Universidad Nacional José Faustino Sánchez Carrión

Escuela de Posgrado

La seguridad de la informacion y su relación con la cultura informatica de los colaboradores en el Gobierno Regional de Lima, 2023

Tesis

Para optar el Grado Académico de Maestro en Gestión Pública

Autor

Wilfredo Javier Lino Quiche

Asesor

Dr. César Armando Díaz Valladares

Huacho – Perú

2026

UNIVERSIDAD NACIONAL
JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

LICENCIADA

(Resolución de Consejo Directivo N° 012-2020-SUNEDU/CD de fecha 27/01/2020

Escuela de Posgrado

METADATOS

DATOS DEL AUTOR (ES):		
APELLIDOS Y NOMBRES	**DNI**	**FECHA DE SUSTENTACIÓN**
Lino Quiche, Wilfredo Javier	46943984	22/07/2026
DATOS DEL ASESOR:		
APELLIDOS Y NOMBRES	**DNI**	**CÓDIGO ORCID**
Díaz Valladares, César Armando	15689062	https://orcid.org/0000-0002-4718-237X
DATOS DE LOS MIEMBROS DE JURADOS – PREGRADO/POSGRADO-MAESTRÍA-DOCTORADO:		
APELLIDOS Y NOMBRES	**DNI**	**CÓDIGO ORCID**
Garivay Torres, Flor de Maria	15587359	https://orcid.org/0000-0002-2051-4901
Huerta Hidalgo, Wilmer	46038002	https://orcid.org/0000-0002-8772-8672
León Sánchez, Carlos Manuel	41199839	https://orcid.org/0000-0003-0730-5504

Wilfredo Javier Lino Quiche 2025-076946

LA SEGURIDAD DE LA INFORMACION Y SU RELACION CON LA CULTURA INFORMATICA DE LOS COLABORADORES EN EL ...

Quick Submit

Quick Submit

DGI_Tesis Posgrado 2025

Detalles del documento

Identificador de la entrega
trn:oid:::1:3450269940

Fecha de entrega
23 dic 2025, 8:48 a.m. GMT-5

Fecha de descarga
23 dic 2025, 8:52 a.m. GMT-5

Nombre del archivo
TESIS_-JLQ.pdf

Tamaño del archivo
1.5 MB

67 páginas

16.500 palabras

72.031 caracteres

20% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Exclusiones

- N.° de coincidencias excluidas

Fuentes principales

19% Fuentes de Internet
7% Publicaciones
7% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.° de alertas de integridad para revisión

No se han detectado manipulaciones de texto sospechosas.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

DEDICATORIA:

Quiero dar las gracias a Dios y a mi familia por su apoyo incondicional durante esta etapa tan importante de mi vida.

También dar las gracias a mis asesores por su ayuda y apoyo durante la realización de este trabajo autofinanciado por mi persona.

AGRADECIMIENTO:

A mis grandes maestros de Posgrado que me inculcaron la pasión por la formación y el emprenndimiento.

Wilfredo Javier

ÍNDICE

DEDICATORIA: v
AGRADECIMIENTO: vi
INDICE vii
INDICE DE TABLAS ix
INDICE DE FIGURAS x
RESUMEN xi
ABSTRACT xii
INTRODUCCIÓN xiii
Capítulo I PLANTEAMIENTO DEL PROBLEMA 15
1.1 Descripción de la realidad problemática 11
1.2 Formulación del problema 14
1.3 Objetivos de la investigación 19
1.3.1. Objetivo general. 19
1.3.2. Objetivo específico. 19
1.4 Justificación de la investigación 19
1.5 Delimitaciones del estudio 16
Capítulo II MARCO TEÓRICO 21
2.1 Antecedentes de la investigación 21
2.1.1 Investigaciones internacionales 21
2.1.2 Investigaciones nacionales 22
2.2 Bases teóricas 23
2.3 Definición de términos básicos 33
2.4 Hipótesis de investigación 36
2.4.1 Hipótesis general 36
2.4.2 Hipótesis específicas 36
2.5 Matriz de operacionalización de variables 36
Capítulo III METODOLOGÍA 39
3.1 Diseño 39
3.2 Población y muestra 39
3.2.1 Población 39
3.2.2 Muestra 36

3.3 Técnicas de recolección de datos 36
3.4 Técnicas de procesamiento de datos 36
Capítulo IV ANALISIS DE LOS RESULTADOS 41
4.1. Análisis de los resultados 41
4.2. Generalización entorno la hipótesis central 46
CAPITULO V DISCUSIÓN 54
5.1. Discusión de los resultados 54
Capitulo VI CONCLUSIONES Y RECOMENDACIONES 573
6.1. Conclusiones 573
6.2. Recomendaciones 584
REFERENCIAS 55
ANEXOS 617
Instrumento: Seguridad de Información 617
Matriz de datos 651

ÍNDICE DE TABLAS

Tabla 1. Seguridad de la información..... .41
Tabla 2. Confidencialidad..... .42
Tabla 3. Integridad.....443
Tabla 4. Disponibilidad 444
Tabla 5. Cultura informática.....455
Tabla 6. Seguridad de la información y la cultura informática 466
Tabla 7. La integridad de la seguridad de la información y la cultura informática.....488
Tabla 8. La confidencialidad de la seguridad de la información y la cultura informática 50
Tabla 9. La disponibilidad de la seguridad de la información y la cultura informática 52

ÍNDICE DE FIGURAS

Figura 1. Seguridad de la información 41
Figura 2. Confidencialidad 42
Figura 3. Integridad 43
Figura 4. Disponibilidad 444
Figura 5. Cultura informática 455
Figura 7. La integridad de la seguridad de la información y la cultura informática 51
Figura 8. La confidencialidad de la seguridad de la información y la cultura informática 53
Figura 9. La infraestructura y equipamiento y la vocación cristiana..... 534

RESUMEN

La investigación titulada: “La seguridad de la información y su vinculación con la cultura informática de los colaboradores en el Gobierno Regional de Lima, 2023”, fue desarrollada con el propósito de optar por el grado de Maestro en la Escuela de Posgrado de la UNJFSC – Huacho. Se enmarcó dentro de un enfoque metodológico básico, con un nivel descriptivo-correlacional. La hipótesis formulada planteó que existe una relación significativa entre la seguridad de la información y la cultura informática de los colaboradores del mencionado organismo durante el año 2023. La población y muestra del estudio estuvo conformada por 158 trabajadores. Para la recolección de datos se empleó un cuestionario como instrumento, cuyos resultados confirmaron la existencia de una relación estadísticamente significativa entre ambas variables en el contexto del Gobierno Regional de Lima.

La autora

Palabras clave**:** seguridad, información, cultura, informática, colaboradores.

ABSTRACT

The research, entitled "Information security and its relationship with the IT culture of employees in the Regional Government of Lima, 2023," was developed for the purpose of obtaining a Master's degree from the Graduate School of the UNJFSC - Huacho. It was framed within a basic methodological approach, with a descriptive-correlational level. The hypothesis formulated stated a significant relationship between information security and the IT culture of employees of the aforementioned organization during the year 2023. The study population and sample consisted of 158 employees. A questionnaire was used as a data collection instrument, the results of which confirmed the existence of a statistically significant relationship between both variables in the context of the Regional Government of Lima.

The author

Keywords: security, information, culture, IT, collaborators

INTRODUCCIÓN

La investigación aborda un tema de creciente relevancia en el ámbito organizacional y gubernamental: la seguridad de la información y su relación con la cultura informática de los colaboradores. En un contexto global caracterizado por el incremento de amenazas digitales, vulneraciones de datos y ataques cibernéticos, las instituciones públicas enfrentan el desafío no solo de fortalecer sus sistemas tecnológicos, sino también de fomentar una cultura organizacional que asegure el uso responsable y consciente de la información.

En este marco, el Capítulo I expone la descripción de la realidad problemática a nivel mundial, europeo, latinoamericano y nacional, contextualizando la situación específica del Gobierno Regional de Lima en el año 2023. Se plantea la pregunta de investigación, así como los objetivos general y específicos, que buscan determinar la relación entre la seguridad de la información —con énfasis en sus dimensiones de integridad, confidencialidad y disponibilidad— y la cultura informática de los colaboradores.

El Capítulo II desarrolla las bases teóricas y conceptuales que sustentan el estudio, revisando las principales definiciones de seguridad de la información y cultura informática, así como sus dimensiones. Asimismo, se incluyen antecedentes internacionales y nacionales que evidencian la importancia de comprender cómo los factores humanos y culturales inciden en la eficacia de las políticas y prácticas de seguridad institucional.

Posteriormente, el Capítulo III presenta el diseño metodológico adoptado. Se describe el tipo de investigación, la población y muestra seleccionada, así como los instrumentos aplicados para la recolección de datos y el procedimiento seguido en el análisis. La rigurosidad metodológica busca garantizar la validez y confiabilidad de los resultados obtenidos.

El Capítulo IV expone los resultados descriptivos y la contrastación de hipótesis. En este apartado se muestran las relaciones halladas entre la seguridad de la información y la cultura informática, interpretando los datos de manera objetiva y vinculándolos con los objetivos de investigación.

Finalmente, el Capítulo V desarrolla la discusión de los resultados, comparándolos con antecedentes nacionales e internacionales. A partir de esta reflexión, se formulan conclusiones y recomendaciones que buscan contribuir al fortalecimiento de la gestión de la seguridad de la información en el Gobierno Regional de Lima, resaltando la necesidad de integrar la cultura informática como eje estratégico para la sostenibilidad de las políticas de seguridad.

De esta manera, el estudio no solo pretende aportar evidencia empírica en el campo de la seguridad de la información, sino también ofrecer insumos para el diseño de estrategias formativas y organizacionales que fortalezcan la cultura informática de los colaboradores, elemento clave para mitigar riesgos y garantizar la protección de los activos informacionales en la gestión pública.

Capítulo I
PLANTEAMIENTO DEL PROBLEMA

1.1 Descripción de la realidad problemática

En el ámbito global, la seguridad de la información se ha convertido en una prioridad debido al crecimiento exponencial de los datos digitales y a la sofisticación de las ciberamenazas. Los gobiernos y las organizaciones enfrentan retos significativos en la protección de infraestructuras críticas, que incluyen bases de datos de ciudadanos, sistemas de salud y plataformas de gobernanza electrónica. A pesar de los avances tecnológicos, la falta de una cultura informática consolidada entre los colaboradores de los sectores público y privado sigue siendo un obstáculo. En muchos casos, los errores humanos, como el uso inadecuado de contraseñas o la falta de atención a los protocolos de seguridad, son responsables de vulnerabilidades que pueden ser explotadas por actores malintencionados.

Europa, conocida por su enfoque riguroso en la protección de datos gracias al Reglamento General de Protección de Datos (GDPR), enfrenta retos particulares en la armonización de estándares de seguridad en los diversos países miembros. Aunque la normativa europea fomenta un alto nivel de protección, muchas organizaciones gubernamentales aún carecen de personal capacitado que comprenda la importancia de la cultura informática y los riesgos asociados a la ciberseguridad. Además, la presión por implementar sistemas de gobernanza digital eficiente en un marco multicultural y multilingüe a menudo complica la adopción de protocolos estandarizados. Esto resalta la necesidad de una capacitación integral y constante de los colaboradores para reducir la brecha entre la política y la práctica.

En Latinoamérica, la problemática de la seguridad de la información está vinculada a la limitada inversión en infraestructura tecnológica y la baja alfabetización digital en la población general. En el sector gubernamental,

muchos colaboradores carecen de conocimientos básicos sobre ciberseguridad, lo que expone a los sistemas a riesgos significativos. Además, la región enfrenta desafíos adicionales como la corrupción, el subdesarrollo tecnológico y una cultura organizacional que muchas veces subestima la importancia de la información como un activo estratégico. Aunque algunos países han adoptado normativas específicas en materia de protección de datos, su implementación suele ser desigual y depende en gran medida de la capacitación y compromiso de los equipos humanos.

En el Perú, y particularmente en el Gobierno Regional de Lima, la seguridad de la información se ve afectada por múltiples factores estructurales y culturales. A pesar de los esfuerzos por digitalizar procesos administrativos y optimizar la gestión pública, la falta de una cultura informática sólida entre los colaboradores representa una barrera crítica. Muchos trabajadores no poseen los conocimientos necesarios para identificar amenazas cibernéticas o aplicar prácticas básicas de seguridad, como el manejo adecuado de contraseñas, el uso de dispositivos electrónicos personales en redes de trabajo y la gestión segura de datos sensibles. Asimismo, la escasez de recursos destinados a la capacitación y actualización tecnológica agrava la situación, dejando al sistema vulnerable a ataques externos y fallos internos.

Por lo tanto, abordar esta problemática requiere una estrategia integral que combine inversión en tecnología, desarrollo de capacidades humanas y promoción de una cultura organizacional orientada hacia la ciberseguridad. Solo a través de un enfoque conjunto será posible fortalecer la relación entre la seguridad de la información y la cultura informática en el Gobierno Regional de Lima, contribuyendo a un sistema más robusto, seguro y eficiente.

En el Gobierno Regional de Lima, la Oficina de Sistemas es el área encargada de la protección de la infraestructura y los dispositivos, encargado de

gestionar y coordinar todo lo referente a la seguridad de información de la entidad. Los eventos o incidentes de seguridad relacionados a la fuga de información son: por descuido, falta de conciencia, no tener el conocimiento apropiado, inconformidad de los funcionarios, no tener capacitaciones en los temas, por negligencia de las personas ya sea de forma accidental o premeditada ocasionando de esta manera numerosas amenazas.

La problemática de la seguridad de la información y su vínculo con la cultura informática en el Gobierno Regional de Lima surge de una convergencia de factores estructurales, tecnológicos y humanos. Una de las principales causas es la falta de capacitación adecuada de los colaboradores, quienes muchas veces carecen de los conocimientos y habilidades necesarias para manejar información de manera segura en un entorno digital. Esto se debe, en parte, a la ausencia de políticas públicas robustas orientadas a fomentar la alfabetización digital en las instituciones públicas.

