Universidad Nacional Federico Villarreal

VRIN | VICERRECTORADO DE INVESTIGACIÓN

ESCUELA UNIVERSITARIA DE POSGRADO

APLICACIÓN DE LA NORMA ISO/IEC 27009 PARA PREVENIR RIESGOS DEL SISTEMA DE INFORMACIÓN EN LA MUNICIPALIDAD DE CHORRILLOS

Línea de investigación:
Sistemas de información y optimización

Tesis para optar el grado académico de Maestro en Ingeniería de Sistemas con mención en Gestión de Tecnologías de la Información

Autor

Rocha Campos, Wilzer Manuel

Asesor

Zamora Talaverano, Noe Sabino

ORCID: 0000-0002-4368-8955

Jurado

Cachay Boza, Orestes

Vales Carrillo, Jorge Alberto

Ogosi Auqui, José Antonio

Lima - Perú

2026

Universidad Nacional Federico Villarreal

VRIN | VICERRECTORADO DE INVESTIGACIÓN

ESCUELA UNIVERSITARIA DE POSGRADO

APLICACIÓN DE LA NORMA ISO/IEC 27009 PARA PREVENIR RIESGOS DEL SISTEMA DE INFORMACIÓN EN LA MUNICIPALIDAD DE CHORRILLOS

Línea de Investigación:
Sistema de información y optimización

Tesis para optar el grado académico de Maestro en Ingeniería de Sistemas con mención en Gestión de Tecnologías de la Información

Autor:
Rocha Campos, Wilzer Manuel

Asesor:
Zamora Talaverano, Noe Sabino
ORCID: 0000-0002-4368-8955

Jurado
Cachay Boza, Orestes
Vales Carrillo, Jorge Alberto
Ogosi Auqui, José Antonio

Lima – Perú
2026

Dedicatoria

En primer lugar, agradezco a Dios por brindarme salud, fortaleza y sabiduría para culminar esta etapa tan significativa de mi vida.

A mi esposa Estefanie Gadea Ledesma, y a mis hijas Almudena y Aitana, quienes con su amor, paciencia y apoyo incondicional han sido mi mayor inspiración y motor. Este logro también les pertenece, porque cada página escrita lleva impreso el sacrificio y la ternura que me brindaron.

A mi madre Luz Campos Guevara, ejemplo de entrega y perseverancia, cuyo cariño y enseñanzas me han guiado siempre. Y a la memoria de mi padre Manuel Salvador Rocha Lovera, cuya ausencia física no borra la huella imborrable de sus valores ni la fuerza de su legado. Aunque ya no esté a mi lado, su espíritu me acompaña y me impulsa en cada paso, convirtiendo este triunfo en un homenaje a su vida.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Resumen

En esta investigación, nuestro objetivo es identificar cómo la implementación de la norma ISO/IEC 27009 impacta la mitigación de riesgos en el sistema de información de la Municipalidad Distrital de Chorrillos. La principal motivación se origina en la falta de un Sistema de Gestión de Seguridad de la Información (SGSI) formal y de políticas efectivas, situación que expone a la organización a filtraciones de datos personales, interrupciones en los servicios electrónicos y alteraciones en la información administrativa. La incorporación de este estándar del ámbito ISO/IEC 27000 permitirá adaptar las medidas de seguridad a las particularidades del sector público municipal y mejorar la disponibilidad y la privacidad de los sistemas informáticos. El estudio tiene un enfoque tecnológico y un diseño descriptivo-correlacional. Se realizarán entrevistas estructuradas a los siete responsables del área de seguridad de la información de la municipalidad. Los datos obtenidos se analizarán mediante técnicas estadísticas descriptivas y la prueba t de Student para evaluar la relación entre la aplicación de la norma y las mejoras en los índices de seguridad. Se espera una reducción del tiempo de inactividad de los sistemas municipales y de los accesos no autorizados a información crítica. Estos resultados apoyarían la hipótesis general de que la ISO/IEC 27009 incrementa la seguridad de la información en la municipalidad. Finalmente, el estudio sugiere un plan de implementación adaptado a este contexto, que podría servir como modelo para otras entidades públicas con desafíos similares.

Palabras clave: ISO/IEC 27009, seguridad de la información, gestión de riesgos, sistema de información, municipalidad, disponibilidad, confidencialidad, SGSI, sector público

Abstract

This research aims to identify how the implementation of the ISO/IEC 27009 standard impacts risk mitigation in the information system of the District Municipality of Chorrillos. The main motivation stems from the lack of a formal Information Security Management System (ISMS) and effective policies, a situation that exposes the organization to personal data breaches, interruptions of electronic services, and alterations of administrative information. Incorporating this standard from the ISO/IEC 27000 family will allow security measures to be adapted to the particularities of the municipal public sector and improve the availability and privacy of information systems. The study has a technological approach and a descriptive-correlational design. Structured interviews will be conducted with the seven persons responsible for the municipality's information security area. The data obtained will be analyzed using descriptive statistical techniques and Student's t-test to assess the relationship between implementation of the standard and improvements in security indicators. A reduction in municipal system downtime and unauthorized access to critical information is expected. These results would support the general hypothesis that ISO/IEC 27009 increases information security in the municipality. Finally, the study suggests an implementation plan adapted to this context, which could serve as a model for other public entities facing similar challenges.

Keywords: ISO/IEC 27009, information security, risk management, information system, municipality, availability, confidentiality, ISMS, public sector.

I. INTRODUCCIÓN

1.1 Planteamiento del problema

En la Municipalidad de Chorrillos vemos algo. Hoy no hay un sistema formal de seguridad. Tampoco hay reglas fuertes para proteger datos. Esta falta hace al lugar débil. Riesgos serios pueden pasar. Datos de gente pueden salir. Servicios por internet pueden parar. Datos del trabajo pueden dañarse. No hay reglas claras escritas. Manejar fallos de seguridad es solo reaccionar. No hay estudio fijo de peligros. Por esto, surge una duda. ¿De qué modo mejoramos la seguridad aquí? Esto se logra poniendo un sistema ISO 27009. El reto es poner buenas formas mundiales. Se debe ver el modo de la alcaldía. Hay que pensar en el dinero y las leyes de ahora. El fin es cuidar muy bien la información del ente. También se deben proteger los servicios al público

1.2 Descripción del problema

A nivel internacional, la norma ISO/IEC 27009 ofrece directrices sectoriales para complementar la ISO/IEC 27001. Por ejemplo, la Municipalidad de Chorrillos en España adoptó la ISO/IEC 27009 para reforzar la seguridad en su sede, enfrentando desafíos como deficiencias en la protección de procesos y una limitada proyección a mediano plazo. Un representante del comité ISO destacó que la ISO/IEC 27009 es muy útil para perfeccionar la arquitectura de protección de la información y consolidar buenas prácticas de privacidad.

En el contexto nacional, nuestra Municipalidad Distrital de Chorrillos también ha buscado mejorar sus servicios mediante tecnologías avanzadas y normas ISO. Actualmente cuenta, por ejemplo, con certificaciones ISO 9001:2008 (mejora de procesos y redes seguras), ISO 14001 (gestión ambiental en infraestructura tecnológica), e ISO/IEC 27001 (normativa general de SGSI). Además, sus contratos de servicios de telecomunicaciones (telefonía fija,

