Gobierno Regional, Lima 2022.

AUTOR: Olivares Zevallos, Jorge William

Variables	Dimensiones	Indicadores	No.	Ítems (Preguntas)	Niveles
	Protección ICO.ORG Information Commissioner's Office (2018) que define que, la protección es el uso justo y adecuado de la información sobre las personas. Asimismo, refiere que la protección de datos es fundamental para la innovación. Las buenas prácticas en la protección de datos son vitales para garantizar la confianza del público, el compromiso y el apoyo a los usos innovadores de los datos tanto en el sector público como en el privado.	Monitoreo	13	¿El acceso a los datos sensibles debe ser ininterrumpido?	
			14	¿Se deben controlar las acciones que se realizan con los datos sensibles?	
		Control de los repositorios	15	¿Los dispositivos de almacenamiento de los datos sensibles deben estar protegidos?	
			16	¿Considera que debería haber una concientización del control de los dispositivos de almacenamiento?	
		Confiabilidad	17	¿Debe existir confiabilidad de los datos sensibles?	
			18	¿Considera que se deben asegurar la accesibilidad y disponibilidad, integridad, confidencialidad y responsabilidad en el tratamiento de los datos sensibles?	
Variable – 2: Prevención de Fuga de Datos Patrizio y Kranz (2021), refiere que la prevención de fuga de datos es una estrategia para evitar	Previene datos en uso Fitzgibbons (2019) que son datos que un sistema está actualizando, procesando, borrando, accediendo o leyendo. Este tipo de datos no se almacenan pasivamente, sino que se mueven activamente a través de partes de una infraestructura de TI.	Monitoreo de actividades	19	¿Se deben monitorear las actividades que se realizan con los datos sensibles?	
			20	¿Considera que las actividades que realiza con los datos sensibles son las correctas?	
		Evaluar almacenamiento	21	¿Se debe evaluar el almacenamiento de los datos sensibles?	
			22	¿Considera que se debe controlar la transferencia de datos sensibles entre usuarios?	

TÍTULO: Incidencia de la tecnología Data Loss Prevention en la Prevención de Fuga de Datos en un Gobierno Regional, Lima 2022.

AUTOR: Olivares Zevallos, Jorge William

Variables	Dimensiones	Indicadores	No.	Ítems (Preguntas)	Niveles
que los clientes o usuarios accedan a datos sensibles que no necesitan, garantizando que el personal no la envíe fuera de la red de la institución de manera accidental o maliciosamente por una infiltración, principalmente de hackers informáticos, mientras están en uso (acciones de terminales), en movimiento (tráfico de red) y en reposo (almacenamiento de datos).		Detección de fuga	23	¿Se deben reportar las fugas de datos sensibles?	Bueno Regular Malo
			24	¿Considera que se debe tener visibilidad del procesamiento de los datos sensibles?	
	Previene datos en movimiento Allen (2016) que nos dice que los datos en movimiento se encuentran en su punto más vulnerable y es donde se deben centrar la atención de la protección porque es donde lidiamos con errores humanos, fallas en la red, intercambio de archivos inseguro, acciones maliciosas entre otras.	Análisis de tráfico de red	25	¿Se debe analizar por dónde y a dónde se dirigen los datos sensibles a través de la red interna o externa?	
			26	¿Considera que de esta manera se asegura el correcto uso de las políticas de seguridad de la información?	
		Monitoreo de violaciones	27	¿Se deben monitorear las posibles violaciones de las políticas de seguridad de la información?	
			28	¿Considera que las violaciones de estas políticas se realizan por errores humanos en el tratamiento y uso de los datos sensibles?	
		Salida de datos no autorizada	29	¿Se debe realizar un seguimiento cuando se realiza una salida no autorizada de datos sensibles?	
			30	¿Considera que la salvaguarda de los datos sensibles es importante para mitigar la salida de datos sensibles?	
	Previene datos en reposo Froehlich (2020) menciona que, para proteger mejor los datos en reposo, las organizaciones deben saber dónde residen todos los datos confidenciales y cómo clasificarlos. Las empresas	Monitoreo de los activos	31	¿Se deben monitorear dónde se almacenan los datos sensibles?	
			32	¿Considera que se tienen inventariados todos los activos de almacenamiento?	
		Retención	33	¿Se debe tener un mínimo de privilegio para evitar la fuga de datos sensibles?	

TÍTULO: Incidencia de la tecnología Data Loss Prevention en la Prevención de Fuga de Datos en un Gobierno Regional, Lima 2022.

AUTOR: Olivares Zevallos, Jorge William

Variables	Dimensiones	Indicadores	No.	Ítems (Preguntas)	Niveles
	necesitan procesos para limitar las ubicaciones donde se almacenan los datos confidenciales, pero eso no puede suceder si no pueden identificar adecuadamente la naturaleza crítica de sus datos.		34	¿Considera que se debe prevenir la divulgación no intencional de los datos sensibles?	
			35	¿A través del cifrado de los datos sensibles se evita la difusión de estos?	
		Cifrado de datos	36	¿Al detectarse una posible fuga de datos sensibles se debe denegar el acceso y/o borrarlo del dispositivo remoto?	

Anexo 3: Instrumento de Recolección de Datos

Cuestionario para usuarios del gobierno regional

Fecha: [/ /]

Edad: []

Sexo: Femenino [] Masculino []

Ocupación: F1 [] F3 [] F6 [] CAS [] Nombrado [] SP [] Tercero []

Grado de estudio: Secundaria [] Superior Técnica [] Superior Universitaria [] Posgrado []

Gerencia o Subgerencia: Gerencia [] Contratos [] Operaciones [] Promociones []

Instrucciones: Marque con un aspa la respuesta que crea conveniente teniendo en consideración el puntaje que corresponda de acuerdo con el siguiente **ejemplo:** Totalmente en desacuerdo (1), En desacuerdo (2), Ni de acuerdo ni en desacuerdo (3), De acuerdo (4) y Totalmente de acuerdo (5).