Además, la infraestructura tecnológica en muchas dependencias gubernamentales es obsoleta, lo que limita la implementación de sistemas de seguridad modernos. La poca inversión en herramientas de ciberseguridad, junto con una cultura organizacional que subestima los riesgos asociados al manejo inadecuado de la información, refuerza esta problemática. Finalmente, la creciente digitalización de procesos administrativos y la falta de protocolos claros para el manejo de datos sensibles también contribuyen a la vulnerabilidad del sistema.

Las deficiencias en la seguridad de la información y en la cultura informática tienen repercusiones significativas tanto a nivel interno como externo. Internamente, la exposición a ciberataques puede provocar la pérdida o el robo de datos confidenciales, generando caos en los procesos administrativos y afectando la confianza de los colaboradores en los sistemas digitales. Esto impacta directamente en la eficiencia y la credibilidad de la institución.

Externamente, las brechas en la seguridad de la información pueden comprometer la privacidad de los ciudadanos, especialmente cuando se manejan datos personales sensibles. La divulgación no autorizada de esta información podría derivar en problemas legales, pérdida de confianza por parte de la población y daño a la reputación del Gobierno Regional. A nivel macro, estas vulnerabilidades también contribuyen al rezago tecnológico y a la percepción de ineficiencia del sector público, afectando la imagen del Perú en el contexto internacional.

Esta investigación busca proporcionar soluciones concretas para fortalecer la seguridad de la información en el Gobierno Regional de Lima mediante el desarrollo de una cultura informática sólida entre sus colaboradores. En primer lugar, ofrecerá un diagnóstico claro y fundamentado de las debilidades actuales en términos de ciberseguridad y manejo de información. Esto permitirá a las autoridades comprender las raíces del problema y priorizar las áreas de intervención.

En segundo lugar, se propondrán estrategias de capacitación y sensibilización para los colaboradores, orientadas no solo a transmitir conocimientos técnicos, sino también a generar conciencia sobre la importancia de la seguridad de la información como un activo institucional estratégico. Además, se sugerirán mejoras en los protocolos y políticas internas para el manejo seguro de datos, alineándolos con estándares internacionales.

Ante esta problemática se desea saber cuál es la relación que existe entre la seguridad de información y la cultura informática de los colaboradores del Gobierno Regional de Lima.

1.2 Formulación del problema

1.2.1. Problema general.

¿Cuál es la relación que existe entre la Seguridad de Información y la Cultura Informática de los colaboradores en el Gobierno Regional de Lima, en el año 2023?

1.2.2. Problema específico

¿Cuál es la relación que existe entre la integridad de la Seguridad de Información y la Cultura Informática?

¿Cuál es la relación que existe entre la confidencialidad de la Seguridad de Información y la Cultura Informática?

¿Cuál es la relación que existe entre la disponibilidad de la Seguridad de Información y la Cultura Informática?

1.3 Objetivos de la investigación

1.3.1. Objetivo general.

- ✓ Determinar la relación que existe entre la Seguridad de Información y la Cultura Informática de los colaboradores en el Gobierno Regional de Lima, en el año 2023.

1.3.2. Objetivo específico.

- ✓ Determinar la relación que existe entre la integridad de la Seguridad de Información y la Cultura Informática.
- ✓ Determinar la relación que existe entre la confidencialidad de la Seguridad de Información y la Cultura Informática.
- ✓ Determinar la relación que existe entre la disponibilidad de la Seguridad de Información y la Cultura Informática.

1.4 Justificación de la investigación

La investigación se justifica por la necesidad urgente de fortalecer la seguridad de la información en las instituciones públicas, dado el creciente riesgo de amenazas cibernéticas y filtraciones de datos. En el caso del Gobierno Regional de Lima, se

evidencia que gran parte de la vulnerabilidad institucional no proviene solo de limitaciones tecnológicas, sino de la baja cultura informática de sus colaboradores. Comprender la relación entre ambos factores permitirá identificar áreas críticas de mejora, proponer estrategias de capacitación y contribuir al desarrollo de una cultura organizacional orientada a la prevención, protección de datos y uso responsable de tecnologías. Este estudio no solo ofrece un diagnóstico pertinente, sino que también aporta insumos clave para la toma de decisiones y la formulación de políticas públicas orientadas a la modernización digital y la gestión segura de la información.

1.5 Delimitaciones del estudio

Delimitación espacial: Se desarrolló en el Gobierno Regional de Lima, específicamente en sus oficinas ubicadas en la ciudad de Huacho, donde laboran los colaboradores administrativos involucrados en el uso y gestión de información digital.

Delimitación temporal: Se realizó durante el año 2023, periodo en el cual se recogieron los datos, se aplicaron los instrumentos de evaluación y se analizaron los resultados en función del contexto institucional vigente.

Delimitación poblacional: La población estuvo conformada por los colaboradores administrativos del Gobierno Regional de Lima, quienes hacen uso frecuente de herramientas informáticas para el desempeño de sus funciones. La muestra fue seleccionada considerando criterios de acceso a la información digital, nivel jerárquico y participación en procesos institucionales que involucren el manejo de datos.

Delimitación temática: La investigación se centró exclusivamente en analizar la relación entre la seguridad de la información y la cultura informática de los colaboradores, dejando fuera otras variables tecnológicas como infraestructura, conectividad o sistemas operativos

Capítulo II
MARCO TEÓRICO

2.1 Antecedentes de la investigación

2.1.1 Investigaciones internacionales

En el año 2018, Álvarez desarrolló un estudio centrado en la gerencia y los desafíos que implica la seguridad de la información dentro de las organizaciones contemporáneas, con el objetivo de analizar la relación entre dichas variables. La investigación tuvo como población a los colaboradores de la empresa Gandalf Comunicaciones. En cuanto al enfoque metodológico, se optó por un diseño de tipo histórico-documental. Para la recolección de información se recurrió a la técnica de observación indirecta, basándose en el análisis de documentos, teorías y aportes de diversos autores especializados, mediante un tratamiento cualitativo. Por la naturaleza del estudio, no se consideró pertinente la aplicación de encuestas ni otros instrumentos cuantitativos, dado que el carácter de la investigación fue netamente documental e histórico.

Lavayen M. (2022) realizó un estudio titulado “Cultura informática y su incidencia en la economía del sector comercial en la ciudad de Guayaquil”, con el objetivo de analizar cómo el cambio en la cultura informática durante 2019-2020 influyó en la economía comercial local. El uso de plataformas tecnológicas permitió a muchas microempresas y PYMES continuar operando fuera de sus locales, evitando cierres y pérdida de empleos. La investigación, de enfoque mixto, aplicó encuestas a gerentes y dueños de negocios, concluyendo que la cultura informática tuvo un impacto positivo en la economía del sector comercial guayaquileño.

Gómez P. y Tomala K. (2017) desarrollaron el proyecto titulado “Análisis de la cultura digital e informática en los comerciantes adultos mayores del cantón Guayaquil, parroquia Bolívar”. La investigación se centró en estudiar la situación de los comerciantes en etapa adulta, con énfasis en cómo la cultura digital e informática incide en su desarrollo productivo. Se identificó que, especialmente en zonas rurales, existe un marcado analfabetismo digital, lo cual profundiza la brecha tecnológica y limita la participación de este grupo en la vida socioeconómica. El estudio resalta la exclusión digital como un obstáculo para el desarrollo comunitario y propone alternativas que favorezcan la inclusión y el crecimiento de esta población.

Valadez S., en su investigación titulada “Cultura informática para el maestro de educación básica en México”, tuvo como propósito elaborar un documento orientado a los docentes de este nivel, abordando temas sobre cultura y alfabetización digital. Concluyó que el dominio de herramientas informáticas, al igual que otros aprendizajes, se desarrolla progresivamente y con mayor eficacia cuando está vinculado a tareas significativas, como las funciones administrativas que los maestros realizan cotidianamente.

2.1.2 Investigaciones nacionales

Huaura, M. (2019) El estudio se centró en la gestión de riesgos de seguridad de la información en empresas del sector telecomunicaciones, con el objetivo de analizar la relación entre esta gestión y el control de riesgos. La investigación fue de tipo no experimental y descriptiva, teniendo como población a 104 trabajadores del sector en Lima Metropolitana, quienes también constituyeron la muestra por su accesibilidad. Se aplicó una encuesta de 10 ítems, diseñada por el investigador y validada por expertos. Los resultados permitieron concluir que una gestión de riesgos basada en la norma NTP ISO/IEC 31000 influye positivamente en el control de riesgos de seguridad de la información en dichas empresas.

Vásquez, E. (2018) La investigación abordó la implementación del sistema de gestión ISO 27001:2013 como mecanismo para proteger la información en los procesos de tecnología de la información (TI), teniendo como población a trabajadores del sector telecomunicaciones en Lima Metropolitana. Se enmarcó en una metodología de tipo descriptiva aplicada, orientada a analizar la influencia del sistema en un contexto real. Como conclusión, se determinó que la adopción del sistema ISO 27001:2013 permite resguardar eficazmente la información frente a diversas amenazas, asegurando el cumplimiento de los objetivos de seguridad y evitando sanciones derivadas de pérdidas de datos en los procesos TI.

Seclen J. (2017) El estudio abordó los factores que influyen en la implementación del Sistema de Gestión de Seguridad de la Información en entidades públicas peruanas, conforme a la norma NTP-ISO/IEC 27001. Su objetivo fue desarrollar una investigación cualitativa utilizando entrevistas como técnica principal para recopilar información de manera estructurada. A través de este enfoque, se buscó identificar tanto las limitaciones como las facilidades que enfrentan dichas entidades, con el fin de aportar insumos útiles para mejorar la aplicación de políticas de seguridad de la información en el marco del Sistema Nacional de Informática.

2.2 Bases teóricas

2.2.1 Seguridad de la información

Definiciones

La seguridad de la información comprende el conjunto de estrategias, políticas y acciones orientadas a preservar la confidencialidad, integridad y disponibilidad de los datos dentro de una organización, protegiéndolos frente a accesos no autorizados, pérdidas o alteraciones (González & Reyes, 2020).

La seguridad de la información no solo implica evitar amenazas, sino también detectar vulnerabilidades y aplicar medidas correctivas para garantizar la continuidad operativa y el resguardo de los activos digitales (Castañeda & León, 2020).

La seguridad de la información está estrechamente relacionada con la cultura organizacional, ya que su eficacia depende del compromiso de los usuarios, directivos y equipos técnicos en la aplicación de buenas prácticas y políticas institucionales (López & Espinoza, 2021).

Este concepto también incluye aspectos legales y normativos, como la protección de datos personales, la privacidad y el cumplimiento de regulaciones nacionales e internacionales relacionadas con el tratamiento de la información (Pérez & Chávez, 2019).

La seguridad de la información puede entenderse como una disciplina basada en la gestión de riesgos, donde se identifican amenazas, se evalúan impactos y se diseñan controles para reducir o eliminar los riesgos que afectan los sistemas informáticos (Ramírez & Pérez, 2019).

La protección de la información involucra medidas técnicas específicas aplicadas a hardware, software, redes y bases de datos, que permiten reducir vulnerabilidades y asegurar el funcionamiento adecuado de los sistemas (Ministerio de Tecnologías de la Información y las Comunicaciones, 2018).

Una adecuada gestión de la seguridad de la información fortalece la confianza de clientes, usuarios y colaboradores, al demostrar que los datos son tratados con responsabilidad, ética y apego a la normativa vigente (Contraloría General de la República del Perú, 2020).

El concepto se rige por estándares como la norma ISO/IEC 27001, que proporciona un marco sistemático para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información (AENOR, 2016).

Con el crecimiento de la transformación digital, la seguridad de la información ha cobrado mayor relevancia, ya que los datos son constantemente intercambiados y almacenados en la nube, lo que exige protocolos sólidos de protección (Martínez & Durán, 2020).

Además de las tecnologías, la seguridad de la información implica formar y sensibilizar al personal sobre el uso adecuado de los recursos digitales, ya que los errores humanos siguen siendo uno de los principales vectores de riesgo (Ruiz & Hernández, 2018).

Importancia de la seguridad de la información

La seguridad de la información es crucial en un entorno cada vez más digitalizado y dependiente de la tecnología. Su principal objetivo es salvaguardar la confidencialidad, integridad y disponibilidad de los datos, evitando accesos no autorizados, alteraciones indebidas o pérdidas de información crítica (González & Reyes, 2020). Esto resulta vital tanto para entidades públicas como privadas, ya que una filtración, un ciberataque o un fallo en los sistemas puede tener consecuencias económicas, legales y reputacionales graves.

Además, la seguridad de la información permite asegurar la continuidad del negocio, reduciendo riesgos operativos y minimizando el impacto de incidentes tecnológicos o humanos (Ramírez & Pérez, 2019). Esto es especialmente relevante en sectores como salud, banca, educación, telecomunicaciones y gobierno, donde la interrupción de servicios puede afectar directamente a miles de personas.

En el plano legal, también cumple un rol importante, ya que ayuda al cumplimiento de normativas de protección de datos, como la Ley de Protección de Datos Personales en Perú o el Reglamento General de Protección de Datos (GDPR) en Europa. No respetar estas normativas puede derivar en sanciones severas para las organizaciones (Pérez & Chávez, 2019).

Por otro lado, una adecuada seguridad de la información fortalece la confianza de clientes, usuarios y aliados estratégicos. Saber que los datos están bien protegidos promueve relaciones sostenibles y mejora la imagen institucional (Contraloría General de la República del Perú, 2020).

En suma, invertir en seguridad de la información no solo protege datos, sino que también protege a las personas, garantiza el cumplimiento normativo y aporta a la sostenibilidad y resiliencia de las organizaciones frente a un mundo cada vez más expuesto a riesgos digitales.

Dimensiones de la seguridad de la información

Confidencialidad

La confidencialidad se refiere a la capacidad de restringir el acceso a la información solo a personas, sistemas o procesos debidamente autorizados. Su propósito es evitar que datos sensibles sean expuestos, filtrados o utilizados por individuos no autorizados, lo cual podría comprometer la privacidad, la competitividad o la legalidad de una organización. La confidencialidad se garantiza mediante técnicas como el cifrado, el control de acceso y la autenticación de usuarios. Cuando esta dimensión se vulnera, los datos pueden caer en manos equivocadas, lo que conlleva sanciones legales, daños a la reputación institucional y pérdida de confianza (López & Espinoza, 2021).