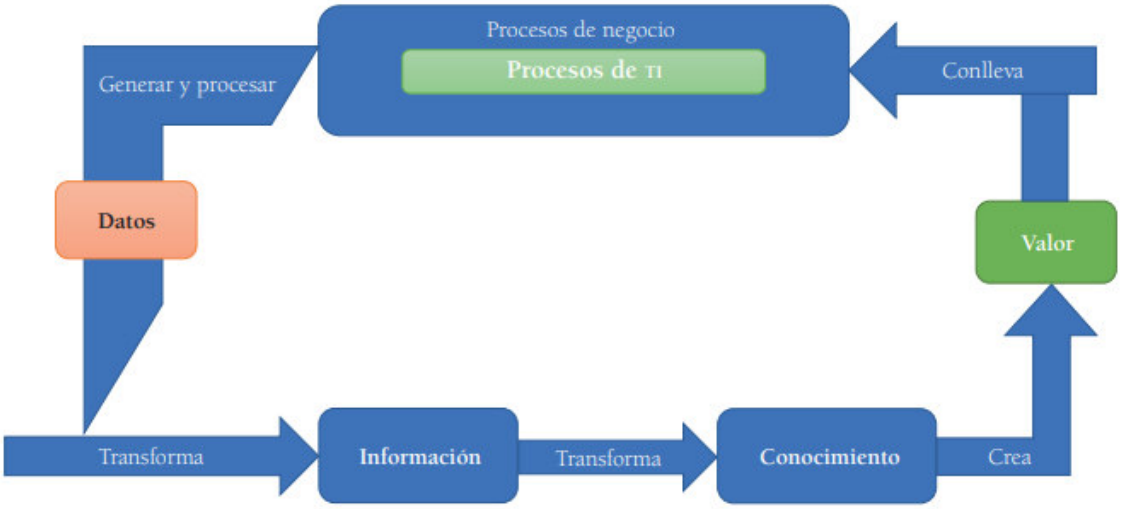
móvil) han sido renovados periódicamente hasta 2027, demostrando una apuesta por la infraestructura de comunicaciones.

Por otro lado, la municipalidad ha estudiado la percepción ciudadana sobre la privacidad en Internet. En una encuesta reciente, el 83,5% de los encuestados otorgó una puntuación entre 7 y 10 en su confianza sobre el manejo de sus datos personales, e incluso el 55,3% calificó con 10 dicha confianza. Esto refleja una valoración alta de la gestión de privacidad por parte de la población. Asimismo, el 65,7% de los participantes consideró importante tener la posibilidad de bloquear accesos no deseados a sus datos sensibles (bancarios, de salud, etc.). Estos hallazgos sugieren que proteger la información personal es una expectativa clave de los ciudadanos y refuerzan la urgencia de mejorar la seguridad de los sistemas municipales

Por ello, la aplicación de la norma ISO/IEC 27009 representa una alternativa técnica para fortalecer la prevención de riesgos del sistema de información en la Municipalidad Distrital de Chorrillos. Su incorporación permitiría orientar la gestión de controles, mejorar la identificación de riesgos, proteger información sensible y contribuir a la continuidad de los servicios municipales. En consecuencia, la presente investigación busca analizar de qué manera la aplicación de la norma ISO/IEC 27009 contribuye a la prevención de riesgos del sistema de información, considerando principalmente las dimensiones de disponibilidad y confidencialidad.

Figura 1

Transformación de datos en información y conocimiento para la gestión institucional



Nota. Elaboración propia para representar la relación entre datos, información, conocimiento y toma de decisiones institucionales.

En el tiempo de la pandemia, la Alcaldía de Chorrillos buscó seguir trabajando bien. También quiso cuidar la salud de sus empleados. Por eso, se empezó a usar el trabajo desde casa. Este cambio fue importante. Pero mostró fallas en lo digital. Había riesgos como el robo de identidad y el ciberataque. También se vio el hurto de claves y fallos en la seguridad de las computadoras (Telefónica del Perú, 2020). Estos problemas mostraron algo claro. No toda la información del gobierno es igual de privada. Ciertos datos necesitan una defensa más fuerte.

En tiempos normales, se cree que los empleados y la gente pueden usar internet. Esto es para hacer trámites o preguntar cosas. No deberían enfrentar peligros al hacerlo. Pero se sabe que dar datos propios en línea causa problemas. Esto pasa si criminales los consiguen. Estos datos son cuentas de banco, dónde vive la gente o copias de documentos. El problema crece mucho más. Esto ocurre si la información compartida tiene cosas muy privadas o médicas. Esos datos se pueden usar mal.

1.3 Formulación del problema

Con base en lo expuesto en el planteamiento, se formulan las siguientes interrogantes de investigación:

1.3.1 Problema general

¿De qué manera la aplicación de la norma ISO/IEC 27009 permite prevenir los riesgos del sistema de información en la Municipalidad Distrital de Chorrillos?

1.3.2 Problemas específicos

- ¿En qué medida la aplicación de la norma ISO/IEC 27009 influye en la disponibilidad del sistema de información de la Municipalidad Distrital de Chorrillos?
- ¿En qué medida la aplicación de la norma ISO/IEC 27009 influye en la confidencialidad del sistema de información de la Municipalidad Distrital de Chorrillos?

1.4 Antecedentes

Diversos estudios previos ofrecen contexto relevante para nuestro trabajo. Por ejemplo, investigaciones internacionales han demostrado la eficacia de integraciones tecnológicas de seguridad:

Noguera (2019) implementó un sistema de detección de intrusos (IDS/IPS) y firewalls en una empresa del sector industrial, logrando identificar ciberataques en tiempo real. En el ámbito de las telecomunicaciones, Ortelli (2018) estudió la adopción de normativas de seguridad en una compañía moderna, resaltando que grandes ciberataques globales han llevado a las organizaciones a reforzar su seguridad y capacitar a profesionales especializados. En el sector energético, Heffel (2016) investigó la ciberseguridad en redes eléctricas de EE.UU., examinando cómo exmiembros de unidades de guerra cibernética gestionan la defensa de sistemas críticos ante amenazas.

En su investigación, Ortelli (2018) exploró la regulación de la seguridad cibernética en relación con Gandalf Comunicaciones C. A. Su principal propósito fue examinar cómo se maneja la seguridad dentro de organizaciones contemporáneas, sobre todo en un contexto de amenazas cibernéticas en aumento. Según el autor, los ataques informáticos que han afectado a importantes empresas globales han llevado a las organizaciones a ser más conscientes de la imperiosa necesidad de salvaguardar sus sistemas de información. Además, se enfatizó la relevancia de disponer de expertos altamente calificados, que estén familiarizados con protocolos, nuevas tecnologías y normas internacionales en el ámbito de la seguridad digital.

Finalmente, Heffel (2016), en su estudio sobre la ciberseguridad en la industria eléctrica, buscó clarificar el concepto de seguridad informática en el entorno industrial, además de investigar la manera en que los sistemas de distribución eléctrica manejan las amenazas cibernéticas. A través de entrevistas con antiguos trabajadores de contratistas del gobierno de Estados Unidos y expertos en ciberamenazas, el autor estableció una conexión entre áreas tecnológicas y los entornos industriales. Según sus descubrimientos, estos individuos tienen habilidades técnicas que, si se emplean de manera inapropiada, podrían poner en grave riesgo los sistemas de energía.

Aguilar-Coronel y Cuenca-Tapia (2025) Hicieron un plan de manejo de datos seguros. Este plan se basó en la regla ISO/IEC 27001. Fue para la firma EJEPROY. Vieron un gran problema allí. Faltaban reglas de cuidado propias para la obra. Esto hizo que la información corriera más riesgos. El estudio miró mucho la regla 27001. Pero su forma de hacer las cosas sigue a la ISO/IEC 27009. Esta regla ayuda a cambiar las reglas de la 27001. Así se hacen aptas para cada tipo de negocio. El fin era crear un plan de seguridad. Este plan usaría la vista de peligros y pondría medidas de cuidado hechas a la medida. Esto debía frenar peligros como entradas sin permiso. También pararía fugas de datos y virus malos. Los creadores vieron algo importante. Adaptar las medidas al sitio de trabajo es clave. Este es un punto central de la ISO

27009. Es vital para manejar bien los riesgos. Sugirieron usar reglas claras como la 27009. Esto mejorará cómo se cuidan los sistemas. Es cierto sobre todo en campos con requerimientos propios, como es la construcción.