N°	Pregunta	Valoración				
		1	2	3	4	5
Sobre Data Loss Prevention						
1	¿Los datos de la institución deben protegerse?	Totalmente en desacuerdo	Parcialmente en desacuerdo	Indiferente	Parcialmente de acuerdo	Totalmente de acuerdo
2	¿Le parece que los datos están identificados?	No observado	Nunca	Ocasionalmente	Generalmente	Siempre
3	¿Los datos sensibles deben estar clasificados?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
4	¿Considera que los datos sensibles están clasificados?	Muy Raramente	Raramente	Ocasionalmente	Frecuentemente	Muy Frecuentemente
5	¿Se debe tener una adecuada autenticación y autorización para acceder a los datos sensibles?	No conozco en lo absoluto	Conozco vagamente	Indeciso	Conozco lo suficiente	Conozco totalmente
6	¿Considera que se debe tener una trazabilidad en el acceso a los datos sensibles?	Nada precisos	Poco precisos	Indeciso	Bastante precisos	Totalmente precisos
7	¿Todos los usuarios de la institución deben estar capacitados en el uso de los datos?	Nunca	Raramente	Ocasionalmente	Frecuentemente	Muy frecuentemente
8	¿Considera que las capacitaciones son útiles para los servidores públicos de la institución?	Nada útil	Poco útil	Algo útil	Útil	Muy útil
9	¿Para que los datos no sufran alteraciones se debe tener una adecuada detección?	Totalmente en desacuerdo	Parcialmente en desacuerdo	Indiferente	Parcialmente de acuerdo	Totalmente de acuerdo
10	¿Considera que se deben cumplir las políticas de seguridad de la información de la institución?	Muy negativo	Negativo	Neutral	Positivo	Muy positivo
11	¿Sólo los usuarios autorizados deben acceder a los datos sensibles?	Nunca	En ocasiones	Regularmente	Usualmente	Siempre
12	¿Se deben controlar todos los dispositivos mediante los cuales se utilizan los datos sensibles?	Totalmente descontrolado	Descontrolado	Neutral	Controlado	Totalmente controlado
13	¿El acceso a los datos sensibles debe ser ininterrumpido?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
14	¿Se deben controlar las acciones que se realizan con los datos sensibles?	Totalmente descontrolado	Descontrolado	Neutral	Controlado	Totalmente controlado
15	¿Los dispositivos de almacenamiento de los datos sensibles deben estar protegidos?	Nunca	Raramente	Ocasionalmente	Frecuentemente	Muy frecuentemente
16	¿Considera que debería haber una concientización del control de los dispositivos de almacenamiento?	Sin importancia	De poca importancia	Indeciso	Importante	Muy importante
17	¿Debe existir confiabilidad de los datos sensibles?	Nunca	Raramente	Indeciso	Frecuentemente	Muy frecuentemente
18	¿Considera que se deben asegurar la accesibilidad y disponibilidad, integridad, confidencialidad y responsabilidad en el tratamiento de los datos sensibles?	Definitivamente no	Probablemente no	Indeciso	Probablemente si	Definitivamente si

N°	Pregunta	Valoración				
		1	2	3	4	5
Sobre Prevención de fuga de Datos						
19	¿Se deben monitorear las actividades que se realizan con los datos sensibles?	Nunca	Raramente	Indeciso	Frecuentemente	Muy frecuentemente
20	¿Considera que las actividades que realiza con los datos sensibles son las correctas?	Muy poco frecuentemente	Poco frecuentemente	Indeciso	Frecuente	Muy frecuente
21	¿Se debe evaluar el almacenamiento de los datos sensibles?	Nunca	Raramente	Indeciso	Frecuentemente	Muy frecuentemente
22	¿Considera que se debe controlar la transferencia de datos sensibles entre usuarios?	Totalmente descontrolado	Descontrolado	Neutral	Controlado	Totalmente controlado
23	¿Se deben reportar las fugas de datos sensibles?	Nunca	Raramente	Indeciso	Frecuentemente	Muy frecuentemente
24	¿Considera que se debe tener visibilidad del procesamiento de los datos sensibles?	No conozco en lo absoluto	Conozco vagamente	Indeciso	Conozco lo suficiente	Conozco totalmente
25	¿Se debe analizar por dónde y a dónde se dirigen los datos sensibles a través de la red interna o externa?	Nunca	Raramente	Indeciso	Frecuentemente	Muy frecuentemente
26	¿Considera que de esta manera se asegura el correcto uso de las políticas de seguridad de la información?	No conozco en lo absoluto	Conozco vagamente	Indeciso	Conozco lo suficiente	Conozco totalmente
27	¿Se deben monitorear las posibles violaciones de las políticas de seguridad de la información?	No observado	Nunca	Ocasionalmente	Generalmente	Siempre
28	¿Considera que las violaciones de estas políticas se realizan por errores humanos en el tratamiento y uso de los datos sensibles?	Nunca	Raramente	Indeciso	Frecuentemente	Muy frecuentemente
29	¿Se debe realizar un seguimiento cuando se realiza una salida no autorizada de datos sensibles?	Totalmente en desacuerdo	En desacuerdo	Indiferente	De acuerdo	Totalmente de acuerdo
30	¿Considera que la salvaguarda de los datos sensibles es importante para mitigar la salida de datos sensibles?	Totalmente en desacuerdo	En desacuerdo	Indiferente	De acuerdo	Totalmente de acuerdo
31	¿Se deben monitorear dónde se almacenan los datos sensibles?	Nunca	Raramente	Indeciso	Frecuentemente	Muy frecuentemente
32	¿Considera que se tienen inventariados todos los activos de almacenamiento?	Nunca	Raramente	Indeciso	Generalmente	Siempre
33	¿Se debe tener un mínimo de privilegio para evitar la fuga de datos sensibles?	Totalmente en desacuerdo	En desacuerdo	Indiferente	De acuerdo	Totalmente de acuerdo
34	¿Considera que se debe prevenir la divulgación no intencional de los datos sensibles?	Nunca	Raramente	Indeciso	Frecuentemente	Muy frecuentemente
35	¿A través del cifrado de los datos sensibles se evita la difusión de estos?	Nunca	Raramente	Indeciso	Frecuentemente	Muy frecuentemente
36	¿Al detectarse una posible fuga de datos sensibles se debe denegar el acceso y/o borrarlo del dispositivo remoto?	No se toma en cuenta	Poco importante	Medianamente importante	Sumamente importante	Indispensable

¡Gracias por su tiempo!