Integridad

La integridad asegura que la información se mantenga exacta, coherente, completa y sin modificaciones no autorizadas durante su ciclo de vida. Esto implica que los datos no deben ser alterados de forma accidental o maliciosa desde su creación hasta su almacenamiento o transmisión. La alteración de un dato, por mínima que sea, puede generar errores en procesos críticos o decisiones equivocadas. Para proteger esta dimensión, se utilizan mecanismos como el control de versiones, registros de auditoría, funciones hash y copias de seguridad verificadas. La integridad es esencial para mantener la fiabilidad y la validez de la información que respalda las operaciones de una organización (González & Reyes, 2020).

Disponibilidad

La disponibilidad hace referencia a que la información y los sistemas que la gestionan estén siempre accesibles y operativos para los usuarios autorizados en el momento que se requiera. Esta dimensión busca evitar interrupciones o caídas de servicios que puedan afectar la productividad, la toma de decisiones o la continuidad del negocio. Para mantener la disponibilidad, se implementan planes de contingencia, redundancia de sistemas, respaldo de datos y mecanismos de recuperación ante desastres. Una baja disponibilidad puede resultar en pérdida de ingresos, insatisfacción del cliente y daño reputacional, especialmente en sectores como salud, finanzas o servicios públicos (Contraloría General de la República del Perú, 2020).

2.2.4 Cultura Informática

La cultura informática constituye un conjunto articulado de conocimientos técnicos, habilidades operativas, criterios éticos y actitudes críticas que permiten al individuo desenvolverse eficazmente en entornos digitales. Esta competencia se expresa no solo en el dominio de herramientas tecnológicas, sino también en la capacidad de proteger la información,

reconocer riesgos y adaptarse a nuevas tecnologías de forma consciente (Area Moreira, 2018).

Implica la incorporación significativa de las tecnologías de la información y comunicación en la vida cotidiana y laboral, entendidas no como instrumentos aislados, sino como parte de una cultura de gestión de la información. En este sentido, la cultura informática también refleja la forma en que las personas interactúan con los dispositivos, comprenden los entornos digitales y desarrollan estrategias seguras para el tratamiento de los datos (Cabero-Almenara & Llorente Cejudo, 2019).

Desde una visión integral, se entiende como el resultado de un proceso de alfabetización digital que ha superado la fase meramente instrumental, para centrarse en el uso reflexivo, ético y eficiente de la información. El dominio de la cultura informática permite al trabajador acceder a fuentes confiables, proteger los datos institucionales y mantener la integridad de los sistemas (Salinas Ibáñez, 2017).

No se trata únicamente de saber usar computadoras, sino de incorporar un pensamiento digital que incluya actitudes preventivas ante amenazas cibernéticas, el uso consciente de contraseñas, la protección de la identidad digital y el cumplimiento de normas institucionales vinculadas a la seguridad informática (Gutiérrez & Tyner, 2012).

En el ámbito institucional, la cultura informática se expresa en los hábitos colectivos, normas y valores que orientan el comportamiento de los colaboradores frente al uso de tecnologías. Aquellas organizaciones que promueven una cultura informática sólida logran reducir significativamente

los riesgos de seguridad de la información, fortalecer la eficiencia interna y consolidar una gestión basada en datos confiables (Martínez, 2020).

También se relaciona con la actitud del trabajador ante el cambio tecnológico: una cultura informática sólida permite a los empleados adaptarse a nuevas plataformas, identificar prácticas inadecuadas, y contribuir a una transición digital segura y ordenada en las organizaciones públicas y privadas (Silva Quiroz, 2016).

La cultura informática incorpora además los principios de ciudadanía digital y responsabilidad en el uso de las redes. En este sentido, se convierte en un componente fundamental de la formación profesional y del desempeño ético, especialmente en contextos donde la información representa un recurso estratégico (UNESCO, 2019).

Desde el enfoque de competencias, se articula con el desarrollo de habilidades digitales para resolver problemas, tomar decisiones basadas en datos, colaborar en entornos virtuales, y participar en procesos de innovación tecnológica. A mayor desarrollo de esta cultura, mayor es la capacidad del trabajador para actuar en entornos inciertos, con herramientas en constante evolución (Area Moreira & Pessoa, 2012).

La cultura informática también promueve la capacidad crítica para filtrar información, evitar la desinformación, proteger los datos personales y actuar de forma ética en entornos interconectados. No basta con acceder a la tecnología, sino con saber usarla de forma estratégica y responsable (González, 2018).

Finalmente, esta cultura se consolida cuando los individuos no solo consumen herramientas digitales, sino que comprenden sus alcances, evalúan

sus implicancias y se convierten en agentes activos en la construcción de entornos digitales seguros, productivos y participativos (Piscitelli, 2015).

Componentes de la cultura informática

Hablar de cultura informática implica comprender que no se trata simplemente del manejo técnico de una computadora, sino de una construcción más compleja que articula conocimientos, habilidades y actitudes que permiten al ser humano desenvolverse de manera efectiva, segura y ética en el entorno digital. En este proceso, se identifican tres componentes esenciales que dan forma y sentido a la cultura informática: el cognitivo, el procedimental y el actitudinal.

El primer componente, de naturaleza cognitiva, se relaciona con los saberes que el individuo posee sobre el funcionamiento de las tecnologías de la información. No basta con saber usar un programa: se requiere comprender las lógicas que rigen el mundo digital, como el rol del software y el hardware, el significado de la protección de datos, los riesgos vinculados a la exposición en línea, y los principios fundamentales de seguridad de la información. Es decir, el trabajador que conoce, por ejemplo, lo que implica el cifrado de datos o las consecuencias de una brecha de seguridad, está en mejores condiciones de tomar decisiones informadas y proteger adecuadamente la información institucional (Area Moreira, 2018).

Pero el conocimiento, por sí solo, no es suficiente. Es necesario que este se traduzca en habilidades concretas para operar herramientas y plataformas tecnológicas con destreza. Aquí aparece el componente procedimental, vinculado al saber hacer. Este aspecto se manifiesta en la capacidad de utilizar software de oficina, sistemas de gestión de documentos, correo institucional, almacenamiento en la nube, entre otros. La persona que posee una sólida competencia procedimental no solo ejecuta tareas digitales con eficiencia, sino que también es capaz de aplicar criterios de seguridad mínimos en su quehacer diario, como generar contraseñas robustas, identificar correos maliciosos o realizar copias de

respaldo de manera periódica.

No obstante, el eje más profundo y determinante de la cultura informática se encuentra en el componente actitudinal. Este se refiere a la conciencia crítica, la responsabilidad personal y la ética digital con la que se actúa en entornos informáticos. La actitud de un colaborador frente al uso de la información es lo que marca, en muchos casos, la diferencia entre una práctica segura y una riesgosa. Una persona puede tener conocimientos y habilidades, pero si no valora la importancia de proteger los datos o si actúa de manera negligente, toda la estructura informática institucional puede quedar expuesta. Por ello, fomentar la actitud preventiva, el respeto por la privacidad, la disposición al aprendizaje continuo y la adhesión a normativas institucionales es clave en la consolidación de una cultura digital sólida (Piscitelli, 2015; UNESCO, 2019).

En conjunto, estos tres componentes conforman un entramado indispensable para garantizar que los trabajadores públicos —como en el caso del Gobierno Regional de Lima— no solo utilicen la tecnología, sino que lo hagan con conciencia, responsabilidad y visión estratégica. La cultura informática no es estática ni mecánica; es una práctica viva, que se construye, se refuerza y se transforma en la medida en que las personas se comprometen con el entorno digital en el que operan.

Cultura informática como estrategia de modernización institucional

En la actualidad, el proceso de modernización institucional no puede concebirse sin la incorporación consciente y planificada de la cultura informática. Las entidades públicas enfrentan desafíos crecientes en términos de eficiencia, transparencia y seguridad, y para responder a ellos no basta con adquirir tecnología: se requiere una cultura organizacional que entienda, integre y valore el uso estratégico de las tecnologías de la información. En ese sentido, la cultura

informática se convierte en una herramienta clave para impulsar procesos de cambio estructural, mejorar la calidad del servicio público y fortalecer la gobernanza digital.

Cuando los colaboradores de una institución pública desarrollan una cultura informática sólida, son capaces de interactuar de forma eficiente con plataformas de gestión, manejar datos con criterios de seguridad y ética, y responder con flexibilidad a los cambios tecnológicos. Esta capacidad no solo optimiza los procesos internos, sino que también contribuye al cumplimiento de los principios de transparencia y acceso a la información que exigen los marcos legales modernos (Cabero-Almenara & Llorente Cejudo, 2019). Es decir, una cultura informática bien implementada no solo forma parte del soporte técnico de la organización, sino que se alinea con la misión institucional y fortalece su legitimidad frente a la ciudadanía.

Diversos estudios han demostrado que las instituciones que invierten en el desarrollo de competencias digitales y promueven una cultura informática participativa logran avanzar con mayor solidez hacia la digitalización de sus procesos administrativos (Area Moreira, 2018). Esto incluye desde la implementación de sistemas de gestión documental electrónica hasta el uso de plataformas interoperables entre entidades. Pero estos cambios solo son sostenibles si se acompañan de una transformación cultural, en la que los trabajadores internalicen prácticas digitales seguras, colaborativas y orientadas al bien común.

En contextos como el del Perú, donde muchos gobiernos regionales y locales aún enfrentan limitaciones en infraestructura tecnológica, el fortalecimiento de la cultura informática representa una vía estratégica para cerrar brechas institucionales. Más allá de los recursos físicos, lo que define el éxito de la modernización es la actitud del personal frente al cambio digital. Tal como advierte la UNESCO (2019), **la transformación institucional no se logra únicamente con herramientas, sino con personas que sepan usarlas de forma**

ética, crítica y eficiente.

Por ello, la cultura informática debe ser entendida no como un resultado final, sino como un proceso continuo de aprendizaje organizacional. Promover entornos donde se valore la capacitación constante, el intercambio de saberes y la construcción colectiva del conocimiento digital permitirá no solo enfrentar las amenazas del ciberespacio, sino también fortalecer la institucionalidad democrática desde el interior del aparato estatal (González, 2018).

En síntesis, incorporar la cultura informática como estrategia de modernización no solo mejora el desempeño funcional de las instituciones, sino que también transforma las relaciones laborales, empodera al trabajador público y promueve una gestión basada en datos, innovación y sostenibilidad. En el caso del Gobierno Regional de Lima, esto resulta fundamental para avanzar hacia una administración pública eficiente, segura y al servicio del ciudadano.

2.3 Definición de términos básicos

Seguridad de la información

Es el conjunto de procesos, políticas y herramientas orientadas a proteger los datos frente a accesos no autorizados, garantizando su confidencialidad, integridad y disponibilidad dentro de una organización (González & Reyes, 2020).

Gestión de riesgos

Consiste en identificar, analizar y controlar los riesgos que pueden comprometer los activos de información, con el fin de minimizar los impactos negativos y asegurar la continuidad operativa (Ramírez & Pérez, 2019).

Cultura informática

Hace referencia a los conocimientos, actitudes y competencias que tienen los

individuos sobre el uso adecuado, ético y seguro de las tecnologías digitales en distintos contextos, especialmente laborales y educativos (Soto, 2018).

Brecha digital

Es la desigualdad existente entre personas, regiones o sectores sociales en cuanto al acceso, uso efectivo y apropiación crítica de las tecnologías de la información y la comunicación (Gómez & Navarro, 2017).

Confidencialidad

Es la propiedad de la información que garantiza que solo las personas autorizadas pueden acceder a ella, evitando filtraciones o accesos indebidos (INEI, 2021).

Integridad

Se refiere a la exactitud y completitud de la información, asegurando que no haya sido alterada sin autorización durante su almacenamiento, procesamiento o transmisión (Ministerio de Tecnologías de la Información y las Comunicaciones, 2018).

Disponibilidad

Implica que los sistemas y la información estén accesibles para los usuarios autorizados cuando lo requieran, evitando interrupciones que afecten la productividad o los servicios (Contraloría General de la República del Perú, 2020).

Política de seguridad de la información

Es un documento normativo que define los lineamientos, roles y procedimientos necesarios para proteger los activos de información dentro de una organización (Pérez & Chávez, 2019).

Sistema de gestión de seguridad de la información (SGSI)

Conjunto de normas, políticas, procedimientos y recursos técnicos y humanos que permiten implementar, mantener y mejorar la seguridad de la información de

manera sistemática (López & Espinoza, 2021).

ISO/IEC 27001

Norma internacional que establece los requisitos para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información (AENOR, 2016).

Análisis de vulnerabilidades

Proceso técnico que identifica fallas o debilidades en los sistemas de información que podrían ser explotadas por amenazas internas o externas (Castañeda & León, 2020).

Phishing

Tipo de ataque informático que busca engañar al usuario para que revele información confidencial como contraseñas o datos bancarios mediante correos o sitios web falsificados (Ramos & Ugarte, 2022).

Control de acceso

Conjunto de mecanismos físicos o lógicos que regulan quién puede entrar a sistemas o consultar información, basado en privilegios y autenticación (Ruiz & Hernández, 2018).

Backup (copia de seguridad)

Es el proceso de duplicar datos críticos con el fin de recuperarlos en caso de pérdida, corrupción o ataque cibernético (Torres & Andrade, 2019).

Ciberseguridad

Área especializada de la seguridad informática que se ocupa de proteger redes, dispositivos, programas y datos contra ataques, daños o accesos no autorizados en entornos digitales (Martínez & Durán, 2020).

2.4 Hipótesis de investigación

2.4.1 Hipótesis general

Existe relación significativa de la Seguridad de Información y la Cultura Informática de los colaboradores en el Gobierno Regional de Lima, en el año 2023.