Al examinar las investigaciones sobre seguridad informática, tanto las realizadas en Perú como las internacionales, se identifican varias tácticas clave para fortalecer la protección de los datos en instituciones públicas, como la Municipalidad de Chorrillos. Por ejemplo, Peña (2016), en su trabajo con la empresa C-Internet S.A., investigó la implementación del protocolo LDAP en las redes privadas virtuales (VPN) de uso corporativo, que sirven para proteger las conexiones de acceso remoto. Su estudio demostró que al integrar LDAP, se mejora considerablemente la autenticación de los usuarios, abarcando desde el inicio de sesión en Windows hasta el acceso final a través de la VPN. Además, Peña sugiere dos medidas esenciales para mantener la seguridad a largo plazo: auditar los sistemas de red periódicamente y mantener actualizadas las licencias de software (Peña, 2016).

En el ámbito de la ciberseguridad para pymes, un equipo de investigadores (Antunes et al., 2022) desarrolló una plataforma web personalizable para gestionar el cumplimiento normativo en auditorías de seguridad. Partieron de una realidad conocida: las herramientas existentes suelen ser costosas, muy rígidas y están pensadas para grandes corporaciones, lo que deja a las organizaciones más pequeñas en desventaja y limita muchísimo su adopción. Así, su objetivo principal fue crear un sistema genérico y accesible, basado en web, que permitiera cargar listas de controles a medida y generar informes de auditoría de forma automática. ¿El resultado? En pruebas reales con 50 pymes, la plataforma demostró ser una herramienta flexible y muy eficaz. Permitió realizar auditorías tanto parciales como completas bajo el estándar ISO 27001, y mostró un gran potencial para estandarizar procesos, centralizar la gestión y, algo muy valioso, facilitar la autoevaluación de ciberseguridad. En esencia, lograron brindar a las pymes un apoyo tangible y adaptado a sus necesidades reales.

Desde el sector financiero mexicano, un interesante estudio de Hernández y Torres (2021) abordó un desafío muy concreto: los marcos genéricos de ciberseguridad a menudo pasaban por alto amenazas específicas y muy dañinas, como el fraude electrónico o la suplantación de identidad. Partiendo de esta problemática, los investigadores desarrollaron un marco basado en la ISO/IEC 27009, con el claro objetivo de crear controles personalizados que mitigaran no solo riesgos operativos, sino también aquellos reputacionales, tan críticos en el ámbito financiero. Los resultados fueron alentadores: la implementación demostró una mejora del 40% en la capacidad de respuesta ante incidentes. Su conclusión fue clara: adoptar la ISO/IEC 27009 como base para esquemas sectoriales es una estrategia muy sólida.

Gestión integral en el sector público

Por otro lado, Rocha (2019) dirigió su mirada al sector público, analizando cómo se gestiona la seguridad de la información en organismos estatales. Su trabajo, basado en la norma ISO/IEC 27001, subraya algo fundamental: la importancia de garantizar la confidencialidad, integridad y disponibilidad de la información. Entre las brechas más significativas que identificó, destaca una que suele ser común: la falta de un reconocimiento formal y una valoración clara de los activos, tanto tangibles como intangibles. Este hallazgo es crucial, pues sin un inventario exhaustivo y bien clasificado, es muy difícil priorizar recursos y asignar los niveles de protección que realmente se necesitan.

La cultura como pilar de la seguridad

Más allá de los marcos y las normas, la cultura organizacional juega un papel determinante. Rodríguez (2019) lo comprobó al estudiar empresas proveedoras de Software como Servicio (SaaS). Su conclusión es reveladora: fomentar una cultura sólida de gestión de riesgos no es un complemento, sino un factor que facilita respuestas ágiles y adaptativas ante entornos cambiantes. Esta mentalidad, según el estudio, empuja a las personas y a los equipos

a adoptar posturas más críticas y creativas frente a las amenazas. Para una institución como una municipalidad, inculcar esta cultura podría marcar la diferencia, permitiendo al personal reaccionar con mayor rapidez y eficacia ante cualquier incidente.

Modelos metodológicos adaptables

En cuanto a metodologías concretas, encontramos aportes valiosos en distintos sectores. Por ejemplo, Banda (2019) desarrolló un modelo para el sector agroindustrial, pensado específicamente para mejorar la seguridad de los activos tecnológicos. De forma complementaria, García (2018) Creó un plan centrado en cuidar el medio ambiente. Lo bueno de esas dos situaciones es que usaron normas y formas de trabajo. Estas se pueden aplicar bien a otras empresas si se ajustan con cuidado. Por cierto, expertos vieron el plan de García como lógico y completo. Juntos, estos trabajos enseñan que el gobierno puede mirar ejemplos de otros campos. Así pueden organizar sus propios sistemas para manejar peligros.

El mirar la protección de datos, sobre todo al poner reglas como la ISO 27009, ha sido tema de mucha pesquisa en todo el mundo y aquí mismo. Por esto, los escritos sobre usar esta regla en varios campos muestran que se necesitan estructuras. Estas estructuras deben ajustar las medidas de cuidado a lo propio de cada grupo. Ahora, veremos algunos hechos importantes sobre este tema.

En un trabajo de Noguera (2019), se vio cómo usar un modo para encontrar gente rara dentro de Vidrio de Venezuela, S.A. Se observó la manera de poner normas de tecnología. Estas normas tomaron como base las guías ISO. Esto es para mejorar el cuidado digital. El estudio vio que mirar bien los riesgos y saber usar los sistemas de defensa fue vital. Esto hizo que hubiese menos fallos en la red de esa firma. Este ejemplo prueba que seguir un modo fijo es muy necesario. Ese modo es el que da ISO/IEC 27009 para guardar bien todos los datos.

A nivel del país, Ortelli (2018) en su estudio sobre el cuidado digital en firmas de Venezuela, recalcó algo. Los ataques nuevos a empresas grandes hicieron crecer el saber. Se vio la necesidad de hacer mejor el cuidado de la data. Su estudio dijo que formar a la gente y usar normas mundiales como ISO 27001 era clave. Esto es para hacer frente a los peligros del ciberespacio. Este punto se junta con lo que dice ISO/IEC 27009. Esta norma fija reglas de defensa por sector. Esto mejora el cuidado de datos. Esto aplica al sector privado y también a las oficinas del Estado.

Sobre trabajos locales, García (2018) sugirió un plan de datos seguros para el Estado en Lambayeque. Este plan usó la norma ISO 27001 como base. La investigación resaltó cuán importante es saber qué bienes de datos hay. También es clave ver los riesgos de la información en sitios del Estado. El estudio mostró que, si bien se hacen cosas, aún faltan pasos. Hay huecos al poner todos los controles de defensa. Esto pasa también en sitios del municipio como la Alcaldía de Chorrillos. Poner en práctica ISO/IEC 27009 podría ayudar a llenar esos vacíos. Así se haría más fuerte la defensa en las sedes del gobierno.

De igual forma, Peña (2016) destacó la relevancia de la protección de datos mediante el uso de redes privadas y sistemas de autenticación, en el contexto de la seguridad de la información en empresas como C-Internet S.A. Su estudio mostró que la autenticación remota y los sistemas cifrados son herramientas eficaces para proteger la confidencialidad de la información. Esta investigación resalta un aspecto esencial de la norma ISO/IEC 27009: la protección de datos sensibles y su adaptación a las necesidades del sector específico.

La propuesta de Rocha (2019) sobre modelos de gestión de seguridad en el sector público también es relevante, ya que su investigación señala que la gestión de riesgos y la aplicación de políticas de seguridad son fundamentales para garantizar la confidencialidad, integridad y disponibilidad de la información en las entidades gubernamentales. En este sentido, la norma ISO/IEC 27009 ofrecería a la Municipalidad de Chorrillos un marco claro y

específico para gestionar la seguridad de su información, adaptado a las características y necesidades del sector público.

Finalmente, Dejan Kosutic (2019) Dice que poner en marcha la ISO/IEC 27009 es difícil. Esto se debe a que el proceso es complicado. Implica muchas tareas distintas a través del tiempo. Poca gente o poco dinero pueden ser un gran problema. Pero, si hay un plan bueno y correcto, las empresas logran proteger bien sus datos. Esta idea va junto con lo que piensa la Municipalidad de Chorrillos. Ellos necesitan los medios suficientes para aplicar bien la norma.