Anexo 4: Certificado de Validación del Instrumento de Recolección de Datos

Validación del Experto N°1



CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LA VARIABLE: DATA LOSS PREVENTION

N°	DIMENSIONES / ítems	Pertinencia ¹		Relevancia ²		Claridad ³		Sugerencias
		SI	No	SI	No	SI	No	
DIMENSIÓN 1: DESCUBRIMIENTO								
1	¿Los datos de la institución deben protegerse?	X		X		X		
2	¿Le parece que los datos están identificados?	X		X		X		
3	¿Los datos sensibles deben estar clasificados?	X		X		X		
4	¿Considera que los datos sensibles están clasificados?	X		X		X		
5	¿Se debe tener una adecuada autenticación y autenticación para acceder a los datos sensibles?	X		X		X		
6	¿Considera que se debe tener una trazabilidad en el acceso a los datos sensibles?	X		X		X		
DIMENSIÓN 2: PREVENCIÓN								
7	¿Todos los usuarios de la institución deben estar capacitados en el uso de los datos?	X		X		X		
8	¿Considera que las capacitaciones son útiles para los servidores públicos de la institución?	X		X		X		
9	¿Para que los datos no sufran alteraciones se debe tener una adecuada detección?	X		X		X		
10	¿Considera que se deben cumplir las políticas de seguridad de la información de la institución?	X		X		X		
11	¿Sólo los usuarios autorizados deben acceder a los datos sensibles?	X		X		X		
12	¿Se deben controlar todos los dispositivos mediante los cuales se utilizan los datos sensibles?	X		X		X		
DIMENSIÓN 3: PROTECCIÓN								
13	¿El acceso a los datos sensibles debe ser ininterrumpido?	X		X		X		
14	¿Se deben controlar las acciones que se realizan con los datos sensibles?	X		X		X		
15	¿Los dispositivos de almacenamiento de los datos sensibles deben estar protegidos?	X		X		X		
16	¿Considera que debería haber una concientización del control de los dispositivos de almacenamiento?	X		X		X		
17	¿Debe existir confiabilidad de los datos sensibles?	X		X		X		
18	¿Considera que se deben asegurar la accesibilidad y disponibilidad, integridad, confidencialidad y responsabilidad en el tratamiento de los datos sensibles?	X		X		X		



CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LA VARIABLE: PREVENCIÓN DE FUGA DE DATOS

N°	DIMENSIONES / ítems	Pertinencia ¹		Relevancia ²		Claridad ³		Sugerencias
		SI	No	SI	No	SI	No	
DIMENSIÓN 1: PREVIENE DATOS EN USO								
19	¿Se deben monitorear las actividades que se realizan con los datos sensibles?	X		X		X		
20	¿Considera que las actividades que realiza con los datos sensibles son las correctas?	X		X		X		
21	¿Se debe evaluar el almacenamiento de los datos sensibles?	X		X		X		
22	¿Considera que se debe controlar la transferencia de datos sensibles entre usuarios?	X		X		X		
23	¿Se deben reportar las fugas de datos sensibles?	X		X		X		
24	¿Considera que se debe tener visibilidad del procesamiento de los datos sensibles?	X		X		X		
DIMENSIÓN 2: PREVIENE DATOS EN MOVIMIENTO								
25	¿Se debe analizar por dónde y a dónde se dirigen los datos sensibles a través de la red interna o externa?	X		X		X		
26	¿Considera que de esta manera se asegura el correcto uso de las políticas de seguridad de la información?	X		X		X		
27	¿Se deben monitorear las posibles violaciones de las políticas de seguridad de la información?	X		X		X		
28	¿Considera que las violaciones de estas políticas se realizan por errores humanos en el tratamiento y uso de los datos sensibles?	X		X		X		
29	¿Se debe realizar un seguimiento cuando se realiza una salida no autorizada de datos sensibles?	X		X		X		
30	¿Considera que la salvaguarda de los datos sensibles es importante para mitigar la salida de datos sensibles?	X		X		X		
DIMENSIÓN 3: PREVIENE DATOS EN REPOSO								
31	¿Se deben monitorear dónde se almacenan los datos sensibles?	X		X		X		
32	¿Considera que se tienen inventariados todos los activos de almacenamiento?	X		X		X		
33	¿Se debe tener un mínimo de privilegio para evitar la fuga de datos sensibles?	X		X		X		
34	¿Considera que se debe prevenir la divulgación no intencional de los datos sensibles?	X		X		X		
35	¿A través del cifrado de los datos sensibles se evita la difusión de los mismos?	X		X		X		
36	¿Al detectarse una posible fuga de datos sensibles se debe denegar el acceso y/o borrarlo del dispositivo remoto?	X		X		X		

Observaciones (preclarificar si hay suficiencia): _____

✓ Opinión de aplicabilidad: Aplicable [x] Aplicable después de corregir [] No aplicable []

Apellidos y nombres del juez validador: RAMIREZ PACHECO, LUIS ENRIQUE..... DNI:09468263.....

Especialidad del validador: Estadístico.....

¹Pertinencia: El ítem corresponde al concepto teórico formulado.

²Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo.

³Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo.

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión.