2.4.2 Hipótesis específicas

- ✓ Existe relación significativa de la integridad de la Seguridad de Información y la Cultura Informática.
- ✓ Existe relación significativa de la confidencialidad de la Seguridad de Información y la Cultura Informática.
- ✓ Existe relación significativa de la Seguridad de Información y la Cultura Informática

2.5 Matriz de operacionalización de variables

OPERACIONALIZACIÓN DE VARIABLES

VARIABLES	DEFINICIÓN CONCEPTUAL	DIMENSIONES	INDICADORES	ITEMS	Unidad de Medida	Escala de Medición
VARIABLE 1 **SEGURIDAD DE LA INFORMACION**	La seguridad de la información es el conjunto de medidas y técnicas utilizadas para controlar y salvaguardar todos los datos que se manejan dentro de la organización y asegurar que los datos no salgan del sistema que ha establecido la organización.	**Confidencialidad**	- Control de Acceso - Autenticación - Autorización	**1-9**	Cuestionario	Escala Likert: (5) Siempre (4) Casi siempre (3) Neutro (2) A veces (1) Nunca
		Integridad	- Seguridad de los procedimientos - Protección	**10-15**		
		Disponibilidad	- Acceso a la información	**16-18**		
VARIABLE 2 **CULTURA INFORMATICA**	La cultura informática es el conjunto de prácticas, formas y costumbres de interactuar con los recursos o herramientas tecnológicas, generando un cambio de transformación digital que, siendo utilizadas de manera	**Informacional**	- Procesos de transmisión - Acumulación y tratamiento de la información	**19-22**		
		Tecnológica	- Empleo de los sistemas de Procesamiento de la Información	**23-25**		

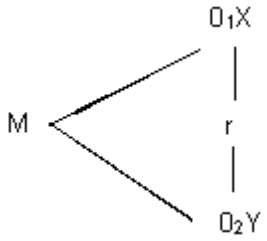
	adecuada, facilitan mejorar las actividades diarias de una sociedad.	**Sociocultural**	- La Percepción - Influencia de la Cultura	**26-30**		

Capítulo III
METODOLOGÍA

3.1 Diseño

Con un enfoque transversal, el estudio se enmarca dentro del diseño no experimental, ya que permite examinar simultáneamente la relación entre variables y describirlas en un solo momento temporal. Esta clase de investigaciones recopila información en un instante específico, asemejándose a una fotografía que captura una situación determinada (Hernández et al., 2010, p. 151).

Siendo su representación la siguiente gráfica:



Dónde:

M = muestra
01X = Observación sobre seguridad de información
02Y = Observación sobre cultura informática
r = Relación entre variables, coeficiente de correlación

Variable 1: seguridad de información (V1)

Variable 2: cultura informática (V2)

3.2 Población y muestra

3.2.1 Población

La muestra estuvo constituida por 158 trabajadores administrativos, tanto nombrados como contratados, pertenecientes al Gobierno Regional de Lima en el año 2022. Según Carrasco (2006), se entiende como muestra al grupo de personas que, al aceptar participar en el estudio, proporcionan la información necesaria para

alcanzar los resultados del trabajo e identificar posibles propuestas de mejora frente a la problemática abordada.

3.2.2 Muestra

Se optó por trabajar con toda la población debido a que su tamaño resulta manejable para el proceso de recolección de datos, facilitando el acceso por parte del investigador y contando con la disposición de los participantes para proporcionar la información requerida. Carrasco (2006) indica que, cuando se considera a la totalidad de los miembros de una población sin exclusión alguna, se está frente a un muestreo de tipo censal, el cual representa un subconjunto íntegro del grupo de estudio.

3.3 Técnicas de recolección de datos

La técnica aplicada fue la encuesta, la cual permitió establecer contacto directo con la población objetivo, haciendo uso de dos instrumentos para la recolección de información.

3.4 Técnicas de procesamiento de datos

En primer lugar, mediante la interpretación de cifras y porcentajes, se llevó a cabo un análisis descriptivo; seguido de ello, se procedió con el análisis inferencial, a través del cual fue posible deducir la complejidad de la problemática actual y considerar qué acciones deberían implementarse en el futuro inmediato para su mejora. Para la verificación de las hipótesis formuladas, se utilizó el estadígrafo conocido como la Correlación de Pearson.

Capítulo IV

ANALISIS DE LOS RESULTADOS

4.1. Análisis de los resultados

Tabla 1. Seguridad de la información

		Frecuencia	Porcentaje
Válido	Alto	73	46,2
	Bajo	6	3,8
	Medio	79	50,0
	Total	158	100,0

.

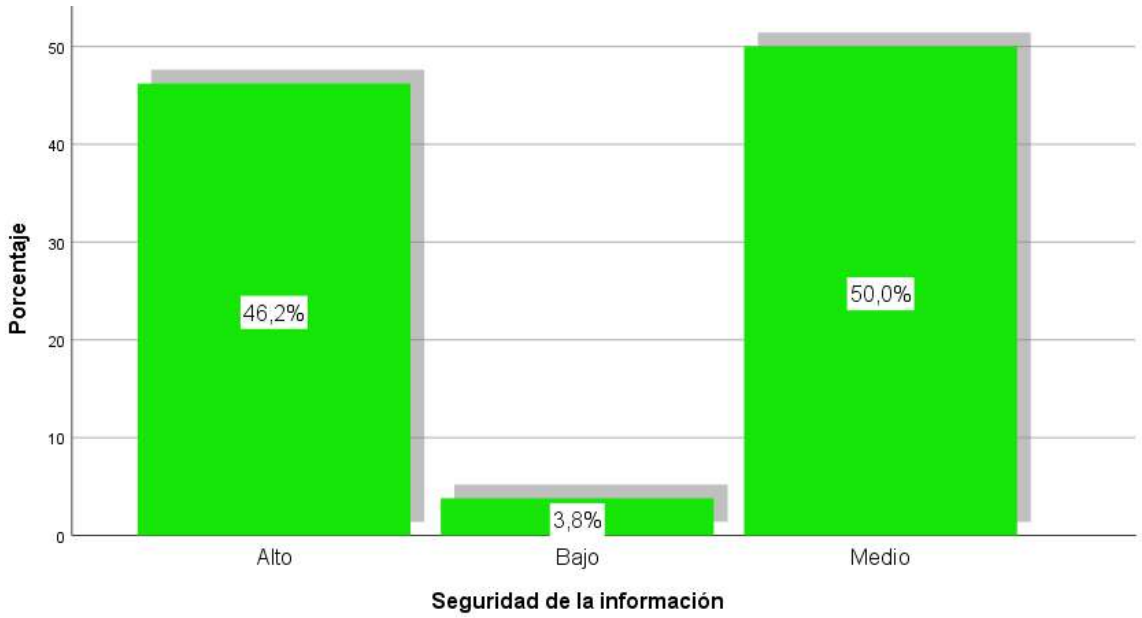


Figura 1. Seguridad de la información

En el año 2023, en el Gobierno Regional de Lima, el 50,0% de los colaboradores indicó haber alcanzado un nivel medio en la variable seguridad de la información; mientras que el 46,2% manifestó haber logrado un nivel alto y solo el 3,8% obtuvo un nivel bajo.

Tabla 2. Confidencialidad

		Frecuencia	Porcentaje
Válido	Alto	75	47,5
	Bajo	6	3,8
	Medio	77	48,7
	Total	158	100,0

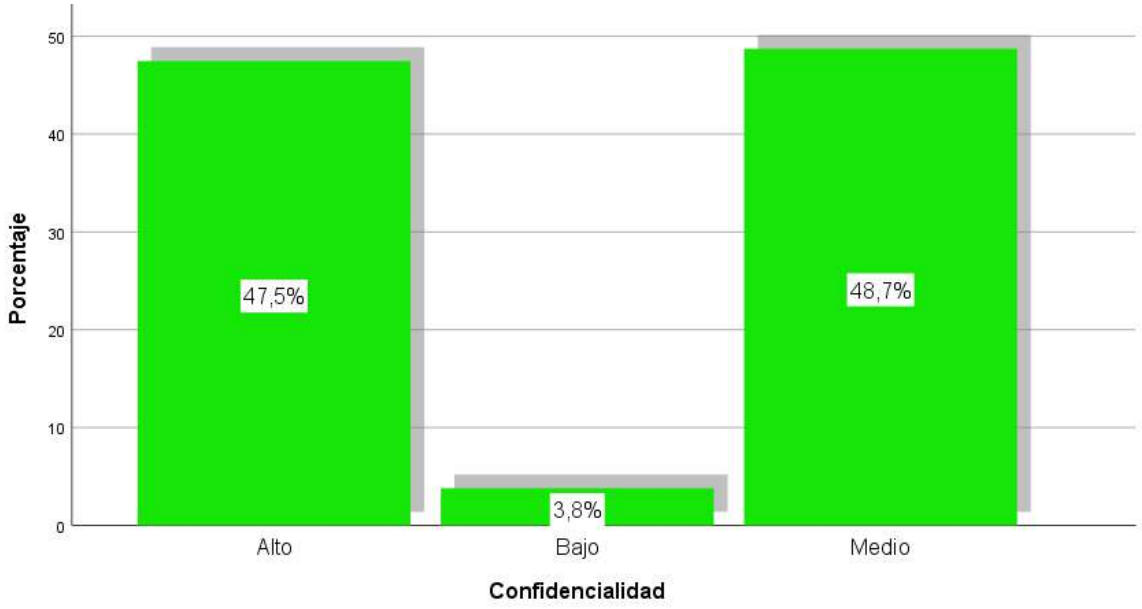


Figura 2. Confidencialidad

Durante el año 2023, en el Gobierno Regional de Lima, el 48,7% de los trabajadores manifestó haber alcanzado un nivel intermedio en cuanto a la dimensión de confidencialidad dentro de la seguridad de la información. Asimismo, un 47,5% indicó haber llegado a un nivel elevado, mientras que solo un 3,8% reportó haber obtenido un nivel bajo en dicha dimensión.

Tabla 3. Integridad.

		Frecuencia	Porcentaje
Válido	Alto	72	45,6
	Bajo	7	4,4
	Medio	79	50,0
	Total	158	100,0

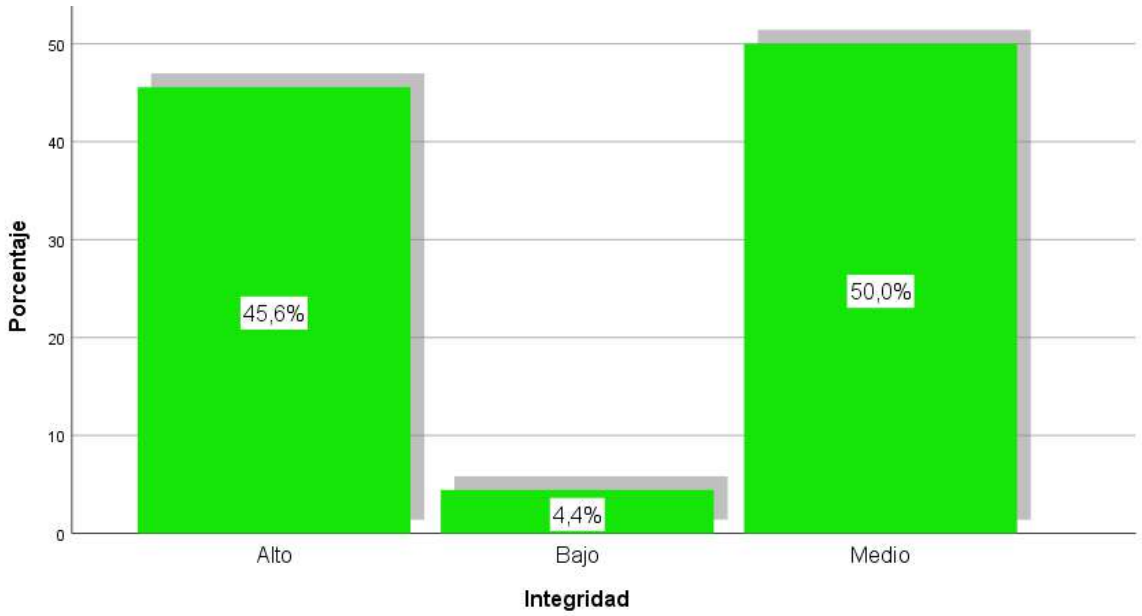


Figura 3. Integridad

En el Gobierno Regional de Lima, durante el año 2023, el 50,0% de los colaboradores indicó haber alcanzado un nivel intermedio en la dimensión integridad relacionada con la seguridad de la información. Por su parte, el 45,6% señaló haber logrado un nivel alto, mientras que un 4,4% manifestó haber obtenido un nivel bajo.

Tabla 4. Disponibilidad

		Frecuencia	Porcentaje
Válido	Alto	50	31,6
	Bajo	6	3,8
	Medio	102	64,6
	Total	158	100,0

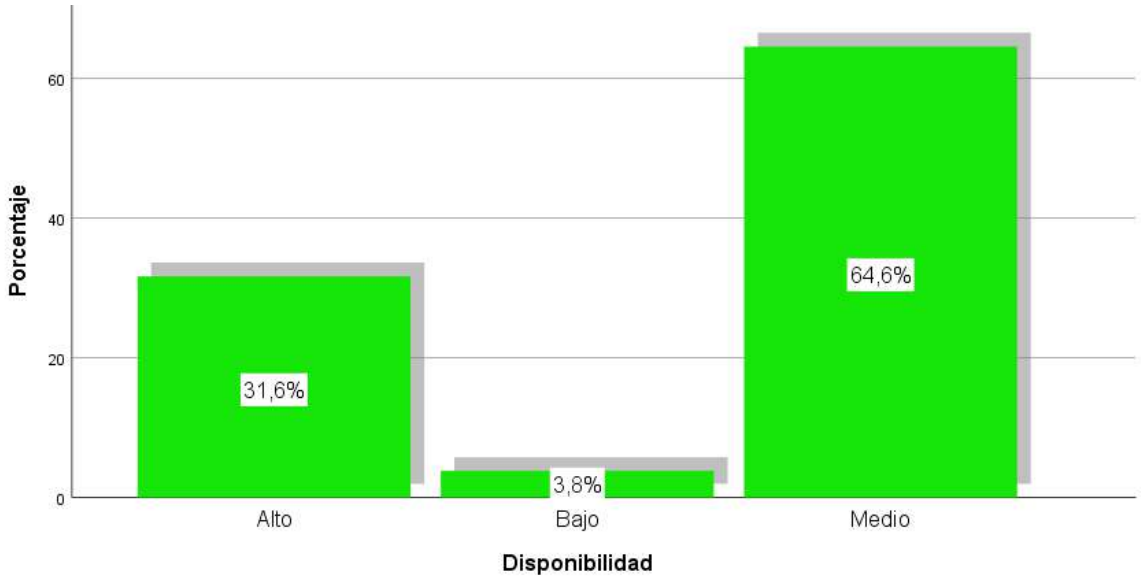


Figura 4. Disponibilidad

Durante el año 2023, en el Gobierno Regional de Lima, el 64,6% de los colaboradores afirmó haber alcanzado un nivel medio en la dimensión disponibilidad dentro del ámbito de la seguridad de la información. Asimismo, un 31,6% reportó un nivel alto, mientras que el 3,8% restante indicó haber obtenido un nivel bajo.