¿Qué significa todo esto para la Municipalidad de Chorrillos?

En resumen, estas investigaciones pintan un panorama claro. Para una entidad como la Municipalidad de Chorrillos, la ruta hacia una seguridad más robusta pasa por considerar soluciones tecnológicas seguras, alinearse con estándares internacionales adaptados a su contexto, implementar auditorías periódicas y, quizás lo más transformador, fomentar una cultura organizacional consciente del riesgo. Al integrar estas lecciones, la municipalidad no solo protegería mejor sus activos digitales, sino que garantizaría con mayor solidez la confidencialidad de la información y la continuidad de los servicios públicos que ofrece a la ciudadanía.

1.5 Justificación de la investigación

Justificación Tecnológica

Las formas de la información mueven un cambio grande en el manejo del gobierno. Esto hace que los procesos de adentro sean mejores. En este punto, poner la regla ISO/IEC 27009 en la Ciudad de Chorrillos es un paso clave. No solo es seguir una medida. Es poner la

base para un método de manejo de seguridad firme. Este método debe ajustarse a lo que necesitan.

Este método dejará, de forma real, hacer automático el mirar los fallos en los servicios a la gente. La meta es simple. Se debe asegurar que la data importante esté siempre segura. Pero también debe estar lista y lista para usarse si hace falta. También, al juntar toda la data de fallos en un sitio, los empleados verán datos pasados muy rápido. Esto importa mucho. Quiere decir que se aprende de lo que pasó. Mejora cómo se arreglan las fallas que se repiten. Permite actuar antes de que sucedan.

En resumen, aparte de cuidar los datos y hacer mejor la maquinaria, este plan completo ayudará a evitar peligros de internet. Y algo igual de vital: subirá mucho la eficiencia del manejo de los servicios para el público. Al final, el objetivo es hacer un gobierno más rápido. Uno que se pueda creer y que esté listo para los retos de hoy en lo digital.

Justificación institucional

Al implementar la norma ISO/IEC 27009, la Municipalidad de Chorrillos ganará un control mucho más efectivo y transparente sobre las incidencias de seguridad y los sistemas municipales. No se trata solo de seguir un protocolo, sino de contar con una herramienta que organiza y da sentido a la información. Como bien señaló Méndez (2006), “esta herramienta facilita el acceso a una gran cantidad de información previamente analizada y disponible al ser requerida, lo que permite tomar decisiones más acertadas” (p. 51). Es decir, con un sistema de gestión basado en esta norma, la municipalidad podrá mantener un registro ordenado y accesible de lo ocurrido durante el año. ¿La ventaja? Mejorará notablemente la calidad del servicio y, algo fundamental, fortalecerá la confianza de la ciudadanía en la gestión pública. Este enfoque no solo hace que las decisiones sean más informadas y precisas, sino que también optimiza los recursos de la institución. Al final, se reflejará en una mejor percepción pública

sobre la eficacia y, sobre todo, la transparencia de la gestión municipal. Se construye, paso a paso, una administración más confiable.

Justificación operativa

En el nivel operativo, el nuevo sistema facilitará la gestión diaria de incidentes. Actualmente no existe un método eficiente para documentar y priorizar las incidencias en la municipalidad, lo que conlleva pérdida de tiempo y recursos. Con la implementación propuesta, será posible generar informes detallados con gráficos e indicadores de gestión (Zambrano, 2011), ayudando a los responsables a priorizar la atención según el impacto. Además, se simplificarán las auditorías internas, mejorando la capacidad de la municipalidad para corregir y prevenir incidentes de seguridad

Justificación económica

Adoptar la ISO/IEC 27009 es también una inversión inteligente. Según Laudon y Keylor (2014), un proyecto de TI no debe verse como un gasto sino como una inversión con beneficios futuros. En la situación actual, resolver incidencias de seguridad implica costos significativos (desplazamientos, horas extra del personal técnico, etc.). Con el nuevo sistema se proyecta reducir aproximadamente un 44% de esos costos mensuales, ya que las incidencias se gestionarán de manera más eficiente y remota. Este ahorro permitirá destinar los recursos públicos a otras necesidades, sin sacrificar la calidad del servicio.

1.6 Limitaciones de la investigación

Este estudio presenta las siguientes limitaciones, que delimitan su alcance y las conclusiones que se puedan extraer:

Ámbito institucional: Es importante destacar que este estudio se circunscribe exclusivamente al ámbito de la Municipalidad Distrital de Chorrillos. Nos hemos centrado en

sus condiciones y necesidades particulares, lo que significa que los hallazgos y las recomendaciones están pensados específicamente para este contexto. Por ello, los resultados no pueden aplicarse directamente a otras municipalidades u organizaciones con realidades diferentes; su alcance es, deliberadamente, local.

Alcance de la seguridad: En cuanto a la seguridad, nuestro trabajo con la norma ISO/IEC 27009 se ha enfocado principalmente en mejorar dos pilares fundamentales para la municipalidad: la disponibilidad y la confidencialidad de sus sistemas de información. Hemos priorizado estas dimensiones porque fueron identificadas como las más críticas en una primera evaluación. Sin embargo, esto implica que otros aspectos igualmente importantes, como la integridad de la información, no serán tratados en profundidad en este proyecto. Es una delimitación consciente, para poder concentrar nuestros esfuerzos donde más se necesitaban. **Recursos y tiempo:** Finalmente, es esencial ser realistas sobre los recursos y el tiempo. Todo el análisis y las propuestas de implementación se han diseñado considerando un período determinado y los recursos disponibles de la institución. En la práctica, algunas de las medidas de seguridad recomendadas podrían no desplegarse por completo durante el desarrollo de esta investigación, sino plantearse como una hoja de ruta para el futuro. Además, la información recopilada —como datos de pruebas o evaluaciones de riesgo— depende de la colaboración y los insumos proporcionados por la municipalidad dentro de los plazos del estudio. Por todo esto, al interpretar los resultados, debemos tener presente que algunos beneficios de aplicar la norma ISO/IEC 27009 podrían apreciarse plenamente a medio o largo plazo, o requerirían de recursos adicionales para una implementación integral.

1.7 Objetivos

1.7.1 Objetivo general

El objetivo general de la investigación es determinar la influencia de la aplicación de la norma ISO/IEC 27009 en la prevención de los riesgos del sistema de información

en la Municipalidad Distrital de Chorrillos. A través de este estudio, se busca evaluar cómo esta norma puede contribuir a mejorar la seguridad de la información manejada por la municipalidad, protegiendo tanto los datos sensibles de los ciudadanos como la infraestructura tecnológica utilizada por la entidad

1.7.2 Objetivos específicos

- Determinar la influencia de la aplicación de la norma ISO/IEC 27009 en la disponibilidad del sistema de información de la Municipalidad de Chorrillos. Este objetivo se centrará en analizar cómo la implementación de la norma puede garantizar que los sistemas de información estén siempre operativos y accesibles para los usuarios, minimizando el riesgo de interrupciones.
- Evaluar la influencia de la aplicación de la norma ISO/IEC 27009 en la confidencialidad del sistema de información de la Municipalidad de Chorrillos. Este objetivo buscará determinar cómo la norma mejora la protección de los datos sensibles y personales de los ciudadanos, asegurando que solo las personas autorizadas tengan acceso a esta información

II. MARCO TEÓRICO

2.1 Marco conceptual

La seguridad de la información

La protección de datos se centra en tres puntos clave: guardar el secreto, mantener lo correcto y asegurar que sirva. En toda empresa, la seguridad implica usar reglas, métodos y herramientas. El fin es que solo gente apta vea la información. También se busca que los datos sean ciertos y que siempre estén listos. Este tema es muy importante para el gobierno. Allí se manejan muchos datos delicados (como datos de la gente, impuestos y salud). Por eso, proteger la información no es solo cosa de técnicos. Es un deber de toda la entidad. Hay que crear una mentalidad que cuide bien esos archivos (ISO, 2016).