Firma del Experto Informante.
Mg. Luis RAMIREZ PACHECO
Especialidad

**PERÚ**

Ministerio de Educación

Superintendencia Nacional de
Educación Superior UniversitariaDirección de Documentación e
Información Universitaria y
Registro de Grados y Títulos**REGISTRO NACIONAL DE GRADOS ACADÉMICOS Y TÍTULOS PROFESIONALES**

Graduado	Grado o Título	Institución
RAMIREZ PACHECO, LUIS ENRIQUE DNI 09468263	BACHILLER EN INGENIERIA DE SISTEMAS Fecha de diploma: 02/04/2002 Modalidad de estudios: - Fecha matrícula: Sin información (***) Fecha egreso: Sin información (***)	UNIVERSIDAD NACIONAL FEDERICO VILLARREAL <i>PERU</i>
RAMIREZ PACHECO, LUIS ENRIQUE DNI 09468263	INGENIERO DE SISTEMAS E INFORMATICA Fecha de diploma: 17/06/2005 Modalidad de estudios: -	UNIVERSIDAD ALAS PERUANAS S.A. <i>PERU</i>
RAMIREZ PACHECO, LUIS ENRIQUE DNI 09468263	MAGISTER EN DOCENCIA UNIVERSITARIA Y GESTION EDUCATIVA Fecha de diploma: 12/04/2012 Modalidad de estudios: - Fecha matrícula: Sin información (***) Fecha egreso: Sin información (***)	UNIVERSIDAD SAN PEDRO <i>PERU</i>

Validación del Experto N°2



CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LA VARIABLE: DATA LOSS PREVENTION

N°	DIMENSIONES / ítems	Pertinencia ¹		Relevancia ²		Claridad ³		Sugerencias
		Si	No	Si	No	Si	No	
DIMENSIÓN 1: DESCUBRIMIENTO								
1	¿Los datos de la institución deben protegerse?	X		X		X		
2	¿Le parece que los datos están identificados?	X		X		X		
3	¿Los datos sensibles deben estar clasificados?	X		X		X		
4	¿Considera que los datos sensibles están clasificados?	X		X		X		
5	¿Se debe tener una adecuada autenticación y autorización para acceder a los datos sensibles?	X		X		X		
6	¿Considera que se debe tener una trazabilidad en el acceso a los datos sensibles?	X		X		X		
DIMENSIÓN 2: PREVENCIÓN								
7	¿Todos los usuarios de la institución deben estar capacitados en el uso de los datos?	X		X		X		
8	¿Considera que las capacitaciones son útiles para los servidores públicos de la institución?	X		X		X		
9	¿Para que los datos no sufran alteraciones se debe tener una adecuada detección?	X		X		X		
10	¿Considera que se deben cumplir las políticas de seguridad de la información de la institución?	X		X		X		
11	¿Sólo los usuarios autorizados deben acceder a los datos sensibles?	X		X		X		
12	¿Se deben controlar todos los dispositivos mediante los cuales se utilizan los datos sensibles?	X		X		X		
DIMENSIÓN 3: PROTECCIÓN								
13	¿El acceso a los datos sensibles debe ser ininterrumpido?	X		X		X		
14	¿Se deben controlar las acciones que se realizan con los datos sensibles?	X		X		X		
15	¿Los dispositivos de almacenamiento de los datos sensibles deben estar protegidos?	X		X		X		
16	¿Considera que debería haber una concientización del control de los dispositivos de almacenamiento?	X		X		X		
17	¿Debe existir confiabilidad de los datos sensibles?	X		X		X		
18	¿Considera que se deben asegurar la accesibilidad y disponibilidad, integridad, confidencialidad y responsabilidad en el tratamiento de los datos sensibles?	X		X		X		



CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LA VARIABLE: PREVENCIÓN DE FUGA DE DATOS

N°	DIMENSIONES / ítems	Pertinencia ¹		Relevancia ²		Claridad ³		Sugerencias
		Si	No	Si	No	Si	No	
DIMENSIÓN 1: PREVIENE DATOS EN USO								
19	¿Se deben monitorear las actividades que se realizan con los datos sensibles?	X		X		X		
20	¿Considera que las actividades que realiza con los datos sensibles son las correctas?	X		X		X		
21	¿Se debe evaluar el almacenamiento de los datos sensibles?	X		X		X		
22	¿Considera que se debe controlar la transferencia de datos sensibles entre usuarios?	X		X		X		
23	¿Se deben reportar las fugas de datos sensibles?	X		X		X		
24	¿Considera que se debe tener visibilidad del procesamiento de los datos sensibles?	X		X		X		
DIMENSIÓN 2: PREVIENE DATOS EN MOVIMIENTO								
25	¿Se debe analizar por dónde y a dónde se dirigen los datos sensibles a través de la red interna o externa?	X		X		X		
26	¿Considera que de esta manera se asegura el correcto uso de las políticas de seguridad de la información?	X		X		X		
27	¿Se deben monitorear las posibles violaciones de las políticas de seguridad de la información?	X		X		X		
28	¿Considera que las violaciones de estas políticas se realizan por errores humanos en el tratamiento y uso de los datos sensibles?	X		X		X		
29	¿Se debe realizar un seguimiento cuando se realiza una salida no autorizada de datos sensibles?	X		X		X		
30	¿Considera que la salvaguarda de los datos sensibles es importante para mitigar la salida de datos sensibles?	X		X		X		
DIMENSIÓN 3: PREVIENE DATOS EN REPOSO								
31	¿Se deben monitorear dónde se almacenan los datos sensibles?	X		X		X		
32	¿Considera que se tienen inventariados todos los activos de almacenamiento?	X		X		X		
33	¿Se debe tener un mínimo de privilegio para evitar la fuga de datos sensibles?	X		X		X		
34	¿Considera que se debe prevenir la divulgación no intencional de los datos sensibles?	X		X		X		
35	¿A través del cifrado de los datos sensibles se evita la difusión de los mismos?	X		X		X		
36	¿Al detectarse una posible fuga de datos sensibles se debe denegar el acceso y/o borrarlos del dispositivo remoto?	X		X		X		

Observaciones (precisar si hay suficiencia): _____

Opinión de aplicabilidad: Aplicable Aplicable después de corregir No aplicable 30 de mayo del 2022


Apellidos y nombres del juez evaluador: Tejada Ruiz, Roberto Juan DNI: 17930425

Especialidad del validador: Metodólogo Temático

Grado: Maestro Doctor

¹Pertinencia: El ítem corresponde al concepto teórico formulado.
²Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo
³Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión


Ms. Roberto Juan Tejada Ruiz
INGENIERO INDUSTRIAL - C.I.P. 242352
 Firma del Experto Informante
 Especialidad

**PERÚ**

Ministerio de Educación

Superintendencia Nacional de
Educación Superior UniversitariaDirección de Documentación e
Información Universitaria y
Registro de Grados y Títulos**REGISTRO NACIONAL DE GRADOS ACADÉMICOS Y TÍTULOS PROFESIONALES**

Graduado	Grado o Título	Institución
TEJADA RUIZ, ROBERTO JUAN DNI 17930425	BACHILLER EN INGENIERIA INDUSTRIAL Fecha de diploma: Modalidad de estudios: - Fecha matrícula: Sin información (***) Fecha egreso: Sin información (***)	UNIVERSIDAD NACIONAL DE TRUJILLO <i>PERU</i>
TEJADA RUIZ, ROBERTO JUAN DNI 17930425	INGENIERO INDUSTRIAL Fecha de diploma: Modalidad de estudios: -	UNIVERSIDAD NACIONAL DE TRUJILLO <i>PERU</i>
TEJADA RUIZ, ROBERTO JUAN DNI 17930425	MAESTRO EN CIENCIAS DE LA EDUCACION CON MENCION EN GERENCIA EDUCATIVA ES TRATEGICA Fecha de diploma: 02/06/20 Modalidad de estudios: PRESENCIAL Fecha matrícula: 26/01/2004 Fecha egreso: 05/05/2006	UNIVERSIDAD NACIONAL PEDRO RÚÍZ GALLO <i>PERU</i>

Validación del Experto N°3



CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LA VARIABLE: DATA LOSS PREVENTION

N°	DIMENSIONES / Items	Pertinencia ¹		Relevancia ²		Claridad ³		Sugerencias
		Si	No	Si	No	Si	No	
DIMENSIÓN 1: DESCUBRIMIENTO								
1	¿Los datos de la institución deben protegerse?	X		X		X		
2	¿Le parece que los datos están identificados?	X		X		X		
3	¿Los datos sensibles deben estar clasificados?	X		X		X		
4	¿Considera que los datos sensibles están clasificados?	X		X		X		
5	¿Se debe tener una adecuada autenticación y autenticación para acceder a los datos sensibles?	X		X		X		
6	¿Considera que se debe tener una trazabilidad en el acceso a los datos sensibles?	X		X		X		
DIMENSIÓN 2: PREVENCIÓN								
7	¿Todos los usuarios de la institución deben estar capacitados en el uso de los datos?	X		X		X		
8	¿Considera que las capacitaciones son útiles para los servidores públicos de la institución?	X		X		X		
9	¿Para que los datos no sufran alteraciones se debe tener una adecuada detección?	X		X		X		
10	¿Considera que se deben cumplir las políticas de seguridad de la información de la institución?	X		X		X		
11	¿Sólo los usuarios autorizados deben acceder a los datos sensibles?	X		X		X		
12	¿Se deben controlar todos los dispositivos mediante los cuales se utilizan los datos sensibles?	X		X		X		
DIMENSIÓN 3: PROTECCIÓN								
13	¿El acceso a los datos sensibles debe ser ininterrumpido?	X		X		X		
14	¿Se deben controlar las acciones que se realizan con los datos sensibles?	X		X		X		
15	¿Los dispositivos de almacenamiento de los datos sensibles deben estar protegidos?	X		X		X		
16	¿Considera que debería haber una concientización del control de los dispositivos de almacenamiento?	X		X		X		
17	¿Debe existir confiabilidad de los datos sensibles?	X		X		X		
18	¿Considera que se deben asegurar la accesibilidad y disponibilidad, integridad, confidencialidad y responsabilidad en el tratamiento de los datos sensibles?	X		X		X		



CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LA VARIABLE: PREVENCIÓN DE FUGA DE DATOS

N°	DIMENSIONES / Items	Pertinencia ¹		Relevancia ²		Claridad ³		Sugerencias
		Si	No	Si	No	Si	No	
DIMENSIÓN 1: PREVIENE DATOS EN USO								
19	¿Se deben monitorear las actividades que se realizan con los datos sensibles?	X		X		X		
20	¿Considera que las actividades que realiza con los datos sensibles son las correctas?	X		X		X		
21	¿Se debe evaluar el almacenamiento de los datos sensibles?	X		X		X		
22	¿Considera que se debe controlar la transferencia de datos sensibles entre usuarios?	X		X		X		
23	¿Se deben reportar las fugas de datos sensibles?	X		X		X		
24	¿Considera que se debe tener visibilidad del procesamiento de los datos sensibles?	X		X		X		
DIMENSIÓN 2: PREVIENE DATOS EN MOVIMIENTO								
25	¿Se debe analizar por dónde y a dónde se dirigen los datos sensibles a través de la red interna o externa?	X		X		X		
26	¿Considera que de esta manera se asegura el correcto uso de las políticas de seguridad de la información?	X		X		X		
27	¿Se deben monitorear las posibles violaciones de las políticas de seguridad de la información?	X		X		X		
28	¿Considera que las violaciones de estas políticas se realizan por errores humanos en el tratamiento y uso de los datos sensibles?	X		X		X		
29	¿Se debe realizar un seguimiento cuando se realiza una salida no autorizada de datos sensibles?	X		X		X		
30	¿Considera que la salvaguarda de los datos sensibles es importante para mitigar la salida de datos sensibles?	X		X		X		
DIMENSIÓN 3: PREVIENE DATOS EN REPOSO								
31	¿Se deben monitorear dónde se almacenan los datos sensibles?	X		X		X		
32	¿Considera que se tienen inventariados todos los activos de almacenamiento?	X		X		X		
33	¿Se debe tener un mínimo de privilegio para evitar la fuga de datos sensibles?	X		X		X		
34	¿Considera que se debe prevenir la divulgación no intencional de los datos sensibles?	X		X		X		
35	¿A través del cifrado de los datos sensibles se evita la difusión de los mismos?	X		X		X		
36	¿Al detectarse una posible fuga de datos sensibles se debe denegar el acceso y/o borrarlos del dispositivo remoto?	X		X		X		

Observaciones (precisar si hay suficiencia): **Si hay suficiencia**

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [] No aplicable [] Lima, 30 de mayo del 2022

Apellidos y nombre s del juez evaluador: Matos Guerrero, Cesar David DNI: 10251980

Especialidad del validador: Metodológico [] Temático [X]

Grado: Maestro [X] Doctor []

¹Pertinencia: El ítem corresponde al concepto teórico formulado.
²Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo.
³Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo.