Tabla 5. Cultura informática

		Frecuencia	Porcentaje
Válido	Alto	59	37,3
	Bajo	7	4,4
	Medio	92	58,2
	Total	158	100,0

.

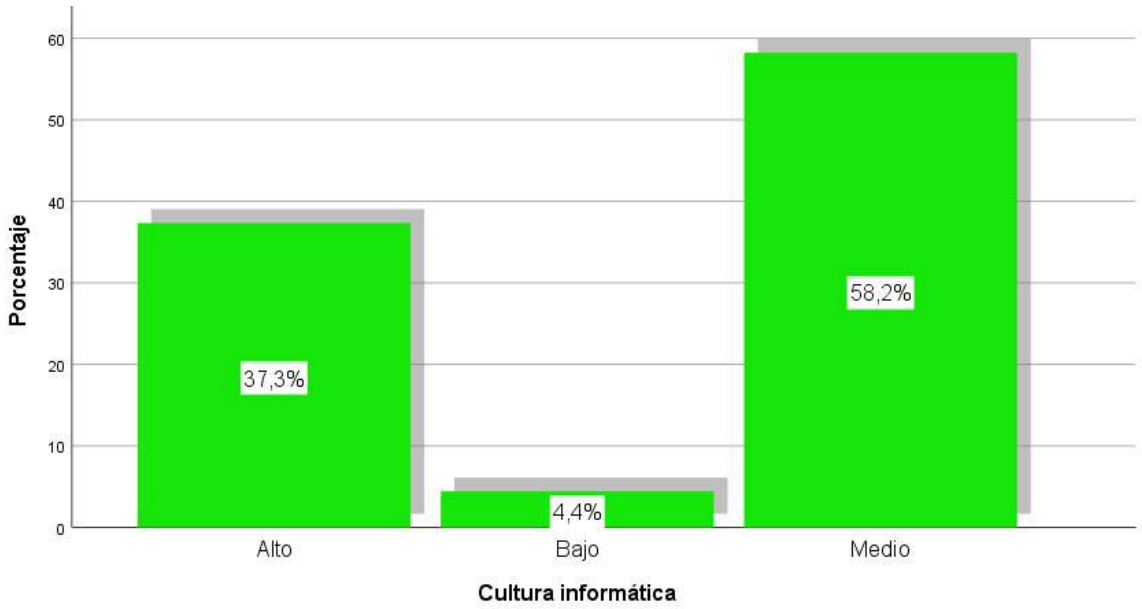


Figura 5. Cultura informática

En el año 2023, dentro del Gobierno Regional de Lima, el 58,2% de los colaboradores indicó haber alcanzado un nivel medio en la variable cultura informática. Por otro lado, un 37,3% manifestó haber llegado a un nivel alto, mientras que solo el 4,4% reportó haber obtenido un nivel bajo.

4.2. Generalización entorno la hipótesis central

Hipótesis general

Ha: Existe relación significativa de la Seguridad de Información y la Cultura Informática de los colaboradores en el Gobierno Regional de Lima, en el año 2023.

Tabla 6. Seguridad de la información y la cultura informática

Correlaciones

			Seguridad de la información	Cultura informática
Rho de Spearman	Seguridad de la información	Cof de correlación	1,000	,523**
		Significacia	.	,000
		n	158	158
	Cultura informática	Cof de correlación	,523**	1,000
		Significacia	,000	.
		n	158	158

El coeficiente de correlación obtenido fue de r = 0,523, acompañado de un valor de significancia menor a 0,05, lo que permite rechazar la hipótesis nula y aceptar la alternativa. Esto evidencia que existe una relación entre la seguridad de la información y la cultura informática de los colaboradores del Gobierno Regional de Lima durante el año 2023, siendo dicha relación de intensidad moderada.

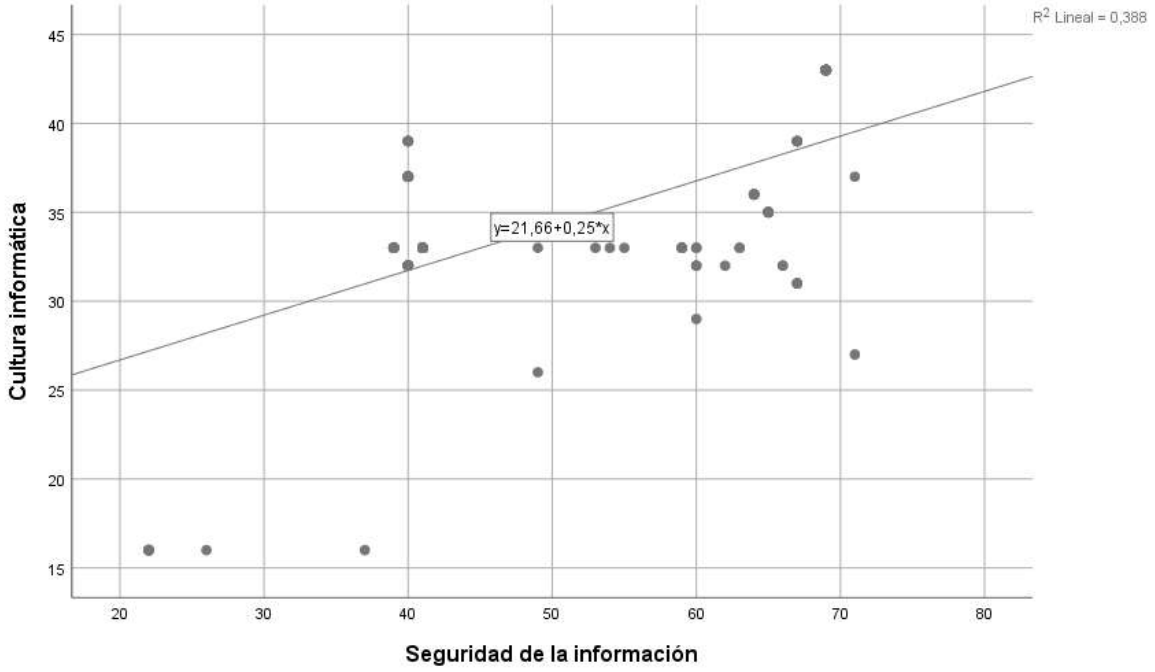


Figura Seguridad de la información y la cultura informática

Hipótesis especifica 1

Ha: Existe relación significativa de la integridad de la Seguridad de Información y la Cultura Informática de los colaboradores en el Gobierno Regional de Lima, en el año 2023

Tabla 7. La integridad de la seguridad de la información y la cultura informática

Correlaciones

			Integridad	Cultura informática
Rho de Spearman	Integridad	Cof de correlación	1,000	,553**
		Significacia	.	,000
		n	158	158
	Cultura informática	Cof de correlación	,553**	1,000
		Significacia	,000	.
		n	158	158

**. La correlación es significativa en el nivel 0,01 (bilateral).

La tabla reporta un coeficiente de correlación de r = 0,553 con un nivel de significancia menor a 0,05, lo que lleva a aceptar la hipótesis alternativa y rechazar la nula. En consecuencia, se confirma que, durante el año 2023, en el Gobierno Regional de Lima, la integridad de la seguridad de la información mantiene una relación moderada con la cultura informática de sus colaboradores.

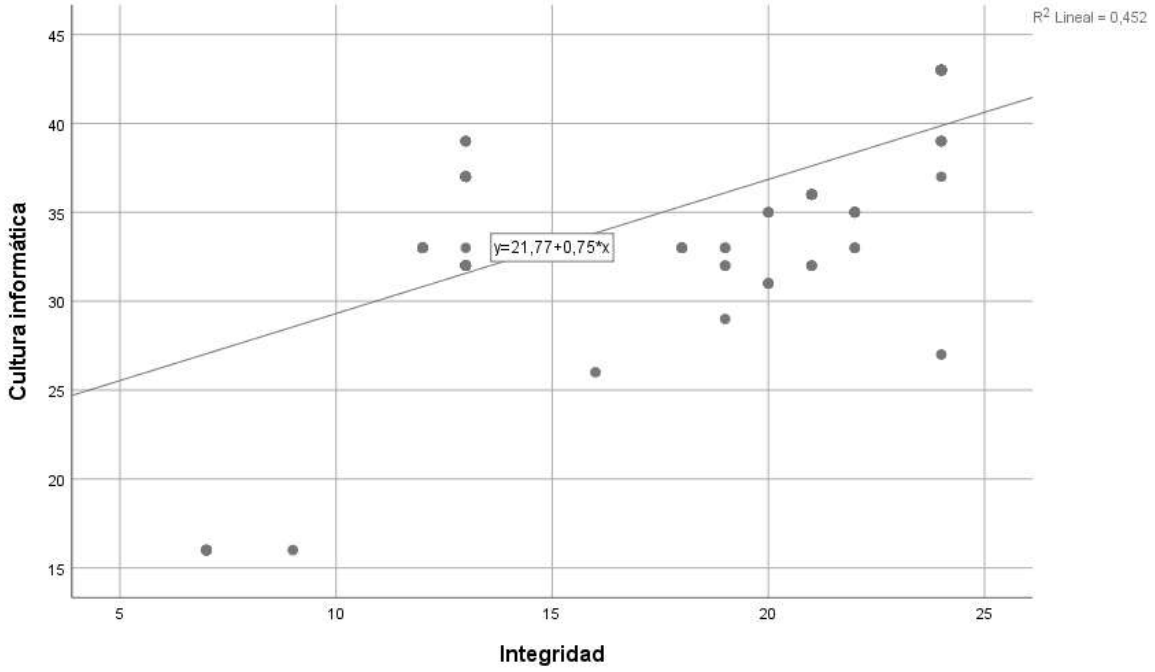


Figura 6. La integridad de la seguridad de la información y la cultura informática

Hipótesis especifica 2

Ha: Existe relación significativa de la confidencialidad de la Seguridad de Información y la Cultura Informática de los colaboradores en el Gobierno Regional de Lima, en el año 2023.

Tabla 8. La confidencialidad de la seguridad de la información y la cultura informática

Correlaciones

			Confidencialidad	Cultura informática
Rho de Spearman	Confidencialidad	Cof de correlación	1,000	,424**
		Significacia	.	,000
		n	158	158
	Cultura informática	Cof de correlación	,424**	1,000
		Significacia	,000	.
		n	158	158

**. La correlación es significativa en el nivel 0,01 (bilateral).

Se obtuvo en la tabla un coeficiente de correlación de r = 0,424, junto con un nivel de significancia inferior a 0,05, lo que condujo a rechazar la hipótesis nula y aceptar la alternativa. De esta manera, se confirma que en el Gobierno Regional de Lima, durante el año 2023, la confidencialidad en la seguridad de la información presenta una relación moderada con la cultura informática de los colaboradores.

.

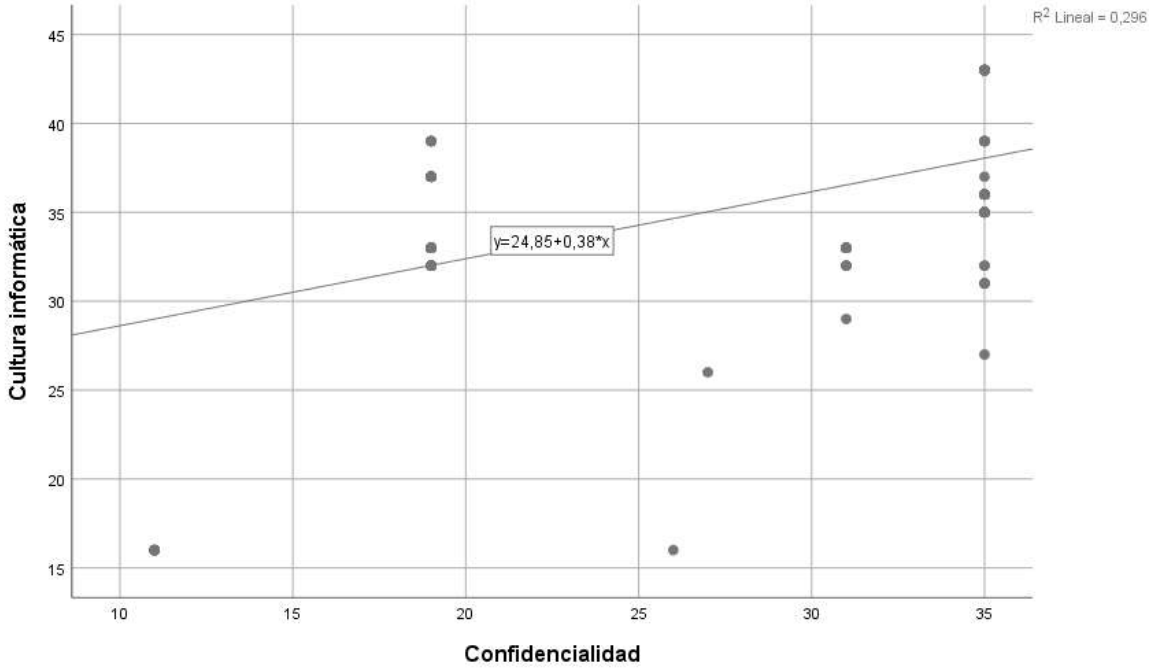


Figura 7. La confidencialidad de la seguridad de la información y la cultura informática

Hipótesis especifica 3

Ha: Existe relación significativa de la disponibilidad de la seguridad de Información y la Cultura Informática de los colaboradores en el Gobierno Regional de Lima, en el año 2023.