Un modelo usado mucho para esto es la norma ISO/IEC 27001. Esta norma se puede certificar. Fija lo que se debe hacer para montar, usar y seguir un Sistema de Gestión de Seguridad (SGSI). Humphreys (2016) dice que usar ISO 27001 da a las firmas un modo ordenado. Se miran los peligros. Luego se deciden qué medidas tomar y se cuidan bien los bienes de la computación. Si el Municipio de Chorrillos usa ISO 27001, podrá ver sus cosas vitales. Luego verá los riesgos propios y pensará en formas buenas de bajarlos. Además, la ISO 27001 usa el ciclo de mejorar siempre (Pensar–Hacer–Chequear–Actuar). Esto hace que el SGSI crezca para enfrentar nuevos daños.

En este punto, la norma ISO/IEC 27009 ayuda. La ISO 27001 da ideas para todos. En cambio, la ISO 27009 da reglas para el sector público. Ayuda a mejorar los pasos de la ISO 27001 con los riesgos del municipio. Por ejemplo, esta norma mira daños que son propios de lo público. Esto incluye ver quién entra sin permiso a las listas de ciudadanos o cambiar datos de servicios básicos (Kosutic, 2019). En corto, la ISO 27009 adapta el modo de seguridad al sitio de la alcaldía. Así se cuida mejor la información que manejan.

Aparte de poner las normas, cuidar la información necesita planes que sigan. Es vital enseñar al personal sobre seguridad. Se deben crear políticas claras y revisar los sistemas a menudo. Peña (2016) dice que crear una idea de seguridad es vital. No basta con poner máquinas de control. Todo el personal debe entender y seguir las reglas. Así, la seguridad pasa de ser solo técnica. Se vuelve una meta que todos comparten en la entidad.

2.1.1 Marco Normativo Ampliado: La Familia ISO/IEC 27000 - Un Ecosistema de Seguridad

El grupo ISO/IEC 27000 es mucho más que una simple colección de reglas. Tal como indican Calder y Watkins (2020), esto es un verdadero jardín de cosas unidas y pegadas, donde cada regla tiene una misión concreta y, lo crucial, se toca y ayuda a las otras (p. 45). Esta idea la tiene también Itrad (2019), quien la imagina como un andamiaje escalonado y de apoyo mutuo, donde cada pedazo se hace más fuerte gracias a los vecinos (p. 78).

A. Normas Fundamentales o "El Núcleo del SGSI"

Podríamos decir que estas normas son los cimientos esenciales. Sin ellas, simplemente no puede existir un Sistema de Gestión de Seguridad de la Información efectivo, tal como apunta Fernández (2021, p. 93).

ISO/IEC 27000: Visión general y vocabulario

Esta norma es la piedra angular, el punto de partida que sienta las bases terminológicas para todo lo demás (Calder, 2019, p. 112). Define con precisión términos clave como "activo de información", "amenaza", "riesgo" o "incidente de seguridad" (Watkins, 2022, p. 67). ¿Por qué es tan crucial, especialmente en investigación? Como explica Itrad (2020), garantiza que todos —investigadores y lectores— hablemos el mismo idioma técnico, evitando confusiones y ambigüedades (p. 145).

ISO/IEC 27001: Requisitos

Esta es la norma certificable, el estándar que establece los requisitos mínimos que una organización debe cumplir para implementar y mantener un SGSI (Fernández, 2021, p. 105). Incluye componentes críticos como el contexto de la organización, el liderazgo y la planificación basada en riesgos (Calder, 2020, p. 88). Un elemento central es la Declaración de Aplicabilidad (SoA), un documento vivo que lista los controles elegidos de la ISO 27002 (Watkins, 2022, p. 156). En pocas palabras, la ISO 27001 actúa como el "paraguas" bajo el cual se aplica la norma sectorial ISO 27009, alimentando directamente esa SoA (Itrad, 2019, p. 134).

ISO/IEC 27002: Código de práctica para controles

Podemos ver esta norma como el catálogo de referencia. No es certificable por sí sola, pero proporciona la guía práctica indispensable para implementar los controles (Calder & Watkins, 2020, p. 172). Su estructura se organiza en pilares fundamentales: controles organizativos, sobre las personas, físicos y tecnológicos (Fernández, 2021, p. 118). Para la sectorización, es la "materia prima" que la ISO 27009 modifica y adapta; sin ella, el proceso carecería de fundamento (Itrad, 2020, p. 167).

B. Normas de Soporte Específico

Estas normas son como las herramientas especializadas que nos ayudan a profundizar en aspectos críticos del SGSI (Watkins, 2022, p. 203).

ISO/IEC 27003: Funciona como una guía paso a paso para implementar la ISO 27001, llena de ejemplos prácticos (Calder, 2019, p. 195).

ISO/IEC 27004: Responde a la pregunta clave: "¿cómo sé si mi SGSI realmente funciona?" Desarrolla métricas para medir el desempeño y la eficacia de los controles (Itrad, 2020, p. 178).

ISO/IEC 27005: Es el manual de gestión de riesgos de la familia, describiendo el proceso completo desde el análisis hasta el tratamiento (Fernández, 2021, p. 162). Su flexibilidad permite usar metodologías cualitativas o cuantitativas (Calder, 2020, p. 145). Es fundamental, porque el proceso de la ISO 27009 se alimenta directamente de sus resultados: es el análisis de riesgos sectorial el que indica qué controles deben adaptarse (Itrad, 2019, p. 156).

Normas Sectoriales (El Dominio de la ISO/IEC 27009)

Aquí es donde la ISO/IEC 27009 despliega todo su potencial, generando normas especializadas para sectores con necesidades muy concretas (Watkins, 2022, p. 234).

ISO/IEC 27009: Especificaciones para la creación de normas sectoriales

Esta norma actúa como la "constitución" o el marco de reglas para la adaptación (Fernández, 2021, p. 189). Su proceso es riguroso: implica analizar el sector objetivo y hacer un mapeo exhaustivo con la ISO 27002 (Itrad, 2020, p. 201). Sus reglas permiten añadir, modificar, refinar o incluso suprimir controles, siempre y cuando exista una justificación sólida (Calder, 2019, p. 167).

Ejemplos Emblemáticos de Normas Sectoriales:

Estos son el resultado tangible de aplicar la ISO 27009. Por ejemplo:

ISO/IEC 27011 (Telecomunicaciones): Añade controles específicos para la seguridad en redes y servicios de comunicaciones (Itrad, 2020, p. 213).

ISO/IEC 27017 (Cloud Computing): Aclara la responsabilidad compartida entre proveedor y cliente, y añade controles para entornos en la nube (Fernández, 2021, p. 201).

ISO/IEC 27019 (Sector Energético): Proporciona guías especializadas para sistemas de control de procesos en infraestructuras críticas (Calder, 2019, p. 178).

Marco Específico: La Norma ISO/IEC 27009 y la Sectorización

¿Por qué es tan necesaria esta especificidad? Porque un enfoque genérico tiene limitaciones evidentes. Los riesgos, el impacto operacional y los requisitos legales varían

enormemente entre un hospital, un banco y una empresa de cloud computing (Itrad, 2019, p. 145). La ISO 27002 por sí sola puede resultar insuficiente cuando se enfrenta a realidades sectoriales tan específicas (Fernández, 2021, p. 203).

La teoría es clara: la seguridad óptima solo se logra cuando los controles están perfectamente alineados con el contexto y los riesgos particulares de un sector (Watkins, 2022, p. 312). En otras palabras, la efectividad de un control es directamente proporcional a cuán bien esté adaptado a su entorno operativo específico (Calder, 2019, p. 167).

En esencia, la norma ISO/IEC 27009:2016 establece el camino para esta adaptación. Guía a organizaciones y sectores enteros en la personalización de los controles de la ISO 27001, lo que facilita una gestión de riesgos mucho más precisa y efectiva. Su objetivo final es potente: prevenir riesgos en los sistemas de información mediante la contextualización de controles, evitando así aplicar medidas que puedan ser, a la vez, innecesarias *e* insuficientes. Es el puente entre la teoría general y la práctica especializada.