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión.

Firma del Experto Informante
Especialidad

**PERÚ**

Ministerio de Educación

Superintendencia Nacional de
Educación Superior UniversitariaDirección de Documentación e
Información Universitaria y
Registro de Grados y Títulos**REGISTRO NACIONAL DE GRADOS ACADÉMICOS Y TÍTULOS PROFESIONALES**

Graduado	Grado o Título	Institución
MATOS GUERRERO, CESAR DAVID DNI 10251980	BACHILLER EN INGENIERIA DE SISTEMAS Fecha de diploma: 16/07/2014 Modalidad de estudios: - Fecha matrícula: Sin información (***) Fecha egreso: Sin información (***)	UNIVERSIDAD NACIONAL FEDERICO VILLARREAL <i>PERU</i>
MATOS GUERRERO, CESAR DAVID DNI 10251980	MAESTRO EN GESTIÓN PÚBLICA Fecha de diploma: 12/03/18 Modalidad de estudios: PRESENCIAL Fecha matrícula: 01/04/2015 Fecha egreso: 05/02/2017	UNIVERSIDAD PRIVADA CÉSAR VALLEJO <i>PERU</i>

Anexo 5: Base de datos del Cuestionario para usuarios del gobierno regional

Encuesta	Edad	Sexo	Ocupación	Grado de Estudio	Gerencia O Subgerencia	V1																		V2																			
						D1						D2						D3						D1						D2						D3							
						I1	I2	I3	I4	I5	I6	I7	I8	I9	I10	I11	I12	I13	I14	I15	I16	I17	I18	I19	I20	I21	I22	I23	I24	I25	I26	I27	I28	I29	I30	I31	I32	I33	I34	I35	I36		
						1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36		
1	51	M	Tercero	Posgrado	Operaciones	5	4	5	5	4	4	5	4	4	4	4	5	4	5	5	5	4	4	5	4	4	5	4	4	4	5	4	4	4	5	4	4	5	4	5	4		
2	51	F	F3	Universitaria	Operaciones	5	5	4	4	4	4	5	4	4	4	5	4	5	5	5	5	4	4	4	4	5	5	5	5	4	4	5	4	5	5	5	4	5	4	4	5	5	
3	39	M	Tercero	Universitaria	Operaciones	4	5	4	5	4	4	5	5	5	4	5	5	5	5	4	4	4	4	5	5	4	5	4	4	5	4	5	4	5	4	5	4	4	4	4	5	5	
4	23	M	Tercero	Técnica	Operaciones	4	4	5	5	4	5	4	4	5	5	4	4	5	4	5	5	5	4	4	4	5	5	5	5	4	5	5	4	4	5	5	4	5	4	5	4	4	
5	32	M	CAS	Posgrado	Promociones	4	5	4	4	5	4	5	5	5	4	4	4	4	4	5	4	5	5	5	5	4	5	5	5	5	4	4	5	4	4	5	4	4	5	4	4	4	
6	43	F	CAS	Posgrado	Operaciones	5	5	4	5	5	5	4	5	5	5	4	4	5	4	4	4	5	5	4	5	4	4	4	4	4	5	5	5	5	4	4	5	5	4	4	4	5	4
7	55	F	Tercero	Posgrado	Contratos	4	5	4	5	4	4	5	5	4	4	4	4	4	4	5	5	5	5	4	4	4	5	4	5	5	4	4	5	4	5	5	4	5	5	4	5	5	4
8	41	M	Tercero	Posgrado	Operaciones	5	4	5	4	4	4	5	4	5	4	4	5	4	4	5	4	5	4	4	4	4	5	5	4	5	5	5	4	4	5	5	4	5	5	4	5	4	5
9	39	F	CAS	Posgrado	Promociones	5	4	4	5	4	4	4	5	5	5	4	4	4	5	4	4	4	4	5	5	5	4	5	5	4	4	5	5	4	4	4	5	4	5	5	5	5	
10	29	F	Tercero	Universitaria	Contratos	4	4	4	4	5	5	4	5	5	5	4	5	5	4	4	5	5	4	4	5	4	4	4	4	5	5	5	5	5	5	5	4	5	5	5	5	5	
11	32	M	CAS	Posgrado	Promociones	4	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	4	4	4	5	4	5	5	5	4	4	4	4	4	5	5	5	4	5	5	4
12	35	M	Tercero	Posgrado	Promociones	4	4	4	5	5	4	4	5	4	5	4	4	5	5	5	5	5	4	4	5	4	4	5	5	5	5	4	4	4	4	4	4	5	5	5	4	5	4
13	47	F	CAS	Posgrado	Contratos	4	5	4	5	5	5	4	4	4	4	4	5	4	4	4	4	4	5	5	4	5	4	5	5	5	5	4	5	5	4	4	4	4	4	4	5	4	4
14	45	F	CAS	Posgrado	Operaciones	5	4	5	4	4	5	4	4	5	5	4	4	4	4	4	5	5	4	4	4	4	4	4	5	4	4	5	4	4	5	4	4	4	4	5	5	4	4
15	55	F	SP	Universitaria	Promociones	5	5	4	4	5	4	5	5	5	4	5	4	4	4	4	4	4	4	4	5	4	4	5	4	5	5	4	5	5	4	4	4	5	5	4	5	5	4
16	30	F	Tercero	Universitaria	Gerencia	5	5	4	5	5	5	5	5	5	4	5	5	4	4	4	4	5	5	4	5	5	5	5	4	4	5	5	5	4	4	5	4	4	4	4	5	5	4
17	35	F	CAS	Posgrado	Promociones	4	4	5	5	4	5	4	5	5	5	5	5	5	4	4	4	5	5	5	5	4	4	4	4	5	5	4	5	5	5	5	5	5	5	4	5	5	
18	30	F	SP	Técnica	Contratos	4	4	4	4	5	4	4	5	5	4	5	5	5	4	5	4	5	4	4	5	4	4	4	4	5	5	5	5	4	5	5	4	4	4	4	5	5	
19	46	M	CAS	Posgrado	Promociones	4	5	4	5	4	5	4	5	4	4	5	4	5	5	5	4	5	5	4	4	5	5	4	4	5	5	4	4	5	5	4	4	5	5	5	5	5	
20	33	M	Tercero	Posgrado	Contratos	5	4	5	5	4	5	5	5	5	5	5	5	5	4	5	4	4	4	4	5	5	4	5	4	4	5	5	5	5	4	5	5	4	5	4	4	5	5
21	37	F	Tercero	Posgrado	Contratos	4	5	5	4	5	5	4	5	4	4	5	5	5	4	4	4	5	4	5	4	5	4	4	4	5	5	5	5	5	4	4	5	5	4	4	5	5	5