Tabla 9. La disponibilidad de la seguridad de la información y la cultura informática

Correlaciones

			Disponibilidad	Cultura informática
Rho de Spearman	Disponibilidad	Cof de correlación	1,000	,416**
		Significacia	.	,000
		n	158	158
	Cultura informática	Cof de correlación	,416**	1,000
		Significacia	,000	.
		n	158	158

El coeficiente de correlación obtenido fue r = 0,416, con un nivel de significancia menor a 0,05, lo que permitió rechazar la hipótesis nula y aceptar la alternativa. En consecuencia, se evidenció que, durante el año 2023 en el Gobierno Regional de Lima, la disponibilidad en la seguridad de la información guarda una relación moderada con la cultura informática de los colaboradores.

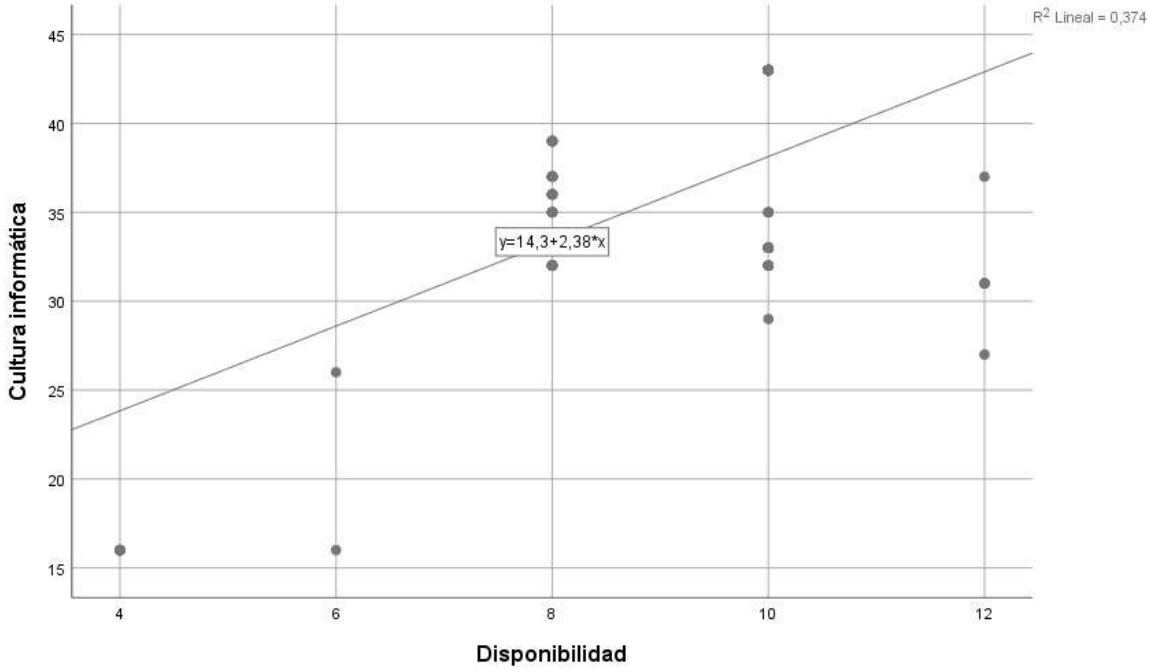


Figura 8. La infraestructura y equipamiento y la vocación cristiana

CAPITULO V
DISCUSIÓN

5.1. Discusión de los resultados

En la era digital, la seguridad de la información se ha convertido en un pilar fundamental para la gestión eficiente y transparente de las entidades públicas. En el caso del Gobierno Regional de Lima, garantizar la protección de los datos institucionales y fomentar una cultura informática sólida entre sus colaboradores es un desafío prioritario. La creciente dependencia de sistemas tecnológicos y el flujo constante de información sensible requieren estrategias efectivas que mitiguen los riesgos asociados a la ciberseguridad, tales como el acceso no autorizado, la filtración de datos y el uso indebido de la información.

Sin embargo, la seguridad de la información no depende únicamente de la implementación de tecnologías avanzadas, sino también del nivel de concienciación y preparación de los trabajadores. Una cultura informática débil puede convertirse en un factor de vulnerabilidad, ya que errores humanos, prácticas inadecuadas o desconocimiento de protocolos pueden comprometer la integridad y confidencialidad de la información. En este sentido, fortalecer la cultura informática de los colaboradores del Gobierno Regional de Lima resulta crucial para garantizar un entorno digital seguro y eficiente.

Habiéndose contrastado la hipótesis central se evidencia estadísticamente que Existe relación entre la Seguridad de Información y la Cultura Informática de los colaboradores en el Gobierno Regional de Lima, en el año 2023, siendo de una intensidad moderada.. Similares resultados se muestran en los trabajos presentado por Alvarez, C. (2018) trabajó en la gerencia y el problema de la seguridad de la Información en las Organizaciones Modernas para lograr el propósito que fue investigar la relación de ambas variables, teniendo como población a los trabajadores de la empresa Gandalf Comunicaciones. En la metodología empleada, se propuso una investigación histórica/documental. Como técnica se utiliza la observación indirecta,

ya que se van a usar documentos, de modo que se van a analizar las teorías y las fuentes de investigadores teóricos de forma cualitativa, por lo que no aplica el uso de encuestas ni de documentos, en tanto que se trata de una investigación de tipo histórico documental.

.

Huaura (2019) investigó la gestión de riesgos de la seguridad de la información en empresas de telecomunicaciones de Lima Metropolitana, con el fin de analizar la relación entre ambas variables. El estudio, de diseño no experimental y descriptivo, consideró a 104 trabajadores como muestra. A través de una encuesta validada y confiable de 10 ítems, se concluyó que la gestión de riesgos basada en la NTP ISO/IEC 31000 influye de manera significativa en el control de la seguridad de la información en dicho sector.

Los hallazgos de este estudio evidencian la necesidad de fortalecer la seguridad de la información en el Gobierno Regional de Lima mediante una mejora sustancial en la cultura informática de sus colaboradores. Se ha identificado que el nivel de concienciación sobre ciberseguridad sigue siendo insuficiente, lo que expone a la institución a riesgos como el acceso no autorizado a datos sensibles, el phishing y el uso inadecuado de los sistemas digitales.

Asimismo, los resultados sugieren que la implementación de capacitaciones periódicas y la adopción de normativas claras sobre el manejo de la información pueden contribuir significativamente a mitigar estos riesgos. Las experiencias en otras instituciones públicas han demostrado que una cultura informática fortalecida no solo protege la información institucional, sino que también optimiza la eficiencia operativa y refuerza la confianza de la ciudadanía en la administración pública.

En conclusión, la relación entre la seguridad de la información y la cultura informática de los colaboradores es un factor determinante en la gestión digital de las entidades gubernamentales. Para garantizar la protección de los datos y el cumplimiento de normativas, es imprescindible adoptar un enfoque integral que combine formación continua, implementación de tecnologías seguras, monitoreo

constante y el fomento de buenas prácticas en toda la organización. Solo así el Gobierno Regional de Lima podrá consolidar un entorno digital seguro y eficiente en el marco de la transformación digital de la gestión pública.

CAPITULO VI
CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones

Primero: Se identificó una relación de intensidad moderada entre la seguridad de la información y la cultura informática en los colaboradores del Gobierno Regional de Lima durante el año 2023.

Segundo: En el caso de la integridad como dimensión de la seguridad de la información, se encontró también una relación moderada con la cultura informática de los trabajadores del Gobierno Regional de Lima en el mismo periodo.

Tercero: Se evidenció una correlación moderada entre la confidencialidad de la información y la cultura informática en los colaboradores pertenecientes al Gobierno Regional de Lima en el año 2023.

Cuarto: De igual manera, la disponibilidad de la seguridad de la información mostró una relación moderada con la cultura informática de los colaboradores del Gobierno Regional de Lima durante el año 2023..

6.2. Recomendaciones

Primero: Implementar programas de capacitación continúa dirigidos a los colaboradores del Gobierno Regional de Lima para fortalecer su cultura informática y concienciarlos sobre la importancia de la seguridad de la información. Estos programas deben abordar temas como la gestión de contraseñas, la identificación de intentos de phishing, el uso seguro de dispositivos electrónicos y la protección de datos sensibles

Segundo: Elaborar y difundir políticas de seguridad de la información claras y accesibles para todos los colaboradores es clave para reducir riesgos de vulnerabilidad. Estas políticas deben establecer normas sobre el uso adecuado de dispositivos, el acceso a sistemas informáticos, la gestión de información confidencial y las sanciones en caso de incumplimiento.

Tercero: Los líderes y directivos den el ejemplo con buenas prácticas de seguridad informática, incentivando hábitos seguros y reforzando el compromiso de los colaboradores con la protección de la información.

Cuarto: Más allá de las capacitaciones y las tecnologías, es clave promover un cambio en la cultura organizacional que valore la seguridad de la información como un pilar fundamental del trabajo en el Gobierno Regional de Lima. Para ello, se deben establecer incentivos para los colaboradores que demuestren buenas prácticas en ciberseguridad, generar campañas de sensibilización internas y fomentar la denuncia de posibles vulnerabilidades

REFERENCIAS

Castañeda, L., & León, M. (2020). *Gestión de riesgos en sistemas de información*. Editorial Universitaria del Norte.

Contraloría General de la República del Perú. (2020). *Lineamientos de seguridad de la información en entidades públicas*. https://www.contraloria.gob.pe/

Gómez, R., & Navarro, F. (2017). *Inclusión digital y brecha tecnológica en América Latina*. Fondo Editorial Universitario.

González, A., & Reyes, P. (2020). *Fundamentos de seguridad informática*. Ediciones Académicas.

INEI. (2021). *Manual de protección de datos e información*. Instituto Nacional de Estadística e Informática del Perú.

López, D., & Espinoza, H. (2021). *Gestión de la seguridad de la información con ISO 27001*. Editorial Alfaomega.

Martínez, J. M. (2020). Cultura informática institucional y ciberseguridad en la administración pública. *Revista Iberoamericana de Tecnología y Sociedad*, *6*(2), 123–135.

Martínez, J., & Durán, C. (2020). *Ciberseguridad: Teoría y práctica*. Grupo Editorial Patria.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2018). *Guía para la gestión de la seguridad de la información*. Gobierno de Colombia.

Pérez, M., & Chávez, T. (2019). *Normativas y políticas en seguridad de la información*. Editorial Digital Académica.

Ramírez, L., & Pérez, J. (2019). *Riesgos informáticos y continuidad del negocio*. Universidad Nacional Autónoma de México.

Ramos, E., & Ugarte, C. (2022). *Ciberataques y amenazas actuales*. Editorial Universitaria.

Ruiz, D., & Hernández, V. (2018). *Gestión de accesos y control en redes seguras*. Editorial Macro.

Salinas Ibáñez, J. (2017). *Innovación educativa y uso de las TIC: Nuevas formas de enseñanza y aprendizaje*. Octaedro.

Silva Quiroz, J. (2016). Cultura informática y desempeño laboral en instituciones públicas. *Revista de Gestión Pública*, *4*(3), 45–58.

Soto, A. (2018). *Alfabetización digital y cultura informática en la educación*. Editorial

Trillas.

Torres, F., & Andrade, M. (2019). *Respaldo de datos y estrategias de recuperación ante desastres*. Fondo Editorial Tecnológico.

ANEXOS

Instrumentos

Instrumento: Seguridad de Información

Cuestionario

Totalmente de acuerdo	4
Indeciso	3
En desacuerdo	2
Totalmente en desacuerdo	1

VARIABLE: SEGURIDAD DE INFORMACION						
Dimensiones	**INDICADORES**		**1**	**2**	**3**	**4**
Confidencialidad	**Control de Acceso**					
	1	¿Cree usted que la confidencialidad es necesaria para controlar el acceso a la información?				
	2	¿Piensa que el control de acceso es un elemento decisivo en la confidencialidad para salvaguardar la información?				
	3	¿Considera que la confidencialidad debe ser un pilar fundamental para garantizar el control de acceso en la seguridad de la información?				
	Autenticación					
	4	¿Debe la autenticación ser obligatoria para asegurar la confidencialidad?				
	5	¿Es la autenticación clave al acceder a información confidencial? ¿Debe la autenticación ser obligatoria para asegurar la confidencialidad?				
	6	• ¿Es la autenticación clave al acceder a información confidencial?				
	Autorización					
	7	¿Cree que la autorización confidencial es necesaria para garantizar la seguridad de la información?				
	8	¿Considera que la confidencialidad requiere autorización para proteger la información?				
	9	¿Debe la autorización ser un requisito clave para acceder y mantener la confidencialidad de los datos?				
	Seguridad del procedimiento					
Integridad	10	• ¿Considera que la integridad debe sustentarse en la seguridad de los procedimientos como elemento esencial de				

		la seguridad de la información?				
	11	• ¿Está de acuerdo en que la documentación, revisión y actualización de los procedimientos son necesarios para garantizar la integridad de la información?				
	12	• ¿Piensa que la seguridad de la información debe contemplar procedimientos específicos para proteger la integridad de los datos?				
	Protección					
	13	¿La protección de datos forma parte de la integridad en la seguridad de la información?				
	14	¿Es la protección de datos esencial para lograr integridad?				
	15	¿La integridad asegura la veracidad mediante la protección de la información?				
	Acceso a la información					
	16	¿Debe la disponibilidad considerar el acceso para asegurar la veracidad de la información?				
Seguridad	17	¿Es el acceso a la información un aspecto clave de la disponibilidad para lograr seguridad?				
	18	¿Es el control de acceso un factor esencial de la disponibilidad para garantizar la seguridad de la información?				