2.1.2 Normas ISO para la seguridad de la información

Las normas ISO/IEC 27001 e ISO/IEC 27009 son, en realidad, dos caras de una misma moneda cuando se trata de construir políticas de seguridad de la información realmente efectivas. Veamos cómo funcionan y por qué importan.

La ISO/IEC 27001 es ampliamente reconocida a nivel global como la base para proteger la información. Lo que hace es establecer los requisitos para crear, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI). Es decir, proporciona el esqueleto, la estructura que organizaciones de todos los tamaños y sectores pueden seguir (Humphreys, 2016).

Para la Municipalidad Distrital de Chorrillos, adoptar esta norma representaría una gran ventaja. Le permitiría, de manera sistemática, identificar sus activos de información más críticos, evaluar los riesgos reales a los que se enfrenta y diseñar estrategias concretas para

mitigarlos. Además, no es un esfuerzo de una sola vez: la ISO 27001 se basa en el ciclo de mejora continua Planificar-Hacer-Verificar-Actuar (PDCA), lo que garantiza que el sistema evolucione y se adapte con el tiempo. Ahora, aquí es donde entra su complemento esencial: la ISO/IEC 27009. Si la 27001 es el esqueleto genérico, la 27009 es la guía que ayuda a adaptar ese esqueleto a la contextura específica de cada sector. Para una entidad como la Municipalidad de Chorrillos, esto es invaluable. Esta norma permitiría ajustar y especificar los controles de seguridad para abordar las necesidades, vulnerabilidades y riesgos particulares del sector público. Proporciona un marco pensado, por ejemplo, para manejar de forma segura el intercambio de datos entre agencias gubernamentales, proteger la información sensible de los ciudadanos y garantizar la continuidad de los servicios públicos esenciales. Implementar estas normas es un proceso que requiere compromiso. Comienza con un análisis exhaustivo de los riesgos de la organización. A partir de ahí, se adoptan medidas correctivas que van desde controles tecnológicos hasta algo igual de importante: la capacitación continua del personal (Kosutic, 2019). En este punto, el rol del liderazgo es absolutamente crucial. Los directivos de la municipalidad deben estar plenamente involucrados, asignando los recursos necesarios y asegurándose de que toda la organización comprenda y se alinee con estas políticas de seguridad. Sin este compromiso desde la cima, el esfuerzo difícilmente prospera.

2.2 El riesgo en la gestión de la seguridad de la información

En el núcleo de la seguridad de la información está el concepto de riesgo. Podríamos definirlo como la posibilidad de que una amenaza cualquiera —un ciberataque, un error humano, una falla técnica— encuentre y aproveche una debilidad en nuestros sistemas, causando un daño real a la información de la organización. Como bien explica Kosutic (2019), para evaluarlo correctamente debemos considerar dos factores: la probabilidad de que ese evento ocurra *y* el impacto que tendría si llegara a materializarse. Esta evaluación no es solo

un trámite; es la base fundamental para tomar decisiones informadas sobre dónde y cómo invertir nuestros esfuerzos de protección.

Para la Municipalidad Distrital de Chorrillos, este proceso adquiere una urgencia particular. Se trata de gestionar el riesgo asociado a sistemas que contienen datos altamente sensibles: desde registros civiles e información fiscal hasta reportes de salud y datos personales de los vecinos. Una evaluación rigurosa permite identificar las amenazas que podrían comprometer la confidencialidad o la integridad de esta información, y lo más importante, priorizar las acciones correctivas. Siguiendo a Ortelli (2018), una evaluación efectiva pasa por hacer un inventario claro de nuestros activos, reconocer las amenazas más probables y, recién entonces, establecer las medidas de protección más adecuadas.

Pero hay un punto crucial: gestionar el riesgo no se reduce a instalar firewalls o software antivirus. Como señala Peña (2016), implica también capacitar y concientizar al personal, y crear políticas claras que regulen el acceso a la información y definan qué hacer ante una incidencia. En el fondo, es un enfoque integral y colaborativo que debe involucrar a todos los departamentos y empleados. La seguridad, al final, es una responsabilidad compartida.

2.3 Implementación de la norma ISO/IEC 27009

Llevar la norma ISO/IEC 27009 a la práctica en una organización como la Municipalidad de Chorrillos es un proceso que requiere una planificación cuidadosa y metódica. Según Humphreys (2016), el primer paso —y tal vez el más revelador— es realizar una evaluación inicial. Esto nos da una foto clara del estado actual de nuestra seguridad y, sobre todo, de las brechas que existen entre lo que tenemos y lo que necesitamos. Identificadas estas brechas, podemos entonces diseñar e implementar los controles de seguridad adecuados, que siempre serán una combinación de medidas tecnológicas y organizativas.

En este camino, dos elementos son absolutamente claves:

La capacitación continua del personal: Como subraya Kosutic (2019), de poco sirven los controles técnicos más avanzados si el equipo no comprende los riesgos o no sabe cómo actuar. La formación convierte a los empleados de eslabones débiles en la primera línea de defensa.

La gestión del cambio: Es frecuente encontrar resistencia cuando se implementan nuevas políticas. Por eso, el apoyo activo y visible de los líderes de la municipalidad es indispensable. Ellos deben comunicar la importancia de la seguridad, asignar los recursos necesarios y asegurar que toda la organización se alinee con este nuevo rumbo (Peña, 2016).

Finalmente, implementar la norma no es un punto final, sino el comienzo de un ciclo de mejora continua. Se requiere un monitoreo constante y evaluaciones periódicas para asegurar que las medidas siguen siendo efectivas y están alineadas con las mejores prácticas. La seguridad de la información no es un proyecto que se termina; es una práctica viva que debe evolucionar constantemente.

2.4 Sistemas de Información

Tradicionalmente, muchas organizaciones han abordado la seguridad con un enfoque fragmentado: se implementan proyectos aislados para proteger elementos específicos, según surgen las necesidades urgentes, pero sin una visión global e interconectada. Este enfoque reactivo suele tener dos consecuencias: no se cumplen los objetivos de protección a largo plazo y, además, se genera una resistencia natural entre los empleados, quienes pueden ver estos parches de seguridad más como un obstáculo que como una ayuda para su trabajo diario.

Fue esta situación la que impulsó la evolución hacia un concepto más integral: tratar la seguridad como un Sistema de Gestión. La idea es que este sistema no viva aislado, sino que esté plenamente integrado con los demás procesos de la organización, con el objetivo claro de mantener los riesgos en un nivel aceptable. Según la norma ISO/IEC 27000:2018, un sistema

de gestión es precisamente un conjunto de elementos interrelacionados que buscan establecer políticas, metas y procesos para lograr los objetivos de la organización. Es, en otras palabras, una forma estructurada y formal de gestionar cualquier aspecto crítico, incluida la seguridad (Morán Abad et al., 2010).