Encuesta	Edad	Sexo	Ocupación	Grado de Estudio	Gerencia O Subgerencia	V1																		V2																		
						D1						D2						D3						D1						D2						D3						
						I1	I2	I3	I4	I5	I6	I7	I8	I9	I1	I2	I3	I4	I5	I6	I7	I8	I9	I1	I2	I3	I4	I5	I6	I7	I8	I9										
						1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	
22	33	M	CAS	Posgrado	Operaciones	5	5	5	4	4	4	4	5	4	4	5	4	5	4	5	5	5	5	5	5	5	4	4	4	4	4	4	4	4	4	5	4	5	4	4	5	
23	63	F	Nombrado	Técnica	Operaciones	5	5	4	5	5	4	5	4	5	5	4	4	5	5	4	4	4	5	4	4	4	5	4	5	5	5	5	5	5	5	5	5	5	5	4	5	
24	45	F	F3	Universitaria	Gerencia	4	4	4	4	5	5	5	4	5	5	4	4	5	5	4	4	4	5	5	4	4	4	5	5	4	5	5	4	5	4	4	4	4	5	4	5	
25	34	M	Tercero	Posgrado	Contratos	3	4	4	4	4	3	3	3	4	4	3	3	3	3	3	4	3	4	4	4	3	4	3	4	3	4	3	3	4	3	3	3	3	3	3	3	
26	30	M	Tercero	Universitaria	Operaciones	3	4	4	3	4	3	4	3	3	4	3	4	4	4	3	4	3	4	4	3	3	3	3	4	3	3	4	3	3	3	3	3	4	4	3	3	
27	35	M	Tercero	Técnica	Operaciones	3	3	4	3	4	3	3	4	3	4	3	3	4	3	4	3	4	4	4	3	3	4	3	4	3	4	4	4	4	4	4	3	3	3	4	4	4
28	33	M	Tercero	Universitaria	Contratos	4	4	3	4	3	3	4	3	4	3	3	4	4	3	4	3	4	3	4	4	3	3	4	4	4	3	4	3	3	3	3	3	4	3	3	4	
29	26	M	Tercero	Técnica	Operaciones	4	3	3	4	4	3	4	4	3	3	3	3	4	4	4	3	3	4	3	3	4	3	3	4	5	4	4	5	5	5	3	4	3	4	3	3	
30	44	M	Tercero	Posgrado	Contratos	4	3	3	4	4	4	4	4	3	4	4	3	3	4	3	3	4	3	4	3	3	4	4	4	4	4	4	4	4	3	4	3	4	3	3	4	
31	32	T	Tercero	Universitaria	Contratos	4	4	4	3	4	3	3	3	3	3	3	3	4	4	4	3	3	4	4	4	4	4	3	3	4	4	4	4	3	3	3	3	4	4	3	3	
32	35	M	Tercero	Posgrado	Operaciones	3	3	3	3	3	3	4	4	4	4	4	4	4	3	3	3	4	3	4	3	3	4	3	3	4	3	3	3	3	3	3	4	4	4	3	3	
33	48	M	CAS	Posgrado	Contratos	4	4	4	3	4	3	3	4	3	3	4	4	3	4	3	3	3	4	3	3	4	4	4	3	3	3	3	3	4	4	3	4	3	4	4		
34	53	M	SP	Universitaria	Operaciones	3	4	4	3	4	4	3	4	4	3	3	3	3	4	3	3	4	4	3	3	3	3	4	3	4	3	3	4	3	3	4	3	4	3	3	3	
35	32	M	Tercero	Posgrado	Promociones	3	4	4	4	3	3	4	4	3	4	4	3	4	3	3	3	3	4	4	4	3	3	4	3	4	4	4	3	4	4	4	3	4	4	4	3	
36	43	M	Tercero	Posgrado	Operaciones	4	4	4	4	3	4	3	3	3	4	3	3	4	4	4	4	4	3	4	4	4	4	4	4	3	4	4	4	3	5	5	4	5	5	4		
37	67	M	CAS	Posgrado	Contratos	4	4	4	3	4	4	3	3	4	4	4	3	3	4	4	3	4	3	4	4	3	3	3	4	3	4	4	4	4	3	4	4	4	4	3	3	
38	20	F	Tercero	Secundaria	Gerencia	4	3	4	4	4	4	4	4	3	4	4	3	3	4	3	4	4	3	4	4	4	4	3	4	4	4	4	4	3	3	3	4	3	4	3		
39	36	F	Tercero	Posgrado	Promociones	4	4	4	3	3	3	4	3	4	4	3	4	3	4	4	4	4	3	4	3	4	4	3	3	3	4	4	3	3	4	3	3	4	3	4	3	
40	50	F	Tercero	Técnica	Operaciones	3	3	4	4	3	4	4	3	4	4	3	3	4	3	4	4	4	4	4	3	4	3	4	4	4	4	3	3	4	3	3	3	4	4	3	4	
41	51	F	CAS	Posgrado	Operaciones	3	4	4	4	3	4	4	3	3	3	3	3	3	3	4	3	4	4	3	4	3	3	4	4	3	3	4	4	4	4	4	4	4	3	3	3	
42	30	M	Tercero	Universitaria	Contratos	3	4	4	3	4	3	4	3	4	4	3	3	3	3	3	3	3	3	4	3	3	4	3	3	3	3	4	4	3	3	4	3	3	3	4		
43	25	M	Tercero	Universitaria	Contratos	3	4	3	4	4	4	4	3	3	4	4	3	3	3	3	3	3	3	4	3	3	3	4	3	4	4	5	4	4	4	3	3	4	3	3	3	
44	34	F	CAS	Universitaria	Promociones	4	3	4	3	3	4	4	3	4	4	4	4	3	3	3	4	4	4	4	4	4	3	3	3	4	4	3	4	4	4	3	3	4	4	4	3	