CUESTIONARIO

Totalmente de acuerdo	4
Indeciso	3
En desacuerdo	2
Totalmente en desacuerdo	1

VARIABLE: CULTURA INFORMATICA							
DIMENSIONES		**INDICADORES**		**1**	**2**	**3**	**4**
		1	**Proceso de Transmisión**				
		1	¿Son los equipos necesarios para una tangibilidad que brinde calidad de servicio?				
		2	¿Debe la tangibilidad asegurar el uso adecuado de los equipos?				
		3	¿Hace el uso correcto de equipos que la tangibilidad sea base del servicio?				
		2	**Tratamiento de la Información**				
		4	¿Es la tangibilidad un factor clave que debe incluir el almacenamiento en la calidad del servicio?				
		5	¿Debe el almacenamiento ser parte importante de la tangibilidad al brindar el servicio?				
		6	¿Debe el almacenamiento integrar la tangibilidad para lograr un servicio de calidad?				
		3	**Condiciones generales**				
		7	¿Debe la tangibilidad incluir condiciones generales para asegurar la calidad del servicio?				
		8	¿Influye la tangibilidad en la calidad del servicio al considerar las condiciones generales?				
		9	¿Afectan las condiciones del servicio la tangibilidad y, con ello, la calidad?				
	Fiabilidad	**1**	**Compromiso**				

		10	¿Es la calidad del servicio resultado de la fiabilidad lograda mediante el compromiso?				
		11	¿Debe el compromiso ser un factor clave de la fiabilidad para alcanzar calidad en el servicio?				
		12	¿Requiere la fiabilidad del compromiso para ofrecer un servicio de calidad?				
		2	**Servicio prometido**				
		13	¿Depende la calidad del servicio del nivel de fiabilidad basado en lo prometido?				
		14	¿Influye el servicio prometido en la fiabilidad necesaria para lograr calidad?				
		15	¿Responde la fiabilidad del usuario a la calidad del servicio que se le prometió?				
		1	**Tiempo de respuesta**				
		16	¿La calidad depende de una respuesta rápida al usuario?				
		17	¿El tiempo influye en la capacidad de respuesta del servicio?				
	Capacidad de respuesta	18	¿Una respuesta oportuna mejora la calidad del servicio?				
		2	**Mejora continua**				
		19	• ¿ La calidad del servicio depende de la capacidad de respuesta?				
		20	• La mejora continua fortalece la capacidad de respuesta.?				
		21	• La capacidad de respuesta al usuario asegura un servicio de calidad?				

Matriz de datos

N	Seguridad de la información																					Cultura informática																	
	Confidencialidad										Integridad							Disponibilidad				ST1	Informacional					Tecnológica				Socio cultural							ST1
	1	2	3	4	5	6	7	8	9	S1	10	11	12	13	14	15	S2	16	17	18	S3		19	20	21	22	S6	23	24	25	S7	26	27	28	29	30	S8	
1	3	3	3	3	3	3	3	3	3	27	2	2	3	3	3	3	16	2	2	2	6	49	3	2	2	3	10	2	2	2	6	2	2	2	2	2	10	26
2	3	2	2	2	2	2	2	2	2	19	2	4	2	2	2	2	14	2	3	3	8	41	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
3	3	1	1	1	1	1	1	1	1	11	2	1	1	1	1	1	7	2	1	1	4	22	3	1	1	1	6	2	1	1	4	2	1	1	1	1	6	16
4	3	4	4	4	4	4	4	4	4	35	4	4	4	4	4	4	24	2	4	4	10	69	3	4	4	4	15	2	4	4	10	2	4	4	4	4	18	43
5	3	2	2	2	2	2	2	2	2	19	2	4	2	2	2	2	14	2	3	3	8	41	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
6	3	2	2	2	2	2	2	2	2	19	2	4	2	2	2	2	14	2	3	3	8	41	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
7	3	2	2	2	2	2	2	2	2	19	2	3	2	2	2	2	13	2	3	3	8	40	3	3	3	2	11	2	4	2	8	2	4	4	4	4	18	37
8	3	4	4	4	4	4	4	4	4	35	2	3	4	4	4	4	21	2	3	3	8	64	3	3	3	4	13	2	3	4	9	2	3	3	3	3	14	36
9	3	4	4	4	4	4	4	4	4	35	3	3	4	4	4	4	22	2	3	3	8	65	3	3	3	3	12	2	4	3	9	2	3	3	3	3	14	35
10	3	2	2	2	2	2	2	2	2	19	2	3	2	2	2	2	13	2	3	3	8	40	3	3	3	2	11	2	3	2	7	2	3	3	3	3	14	32
11	3	4	4	4	4	4	4	4	4	35	4	4	4	4	4	4	24	2	4	4	10	69	3	4	4	4	15	2	4	4	10	2	4	4	4	4	18	43
12	3	2	2	2	2	2	2	2	2	19	2	4	2	2	2	2	14	2	3	3	8	41	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
13	3	2	2	2	2	2	2	2	2	19	2	2	2	2	2	2	12	2	3	3	8	39	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
14	3	2	2	2	2	2	2	2	2	19	2	3	2	2	2	2	13	2	3	3	8	40	3	3	3	2	11	2	4	2	8	2	4	4	4	4	18	37
15	3	4	4	4	4	4	4	4	4	35	4	4	4	4	4	4	24	2	4	4	10	69	3	4	4	4	15	2	4	4	10	2	4	4	4	4	18	43
16	3	2	2	2	2	2	2	2	2	19	2	4	2	2	2	2	14	2	3	3	8	41	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
17	3	4	4	4	4	4	4	4	4	35	4	4	4	4	4	4	24	2	3	3	8	67	3	3	3	3	12	2	4	3	9	2	4	4	4	4	18	39
18	3	2	2	2	2	2	2	2	2	19	2	3	2	2	2	2	13	2	3	3	8	40	3	3	3	4	13	2	4	2	8	2	4	4	4	4	18	39
19	3	2	2	2	2	2	2	2	2	19	2	4	2	2	2	2	14	2	3	3	8	41	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
20	3	4	4	4	4	4	4	4	4	35	4	4	4	4	4	4	24	2	4	4	10	69	3	4	4	4	15	2	4	4	10	2	4	4	4	4	18	43
21	3	2	2	2	2	2	2	2	2	19	2	2	2	2	2	2	12	2	3	3	8	39	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
22	3	2	2	2	2	2	2	2	2	19	2	3	2	2	2	2	13	2	3	3	8	40	3	3	3	2	11	2	3	2	7	2	3	3	3	3	14	32
23	3	1	1	1	1	1	1	1	1	11	2	1	1	1	1	1	7	2	1	1	4	22	3	1	1	1	6	2	1	1	4	2	1	1	1	1	6	16
24	3	4	4	4	4	4	4	4	4	35	4	4	4	4	4	4	24	2	4	4	10	69	3	4	4	4	15	2	4	4	10	2	4	4	4	4	18	43
25	3	2	2	2	2	2	2	2	2	19	2	4	2	2	2	2	14	2	3	3	8	41	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
26	3	2	2	2	2	2	2	2	2	19	2	4	2	2	2	2	14	2	3	3	8	41	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
27	3	2	2	2	2	2	2	2	2	19	2	3	2	2	2	2	13	2	3	3	8	40	3	3	3	2	11	2	4	2	8	2	4	4	4	4	18	37
28	3	4	4	4	4	4	4	4	4	35	2	3	4	4	4	4	21	2	3	3	8	64	3	3	3	4	13	2	3	4	9	2	3	3	3	3	14	36
29	3	4	4	4	4	4	4	4	4	35	3	3	4	4	4	4	22	2	3	3	8	65	3	3	3	3	12	2	4	3	9	2	3	3	3	3	14	35
30	3	2	2	2	2	2	2	2	2	19	2	3	2	2	2	2	13	2	3	3	8	40	3	3	3	2	11	2	3	2	7	2	3	3	3	3	14	32
31	3	4	4	4	4	4	4	4	4	35	4	4	4	4	4	4	24	2	4	4	10	69	3	4	4	4	15	2	4	4	10	2	4	4	4	4	18	43
32	3	2	2	2	2	2	2	2	2	19	2	4	2	2	2	2	14	2	3	3	8	41	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
33	3	2	2	2	2	2	2	2	2	19	2	2	2	2	2	2	12	2	3	3	8	39	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
34	3	2	2	2	2	2	2	2	2	19	2	3	2	2	2	2	13	2	3	3	8	40	3	3	3	2	11	2	4	2	8	2	4	4	4	4	18	37
35	3	4	4	4	4	4	4	4	4	35	4	4	4	4	4	4	24	2	4	4	10	69	3	4	4	4	15	2	4	4	10	2	4	4	4	4	18	43
36	3	2	2	2	2	2	2	2	2	19	2	4	2	2	2	2	14	2	3	3	8	41	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33

37	3	4	4	4	4	4	4	4	4	35	4	4	4	4	4	4	24	2	3	3	8	67	3	3	3	3	12	2	4	3	9	2	4	4	4	4	18	39
38	3	2	2	2	2	2	2	2	2	19	2	3	2	2	2	2	13	2	3	3	8	40	3	3	3	4	13	2	4	2	8	2	4	4	4	4	18	39
39	3	2	2	2	2	2	2	2	2	19	2	4	2	2	2	2	14	2	3	3	8	41	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
40	3	4	4	4	4	4	4	4	4	35	4	4	4	4	4	4	24	2	4	4	10	69	3	4	4	4	15	2	4	4	10	2	4	4	4	4	18	43
41	3	2	2	2	2	2	2	2	2	19	2	2	2	2	2	2	12	2	3	3	8	39	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
42	3	2	2	2	2	2	2	2	2	19	2	3	2	2	2	2	13	2	3	3	8	40	3	3	3	2	11	2	3	2	7	2	3	3	3	3	14	32
43	3	1	1	4	4	1	4	4	4	26	2	1	1	1	1	1	7	2	1	1	4	37	3	1	1	1	6	2	1	1	4	2	1	1	1	1	6	16
44	3	4	4	4	4	4	4	4	4	35	4	4	4	4	4	4	24	2	4	4	10	69	3	4	4	4	15	2	4	4	10	2	4	4	4	4	18	43
45	3	2	2	2	2	2	2	2	2	19	2	4	2	2	2	2	14	2	3	3	8	41	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
46	3	2	2	2	2	2	2	2	2	19	2	4	2	2	2	2	14	2	3	3	8	41	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
47	3	2	2	2	2	2	2	2	2	19	2	3	2	2	2	2	13	2	3	3	8	40	3	3	3	2	11	2	4	2	8	2	4	4	4	4	18	37
48	3	4	4	4	4	4	4	4	4	35	2	3	4	4	4	4	21	2	3	3	8	64	3	3	3	4	13	2	3	4	9	2	3	3	3	3	14	36
49	3	4	4	4	4	4	4	4	4	35	3	3	4	4	4	4	22	2	3	3	8	65	3	3	3	3	12	2	4	3	9	2	3	3	3	3	14	35
50	3	2	2	2	2	2	2	2	2	19	2	3	2	2	2	2	13	2	3	3	8	40	3	3	3	2	11	2	3	2	7	2	3	3	3	3	14	32
51	3	4	4	4	4	4	4	4	4	35	4	4	4	4	4	4	24	2	4	4	10	69	3	4	4	4	15	2	4	4	10	2	4	4	4	4	18	43
52	3	2	2	2	2	2	2	2	2	19	2	4	2	2	2	2	14	2	3	3	8	41	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
53	3	2	2	2	2	2	2	2	2	19	2	2	2	2	2	2	12	2	3	3	8	39	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
54	3	2	2	2	2	2	2	2	2	19	2	3	2	2	2	2	13	2	3	3	8	40	3	3	3	2	11	2	4	2	8	2	4	4	4	4	18	37
55	3	4	4	4	4	4	4	4	4	35	4	4	4	4	4	4	24	2	4	4	10	69	3	4	4	4	15	2	4	4	10	2	4	4	4	4	18	43
56	3	2	2	2	2	2	2	2	2	19	2	4	2	2	2	2	14	2	3	3	8	41	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
57	3	4	4	4	4	4	4	4	4	35	4	4	4	4	4	4	24	2	3	3	8	67	3	3	3	3	12	2	4	3	9	2	4	4	4	4	18	39
58	3	2	2	2	2	2	2	2	2	19	2	3	2	2	2	2	13	2	3	3	8	40	3	3	3	4	13	2	4	2	8	2	4	4	4	4	18	39
59	3	2	2	2	2	2	2	2	2	19	2	4	2	2	2	2	14	2	3	3	8	41	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
60	3	4	4	4	4	4	4	4	4	35	4	4	4	4	4	4	24	2	4	4	10	69	3	4	4	4	15	2	4	4	10	2	4	4	4	4	18	43
61	3	2	2	2	2	2	2	2	2	19	2	2	2	2	2	2	12	2	3	3	8	39	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
62	3	2	2	2	2	2	2	2	2	19	2	3	2	2	2	2	13	2	3	3	8	40	3	3	3	2	11	2	3	2	7	2	3	3	3	3	14	32
63	3	1	1	1	1	1	1	1	1	11	2	1	1	1	1	1	7	2	1	1	4	22	3	1	1	1	6	2	1	1	4	2	1	1	1	1	6	16
64	3	4	4	4	4	4	4	4	4	35	4	4	4	4	4	4	24	2	4	4	10	69	3	4	4	4	15	2	4	4	10	2	4	4	4	4	18	43
65	3	2	2	2	2	2	2	2	2	19	2	4	2	2	2	2	14	2	3	3	8	41	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
66	3	2	2	2	2	2	2	2	2	19	2	4	2	2	2	2	14	2	3	3	8	41	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
67	3	2	2	2	2	2	2	2	2	19	2	3	2	2	2	2	13	2	3	3	8	40	3	3	3	2	11	2	4	2	8	2	4	4	4	4	18	37
68	3	4	4	4	4	4	4	4	4	35	2	3	4	4	4	4	21	2	3	3	8	64	3	3	3	4	13	2	3	4	9	2	3	3	3	3	14	36
69	3	4	4	4	4	4	4	4	4	35	3	3	4	4	4	4	22	2	3	3	8	65	3	3	3	3	12	2	4	3	9	2	3	3	3	3	14	35
70	3	2	2	2	2	2	2	2	2	19	2	3	2	2	2	2	13	2	3	3	8	40	3	3	3	2	11	2	3	2	7	2	3	3	3	3	14	32
71	3	4	4	4	4	4	4	4	4	35	4	4	4	4	4	4	24	2	4	4	10	69	3	4	4	4	15	2	4	4	10	2	4	4	4	4	18	43
72	3	2	2	2	2	2	2	2	2	19	2	4	2	2	2	2	14	2	3	3	8	41	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
73	3	2	2	2	2	2	2	2	2	19	2	4	2	2	2	2	14	2	3	3	8	41	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
74	3	2	2	2	2	2	2	2	2	19	2	3	2	2	2	2	13	2	3	3	8	40	3	3	3	2	11	2	4	2	8	2	4	4	4	4	18	37
75	3	4	4	4	4	4	4	4	4	35	2	3	4	4	4	4	21	2	3	3	8	64	3	3	3	4	13	2	3	4	9	2	3	3	3	3	14	36
76	3	4	4	4	4	4	4	4	4	35	3	3	4	4	4	4	22	2	3	3	8	65	3	3	3	3	12	2	4	3	9	2	3	3	3	3	14	35
77	3	2	2	2	2	2	2	2	2	19	2	3	2	2	2	2	13	2	3	3	8	40	3	3	3	2	11	2	3	2	7	2	3	3	3	3	14	32
78	3	4	4	4	4	4	4	4	4	35	4	4	4	4	4	4	24	2	4	4	10	69	3	4	4	4	15	2	4	4	10	2	4	4	4	4	18	43
79	3	2	2	2	2	2	2	2	2	19	2	4	2	2	2	2	14	2	3	3	8	41	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33