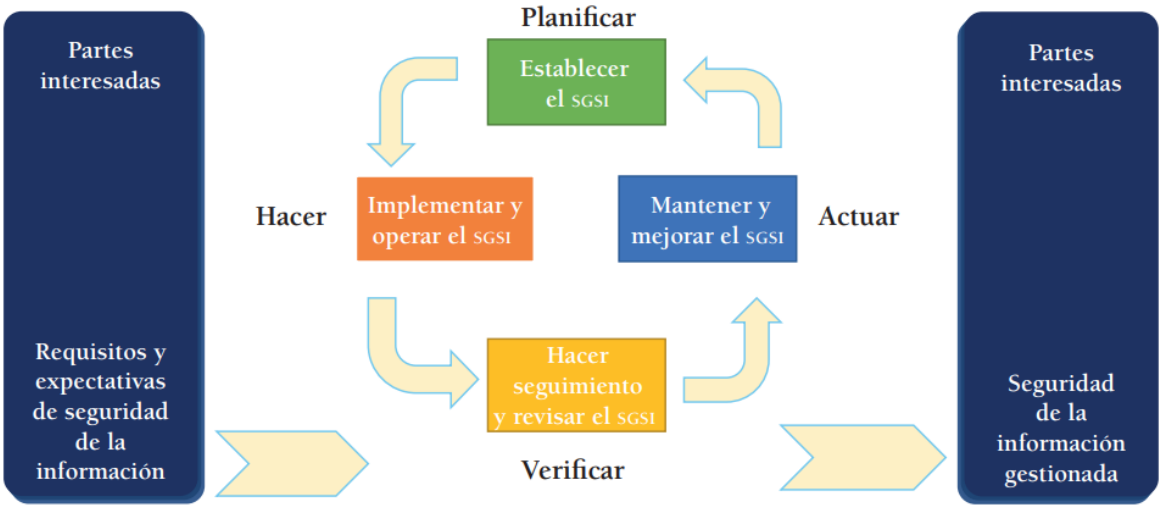
A nivel internacional, el referente para este enfoque es el Sistema de Gestión de Seguridad de la Información (SGSI), basado en la familia de normas ISO/IEC 27000. Y la base operativa de casi todos estos sistemas es el ciclo PHVA (Planificar, Hacer, Verificar, Actuar), también conocido como ciclo de Deming. Este ciclo es el motor de la mejora continua.

Dado que profundizaremos en el SGSI en el próximo capítulo, es útil entender cómo se aplica este ciclo a la seguridad de la información:

Planificar (P): Esta es la fase fundacional. Corresponde a establecer el SGSI: diseñar las políticas, definir los objetivos, y crear los procesos y procedimientos necesarios para gestionar los riesgos y alcanzar el nivel de seguridad que la organización ha decidido aceptar. Es donde se sientan las bases de todo lo que vendrá después.

Figura 2

Ciclo PHVA aplicado a la gestión de seguridad de la información



Nota. Elaboración propia para representar la transformación de los datos en información y conocimiento como soporte para la gestión y protección de los activos de información.

2.5. Diferencias entre seguridad informática, seguridad de la información y ciberseguridad

Es interesante cómo, en el ámbito de la protección digital, a veces usamos términos como si fueran sinónimos. Joyanes Aguilar (2017) nos ayuda a clarificar esta confusión, explicando que la distinción entre seguridad informática, seguridad de la información y ciberseguridad radica realmente en el tipo de recursos que prioriza cada una.

Podríamos pensarlo así:

La seguridad informática se enfoca principalmente en la tecnología en sí: en las infraestructuras, los servidores, las redes y el hardware que gestiona la información dentro de una organización.

La seguridad de la información, en cambio, pone el foco en la protección de la información como un activo estratégico, independientemente de si está en formato digital, en papel o incluso en la mente de las personas. Su valor para la organización es lo central.

Finalmente, la ciberseguridad se refiere específicamente a la protección del mundo digital: la información en formato electrónico y todos los sistemas interconectados que la procesan, almacenan y transmiten (Joyanes Aguilar, 2017).

Aunque las tres comparten la noble finalidad de proteger, sus enfoques son distintos. La seguridad informática se ocupa de lo técnico, de las TIC. La seguridad de la información, por su parte, se concentra en resguardar lo que es esencial para la toma de decisiones. Hay una evolución aquí: antes de la expansión masiva de la tecnología, el concepto predominante era el de seguridad de la información. Hoy, con nuestra profunda dependencia de los sistemas digitales, la seguridad informática se ha convertido también en el medio indispensable para

implementar un buen sistema de gestión de seguridad de la información. Este sistema busca, en última instancia, garantizar la protección de un bien crítico: la información que permite a una organización tomar decisiones acertadas y construir estrategias competitivas.

En esencia, el objetivo de un sistema de gestión es proteger la información porque es un recurso valiosísimo. Esto implica cuidar todos los medios por los cuales esta se genera, se almacena, se procesa y se transmite para convertirse en algo útil para el negocio. Y hoy, sin duda, esos medios incluyen toda la panoplia de tecnologías de la información y comunicación.

Para profundizar, Cano (2011) ofrece una distinción práctica. Define la seguridad informática como la parte táctica y operativa: la que se ocupa de implementar técnicas de protección concretas, como antivirus, firewalls o sistemas de detección de intrusos. Es el "cómo" técnico.

La seguridad de la información, en cambio, es la disciplina más amplia. Abarca la gestión de riesgos y amenazas, el análisis de escenarios, las buenas prácticas y los marcos normativos. Su meta es asegurar procesos y tecnologías para generar confianza en cada etapa del ciclo de vida de la información, desde su creación hasta su eliminación. Es, podríamos decir, la visión estratégica.

Lenguaje de contexto en la seguridad de la información

Podemos pensar en un modelo como un mapa simplificado de la realidad. Es una herramienta que nos permite organizar características complejas y representarlas con un lenguaje común, fácil de entender para todos (Vargas y Parra, 2002). Este lenguaje compartido —con sus términos y conceptos específicos— es fundamental; solo si todos lo comprendemos claramente podremos construir un modelo de seguridad de la información que sea verdaderamente eficaz.

Ahora, dentro de ese modelo, ¿qué le da vida y cohesión? Los procesos de gestión de riesgos. Ellos actúan como el eje central, el mecanismo que integra y hace operativos todos los demás elementos. Por eso decimos que los modelos de gestión de riesgos no son solo una parte,

sino la base misma sobre la cual se desarrolla la seguridad de la información en cualquier organización.

Gestión integral de la seguridad de la información

Por otro lado, el análisis de Rocha (2019) se adentra en los modelos de gestión de seguridad de la información dentro del sector público, planteando estrategias prácticas basadas en la norma internacional ISO/IEC 27001. Su estudio enfatiza algo fundamental: la necesidad de garantizar la confidencialidad, integridad y disponibilidad de los activos informáticos en las instituciones del Estado.

Entre sus observaciones, una de las brechas más importantes que encontró es la falta de un reconocimiento y valoración formal de los activos, tanto los tangibles como aquellos intangibles. Este hallazgo es clave, pues sin una clasificación exhaustiva y consciente de lo que se debe proteger, resulta muy difícil priorizar recursos o asignar los niveles de protección adecuados. En otras palabras, para proteger bien primero hay que saber qué se tiene y qué valor tiene (Rocha, 2019).

Cultura de gestión de riesgos

Un punto vital es el ambiente de trabajo sobre cómo se manejan los peligros. Rodríguez (2019) revisó compañías que dan programas por internet y pensó que impulsar una forma de ver los riesgos ayuda a tener reacciones rápidas cuando las cosas se mueven. Conforme a lo visto, esa forma de pensar anima a la gente y a las agrupaciones a tomar actitudes pensativas y nuevas ante peligros recién llegados. Dentro de lo que hace un ayuntamiento, meter esta idea dejaría que los empleados respondan más deprisa ante fallos de protección o giros en el aparato digital (Rodríguez, 2019).

Modelos metodológicos de gestión de riesgos

Respecto a formas de hacer el manejo de peligros, muchas investigaciones propias de áreas específicas dan datos útiles. Banda (2019) creó una forma en el ámbito de cultivos y

alimentos pensada para hacer más seguras las cosas de computación. Por otro lado, García (2018) pensó una forma de proteger datos enfocada en ayudar con el cuidado del planeta. Los dos trabajos se sirvieron de reglas y caminos que se ajustan al lugar donde se usan. De verdad, expertos dijeron que la idea de García era lógica, importante y completa. Juntos, estos modos de ver muestran que las oficinas del gobierno pueden tomar formas de áreas concretas para organizar sus propios pasos de manejo de riesgos (Banda, 2019; García, 2018).