Encuesta	Edad	Sexo	Ocupación	Grado de Estudio	Gerencia O Subgerencia	V1																		V2																			
						D1						D2						D3						D1						D2						D3							
						I1	I2	I3	I4	I5	I6	I7	I8	I9	I10	I11	I12	I13	I14	I15	I16	I17	I18	I19	I20	I21	I22	I23	I24	I25	I26	I27	I28	I29	I30	I31	I32	I33	I34	I35	I36		
						1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36		
45	35	M	Tercero	Universitaria	Contratos	3	3	3	3	4	4	4	4	4	4	3	3	3	3	4	3	4	3	3	4	4	3	4	3	4	3	3	3	3	4	3	4	4	4	4	4		
46	49	F	CAS	Posgrado	Contratos	3	4	3	4	4	3	3	3	3	3	3	4	3	3	4	3	3	4	4	3	3	4	3	3	3	3	4	3	3	3	3	3	4	4	4	4	4	
47	33	M	CAS	Universitaria	Contratos	1	1	1	2	2	2	1	2	2	2	2	2	2	2	2	1	2	1	1	1	2	1	2	2	1	1	1	1	1	1	1	1	2	1	2	1	1	
48	27	M	CAS	Universitaria	Contratos	1	2	1	1	2	1	2	1	1	2	2	2	1	2	1	2	2	2	2	2	1	2	1	1	2	2	1	1	1	2	2	1	1	1	2	1	1	
49	30	F	CAS	Universitaria	Contratos	2	2	1	1	2	2	1	1	2	2	2	2	2	2	1	2	2	1	2	1	2	2	1	1	2	1	1	2	1	1	2	1	1	2	2	2	2	
50	32	F	CAS	Universitaria	Contratos	1	2	2	1	2	1	2	2	2	1	1	2	1	2	2	1	2	2	1	2	2	2	2	1	2	2	1	2	1	2	2	1	2	2	1	2	2	
51	36	M	Tercero	Posgrado	Contratos	1	2	1	2	2	2	1	2	2	2	1	2	2	2	2	2	2	2	2	2	1	1	2	2	2	1	2	2	2	1	2	2	1	1	1	1	2	
52	39	M	CAS	Universitaria	Contratos	2	1	1	2	2	2	1	1	1	1	1	2	1	1	2	2	1	2	1	1	2	1	1	2	2	2	2	1	2	1	2	1	2	1	1	2	2	
53	50	F	CAS	Universitaria	Contratos	1	2	1	1	1	2	1	2	1	1	1	2	2	2	1	2	1	2	1	1	2	2	1	1	2	1	1	1	1	1	1	2	1	1	1	1	1	
54	45	F	CAS	Posgrado	Contratos	1	2	2	2	2	1	1	1	1	1	2	1	2	1	2	1	1	1	1	1	1	1	2	2	2	2	2	2	2	1	1	2	1	1	2	1	2	2
55	38	M	Tercero	Universitaria	Contratos	1	1	1	1	1	2	1	1	2	1	2	2	2	1	2	1	1	1	1	1	1	2	1	2	2	1	1	1	2	1	1	2	2	2	2	2	2	
56	49	F	SP	Universitaria	Gerencia	1	2	1	2	2	2	1	2	2	1	1	2	1	2	2	1	2	2	1	2	2	2	1	2	2	2	2	2	1	2	2	2	2	1	1	1	1	

Arbol de problemas del gobierno regional

Incidencia de la tecnología Data Loss Prevention en la prevención la fuga de datos en un gobierno regional

Pérdida de confidencialidad

Incumplimiento del objetivo principal de la institución que es mejorar el servicio al ciudadano

Pérdida de disponibilidad

Problema general

¿De qué manera Data Loss Prevention incide en prevención de fuga de datos en un gobierno regional?

Implementación del SGS - ISO
NTP/IEC 27001:2014

Prevención de fuga de datos en
las instituciones estatales

Plan de Continuidad Operativa en
las instituciones estatales

Riesgos inminentes
de confidencialidad

Acceso a datos
sensibles

Prevención de
ataques

Riesgos inminentes
de integridad

Copia de datos al
Google Drive

Recuperación
ante ataques

Riesgos inminentes
de disponibilidad

Descarga de data
no autorizada

Restauración de
los servicios



UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

**PROGRAMA DE MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN
TECNOLOGÍAS DE LA INFORMACIÓN**

Declaratoria de Autenticidad del Asesor

Yo, CARDEÑA PEÑA JORGE MANUEL, docente de la ESCUELA DE POSGRADO de la escuela profesional de MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "Incidencia de la tecnología data loss prevention en la prevención de fuga de datos en un gobierno regional, Lima 2022", cuyo autor es OLIVARES ZEVALLOS JORGE WILLIAM, constato que la investigación tiene un índice de similitud de 15.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha

sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

Apellidos y Nombres del Asesor:	Firma
CARDEÑA PEÑA JORGE MANUEL : 09340727 ORCID: 0000-0003-3176-8613	Firmado electrónicamente por: JCARDENAP el 09- 08-2022 19:23:03

Código documento Trilce: INV - 0881165