80	3	2	2	2	2	2	2	2	2	19	2	2	2	2	2	2	12	2	3	3	8	39	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
81	3	2	2	2	2	2	2	2	2	19	2	3	2	2	2	2	13	2	3	3	8	40	3	3	3	2	11	2	4	2	8	2	4	4	4	4	18	37
82	3	4	4	4	4	4	4	4	4	35	4	4	4	4	4	4	24	2	4	4	10	69	3	4	4	4	15	2	4	4	10	2	4	4	4	4	18	43
83	3	2	2	2	2	2	2	2	2	19	2	4	2	2	2	2	14	2	3	3	8	41	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
84	3	4	4	4	4	4	4	4	4	35	4	4	4	4	4	4	24	2	3	3	8	67	3	3	3	3	12	2	4	3	9	2	4	4	4	4	18	39
85	3	2	2	2	2	2	2	2	2	19	2	3	2	2	2	2	13	2	3	3	8	40	3	3	3	4	13	2	4	2	8	2	4	4	4	4	18	39
86	3	2	2	2	2	2	2	2	2	19	2	4	2	2	2	2	14	2	3	3	8	41	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
87	3	4	4	4	4	4	4	4	4	35	4	4	4	4	4	4	24	2	4	4	10	69	3	4	4	4	15	2	4	4	10	2	4	4	4	4	18	43
88	3	2	2	2	2	2	2	2	2	19	2	2	2	2	2	2	12	2	3	3	8	39	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
89	3	2	2	2	2	2	2	2	2	19	2	3	2	2	2	2	13	2	3	3	8	40	3	3	3	2	11	2	3	2	7	2	3	3	3	3	14	32
90	3	1	1	1	1	1	1	1	1	11	2	1	1	1	1	1	7	2	1	1	4	22	3	1	1	1	6	2	1	1	4	2	1	1	1	1	6	16
91	3	4	4	4	4	4	4	4	4	35	4	4	4	4	4	4	24	2	4	4	10	69	3	4	4	4	15	2	4	4	10	2	4	4	4	4	18	43
92	3	2	2	2	2	2	2	2	2	19	2	4	2	2	2	2	14	2	3	3	8	41	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
93	3	2	2	2	2	2	2	2	2	19	2	4	2	2	2	2	14	2	3	3	8	41	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
94	3	2	2	2	2	2	2	2	2	19	2	3	2	2	2	2	13	2	3	3	8	40	3	3	3	2	11	2	4	2	8	2	4	4	4	4	18	37
95	3	4	4	4	4	4	4	4	4	35	2	3	4	4	4	4	21	2	3	3	8	64	3	3	3	4	13	2	3	4	9	2	3	3	3	3	14	36
96	3	4	4	4	4	4	4	4	4	35	3	3	4	4	4	4	22	2	3	3	8	65	3	3	3	3	12	2	4	3	9	2	3	3	3	3	14	35
97	3	2	2	2	2	2	2	2	2	19	2	3	2	2	2	2	13	2	3	3	8	40	3	3	3	2	11	2	3	2	7	2	3	3	3	3	14	32
98	3	4	4	4	4	4	4	4	4	35	4	4	4	4	4	4	24	2	4	4	10	69	3	4	4	4	15	2	4	4	10	2	4	4	4	4	18	43
99	3	2	2	2	2	2	2	2	2	19	2	4	2	2	2	2	14	2	3	3	8	41	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
100	3	2	2	2	2	2	2	2	2	19	2	4	2	2	2	2	14	2	3	3	8	41	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
101	3	2	2	2	2	2	2	2	2	19	2	3	2	2	2	2	13	2	3	3	8	40	3	3	3	2	11	2	4	2	8	2	4	4	4	4	18	37
102	3	4	4	4	4	4	4	4	4	35	2	3	4	4	4	4	21	2	3	3	8	64	3	3	3	4	13	2	3	4	9	2	3	3	3	3	14	36
103	3	4	4	4	4	4	4	4	4	35	3	3	4	4	4	4	22	2	3	3	8	65	3	3	3	3	12	2	4	3	9	2	3	3	3	3	14	35
104	3	2	2	2	2	2	2	2	2	19	2	3	2	2	2	2	13	2	3	3	8	40	3	3	3	2	11	2	3	2	7	2	3	3	3	3	14	32
105	3	4	4	4	4	4	4	4	4	35	4	4	4	4	4	4	24	2	4	4	10	69	3	4	4	4	15	2	4	4	10	2	4	4	4	4	18	43
106	3	2	2	2	2	2	2	2	2	19	2	4	2	2	2	2	14	2	3	3	8	41	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
107	3	2	2	2	2	2	2	2	2	19	2	2	2	2	2	2	12	2	3	3	8	39	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
108	3	2	2	2	2	2	2	2	2	19	2	3	2	2	2	2	13	2	3	3	8	40	3	3	3	2	11	2	4	2	8	2	4	4	4	4	18	37
109	3	4	4	4	4	4	4	4	4	35	4	4	4	4	4	4	24	2	4	4	10	69	3	4	4	4	15	2	4	4	10	2	4	4	4	4	18	43
110	3	2	2	2	2	2	2	2	2	19	2	4	2	2	2	2	14	2	3	3	8	41	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
111	3	4	4	4	4	4	4	4	4	35	4	4	4	4	4	4	24	2	3	3	8	67	3	3	3	3	12	2	4	3	9	2	4	4	4	4	18	39
112	3	2	2	2	2	2	2	2	2	19	2	3	2	2	2	2	13	2	3	3	8	40	3	3	3	4	13	2	4	2	8	2	4	4	4	4	18	39
113	3	2	2	2	2	2	2	2	2	19	4	4	4	4	4	2	22	2	3	3	8	49	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
114	3	4	4	4	4	4	4	4	4	35	4	4	4	4	4	4	24	2	4	4	10	69	3	4	4	4	15	2	4	4	10	2	4	4	4	4	18	43
115	3	2	4	4	4	4	4	4	2	31	4	4	4	4	4	2	22	4	3	3	10	63	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
116	3	2	4	4	4	4	4	4	2	31	4	3	4	4	4	2	21	4	3	3	10	62	3	3	3	2	11	2	3	2	7	2	3	3	3	3	14	32
117	3	1	1	1	1	1	1	1	1	11	4	1	1	1	1	1	9	4	1	1	6	26	3	1	1	1	6	2	1	1	4	2	1	1	1	1	6	16
118	3	4	4	4	4	4	4	4	4	35	4	4	4	4	4	4	24	4	4	4	12	71	3	2	2	2	9	2	4	2	8	2	2	2	2	2	10	27
119	3	2	4	4	4	4	4	4	2	31	4	4	4	4	4	2	22	4	3	3	10	63	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
120	3	2	4	4	4	4	4	4	2	31	4	2	2	4	4	2	18	4	3	3	10	59	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
121	3	2	4	4	4	4	4	4	2	31	4	3	2	4	4	2	19	4	3	3	10	60	3	3	3	2	11	2	4	2	8	2	2	2	2	2	10	29
122	3	4	4	4	4	4	4	4	4	35	4	3	2	4	4	4	21	4	3	3	10	66	3	3	3	2	11	2	3	2	7	2	3	3	3	3	14	32

123	3	4	4	4	4	4	4	4	4	35	3	3	2	4	4	4	20	4	3	3	10	65	3	3	3	3	12	2	4	3	9	2	3	3	3	3	14	35
124	3	2	4	4	4	4	4	4	2	31	4	3	2	4	4	2	19	4	3	3	10	60	3	3	3	2	11	2	3	2	7	2	3	3	3	3	14	32
125	3	4	4	4	4	4	4	4	4	35	4	2	2	4	4	4	20	4	4	4	12	67	3	2	2	2	9	2	4	2	8	2	2	4	4	2	14	31
126	3	2	4	4	4	4	4	4	2	31	4	2	2	4	4	2	18	4	3	3	10	59	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
127	3	2	4	4	4	4	4	4	2	31	4	2	2	4	4	2	18	4	3	3	10	59	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
128	3	2	4	4	4	4	4	4	2	31	4	3	2	4	4	2	19	4	3	3	10	60	3	3	3	2	11	2	4	2	8	2	2	4	4	2	14	33
129	3	4	4	4	4	4	4	4	4	35	4	3	2	4	4	4	21	4	3	3	10	66	3	3	3	2	11	2	3	2	7	2	3	3	3	3	14	32
130	3	4	4	4	4	4	4	4	4	35	3	3	2	4	4	4	20	4	3	3	10	65	3	3	3	3	12	2	4	3	9	2	3	3	3	3	14	35
131	3	2	4	4	4	4	4	4	2	31	4	3	2	4	4	2	19	4	3	3	10	60	3	3	3	2	11	2	3	2	7	2	3	3	3	3	14	32
132	3	4	4	4	4	4	4	4	4	35	4	2	2	4	4	4	20	4	4	4	12	67	3	2	2	2	9	2	4	2	8	2	2	4	4	2	14	31
133	3	2	4	4	4	4	4	4	2	31	4	2	2	4	4	2	18	4	3	3	10	59	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
134	3	2	4	4	4	4	4	4	2	31	4	2	2	4	4	2	18	4	3	3	10	59	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
135	3	2	4	4	4	4	4	4	2	31	4	3	2	4	4	2	19	4	3	3	10	60	3	3	3	2	11	2	4	2	8	2	2	4	4	2	14	33
136	3	4	4	4	4	4	4	4	4	35	4	2	2	4	4	4	20	4	4	4	12	67	3	2	2	2	9	2	4	2	8	2	2	4	4	2	14	31
137	3	2	4	4	4	4	4	4	2	31	2	2	2	2	2	2	12	4	3	3	10	53	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
138	3	4	4	4	4	4	4	4	4	35	4	2	2	4	4	4	20	4	3	3	10	65	3	3	3	3	12	2	4	3	9	2	2	4	4	2	14	35
139	3	2	4	4	4	4	4	4	2	31	2	3	2	2	2	2	13	4	3	3	10	54	3	3	3	2	11	2	4	2	8	2	2	4	4	2	14	33
140	3	2	4	4	4	4	4	4	2	31	2	4	2	2	2	2	14	4	3	3	10	55	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
141	3	4	4	4	4	4	4	4	4	35	4	4	4	4	4	4	24	4	4	4	12	71	3	2	2	2	9	2	4	4	10	2	4	4	4	4	18	37
142	3	2	2	2	2	2	2	2	2	19	2	2	2	2	2	2	12	2	3	3	8	39	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
143	3	2	2	2	2	2	2	2	2	19	2	3	2	2	2	2	13	2	3	3	8	40	3	3	3	2	11	2	3	2	7	2	3	3	3	3	14	32
144	3	1	1	1	1	1	1	1	1	11	2	1	1	1	1	1	7	2	1	1	4	22	3	1	1	1	6	2	1	1	4	2	1	1	1	1	6	16
145	3	4	4	4	4	4	4	4	4	35	4	4	4	4	4	4	24	2	4	4	10	69	3	4	4	4	15	2	4	4	10	2	4	4	4	4	18	43
146	3	2	2	2	2	2	2	2	2	19	2	4	2	2	2	2	14	2	3	3	8	41	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
147	3	2	2	2	2	2	2	2	2	19	2	4	2	2	2	2	14	2	3	3	8	41	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
148	3	2	2	2	2	2	2	2	2	19	2	3	2	2	2	2	13	2	3	3	8	40	3	3	3	2	11	2	4	2	8	2	4	4	4	4	18	37
149	3	4	4	4	4	4	4	4	4	35	2	3	4	4	4	4	21	2	3	3	8	64	3	3	3	4	13	2	3	4	9	2	3	3	3	3	14	36
150	3	4	4	4	4	4	4	4	4	35	3	3	4	4	4	4	22	2	3	3	8	65	3	3	3	3	12	2	4	3	9	2	3	3	3	3	14	35
151	3	4	4	4	4	4	4	4	4	35	2	3	4	4	4	4	21	2	3	3	8	64	3	3	3	4	13	2	3	4	9	2	3	3	3	3	14	36
152	3	4	4	4	4	4	4	4	4	35	3	3	4	4	4	4	22	2	3	3	8	65	3	3	3	3	12	2	4	3	9	2	3	3	3	3	14	35
153	3	2	2	2	2	2	2	2	2	19	2	3	2	2	2	2	13	2	3	3	8	40	3	3	3	2	11	2	3	2	7	2	3	3	3	3	14	32
154	3	4	4	4	4	4	4	4	4	35	4	4	4	4	4	4	24	2	4	4	10	69	3	4	4	4	15	2	4	4	10	2	4	4	4	4	18	43
155	3	2	2	2	2	2	2	2	2	19	2	4	2	2	2	2	14	2	3	3	8	41	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
156	3	2	2	2	2	2	2	2	2	19	2	4	2	2	2	2	14	2	3	3	8	41	3	3	3	2	11	2	3	3	8	2	3	3	3	3	14	33
157	3	2	2	2	2	2	2	2	2	19	2	3	2	2	2	2	13	2	3	3	8	40	3	3	3	2	11	2	4	2	8	2	4	4	4	4	18	37
158	3	4	4	4	4	4	4	4	4	35	2	3	4	4	4	4	21	2	3	3	8	64	3	3	3	4	13	2	3	4	9	2	3	3	3	3	14	36