Implicaciones para la Municipalidad de Chorrillos

En pocas palabras, estos papeles viejos de otros lados y de aquí apoyan el gusto por tomar métodos completos de cuidado digital y manejo de peligros en las oficinas del gobierno. Especialmente, el Ayuntamiento de Chorrillos sacaría provecho de aparatos digitales que no se cuelen (como túneles secretos con llave de nombres de gente) y de ponerse al nivel de las reglas del mundo (algo como la regla 27001 de las señoras ISO/IEC). Poner en marcha revisiones de vez en cuando y promover la costumbre de pensar en los riesgos hará más fuertes sus bracitos para cuidar las cosas digitales del ayuntamiento. Así, el Ayuntamiento asegurará de forma más certera que sus secretos se queden guardados y que sus servicios a la gente sigan andando sin problemas (Peña, 2016; Rocha, 2019; Rodríguez, 2019; Banda, 2019; García, 2018).

Aplicación de ISO/IEC 27009 en la Municipalidad de Chorrillos

La Municipalidad Distrital de Chorrillos maneja algo muy valioso: la información sensible de sus vecinos. Piensa en toda la data confidencial, los registros, los trámites. Por eso, proteger esa información no es solo un deber técnico, sino una responsabilidad de cuidado hacia la comunidad. Se necesitan medidas de seguridad informática robustas, que garanticen de verdad la confidencialidad, integridad y disponibilidad de los datos. La información debe estar segura, íntegra y accesible cuando se necesite.

Esto no es solo una percepción. Numerosos estudios y expertos (como Yáñez, Olivares, Rodríguez y otros a lo largo de los últimos años) han dejado claro algo: en el sector público, es

fundamental contar con políticas formales de seguridad y un enfoque sistemático para gestionar riesgos. La conclusión común es contundente. Adoptar un Sistema de Gestión de Seguridad de la Información (SGSI), basado en estándares internacionales, es la mejor manera de mitigar amenazas cibernéticas y administrar los riesgos de forma ordenada y proactiva.

Aquí es donde entra en juego una herramienta clave: la norma ISO/IEC 27009. Básicamente, se presenta como una guía práctica, una brújula que ayuda a adaptar los lineamientos reconocidos de la familia ISO 27000 al contexto único y específico de la gestión pública. Al usarla, la municipalidad no solo seguiría buenas prácticas, sino que fortalecería de manera tangible la protección de su información, construyendo una confianza más sólida con la ciudadanía a la que sirve.

Norma ISO/IEC 27009 y su enfoque sectorial

La norma ISO/IEC 27009:2020 es, en esencia, una guía que nos ayuda a crear estándares de seguridad a medida para diferentes sectores, partiendo de la base sólida de la ISO/IEC 27001. ¿Qué quiere decir esto exactamente? Pues que esta norma "especifica los requisitos para elaborar normas sectoriales específicas que complementen o incluso ajusten la ISO/IEC 27002, pensando en las necesidades únicas de un ámbito concreto".

Dicho de un modo más sencillo, la ISO 27009 sirve precisamente para eso: para afinar, personalizar y ampliar los controles de seguridad, adaptándolos a la realidad y los riesgos específicos de un dominio particular. Para la Municipalidad de Chorrillos, esto se traduce en una oportunidad valiosa. Significa que puede usar esta norma como hoja de ruta para moldear su Sistema de Gestión de Seguridad de la Información (SGSI), ajustándolo perfectamente a las particularidades, los desafíos y el contexto propio del sector público local.

La edición actual, la de 2020, es clara en este punto: proporciona directrices prácticas para añadir requisitos o controles adicionales cuando sea necesario, y también para refinar los

que ya están definidos en la ISO/IEC 27001. Así, el proceso no parte de cero, sino que se construye sobre un cimiento reconocido internacionalmente.

De esta manera, la Municipalidad no solo implementa un marco genérico, sino que logra algo mucho más poderoso: complementar la estructura general de la ISO 27001 con requisitos pensados específicamente para la administración pública. El resultado es un sistema de seguridad más pertinente, más eficaz y, en definitiva, más capaz de proteger lo que verdaderamente importa: la información y la confianza de la ciudadanía.

Alcance del SGSI y gestión de riesgos: Definir el alcance es, sin duda, uno de los pasos más importantes al implementar un SGSI. Piensa en esto como dibujar el mapa del territorio que vamos a proteger. Durante la fase de Planificación, es crucial establecer los límites claros del sistema: qué procesos, ubicaciones y, sobre todo, qué activos informáticos quedarán bajo su paraguas de protección.

En el día a día de una municipalidad, esto se vuelve muy concreto. Implica identificar aquellos departamentos y servicios que son el corazón de la gestión, como el área de recaudación, el padrón de contribuyentes o los trámites en línea, junto con los sistemas que manejan su información crítica. Todo ello debe quedar incluido en el alcance. Y claro, no basta con delimitar; también hay que asignar roles y responsabilidades nítidas al equipo de seguridad municipal. Que cada persona sepa qué le toca es la base para que todo funcione.

Otro pilar absolutamente fundamental es la gestión de riesgos. Aquí, la norma ISO 27001 y su familia de estándares nos piden algo metódico pero esencial: hacer un inventario completo de los activos de información y luego analizar a fondo los riesgos que los acechan—sus vulnerabilidades, las amenazas posibles y el impacto que tendría un incidente.

Así, en la fase de “Hacer” del SGSI, nos dedicamos precisamente a eso: a levantar ese inventario detallado y a efectuar un análisis de riesgos minucioso. El objetivo es entender con

claridad el nivel de exposición real de la Municipalidad. Solo con esa fotografía precisa podemos pasar a la acción.

A partir de ese diagnóstico, se desarrollan planes de tratamiento de riesgos. ¿Qué hacemos con cada uno? Podemos mitigarlo, transferirlo (con un seguro, por ejemplo) o, si es menor, aceptarlo de manera consciente. Estos planes son los que permiten aplicar controles específicos y proporcionales para cada activo crítico.

Este enfoque sistemático —primero identificar lo que tenemos, luego evaluar qué podría salir mal y finalmente aplicar los controles necesarios— no es solo un requisito de la norma. Es, sobre todo, la manera sensata de asegurar que los recursos de la entidad se administren con seguridad, y de que los posibles incidentes se puedan prevenir o, si ocurren, enfrentar de la manera más adecuada. Al final, se trata de cuidar lo que es valioso para la institución y para la comunidad.

Documentación, capacitación y resistencia al cambio

Efectivamente, la documentación formal del SGSI es indispensable. No es solo papeleo; es la memoria institucional del sistema de seguridad. La Municipalidad debe elaborar y mantener documentos vivos y útiles: desde la política de seguridad de la información (su declaración de principios) hasta los procedimientos operativos detallados, los registros de auditoría y los planes de contingencia para cuando las cosas no salgan como se espera. Como señala la guía de ISO 27001, la organización debe gestionar esta documentación como parte fundamental del soporte del SGSI.

¿Por qué es tan crucial? Bueno, esto asegura que cada decisión y cada control implementado tenga una trazabilidad clara. No solo da coherencia al proceso, sino que además facilita enormemente las auditorías, tanto internas como externas. Todo queda registrado, por lo que evaluar y mejorar el sistema se vuelve una tánica mucho más objetiva y ordenada.

Ahora, de nada sirve un sistema perfectamente documentado si las personas no están alineadas. Por eso, la capacitación y la concienciación del personal son la otra cara de la moneda. La ISO 27001 lo enfatiza con razón: los empleados deben estar formados y sensibilizados en temas de seguridad. En el ámbito municipal, esto se traduce en acciones concretas: realizar talleres prácticos y campañas informativas continuas. El objetivo es que todo el equipo, desde atención al público hasta la alta dirección, comprenda los riesgos y adopte buenas prácticas cotidianas, como el manejo seguro de credenciales, la protección de sus equipos o saber cómo actuar ante un posible incidente. El propio ciclo del SGSI contempla "asegurar la competencia y concienciación" como un paso activo y continuo.

Esto nos lleva a un punto delicado pero inevitable: gestionar la resistencia al cambio. Implementar un SGSI significa, en la práctica, modificar procesos y hábitos establecidos, y eso puede generar escepticismo. La clave aquí es un liderazgo visible. Se debe involucrar activamente a la alta dirección, que debe actuar como el principal promotor del cambio, comunicando de forma clara y constante los beneficios para todos: una mayor confianza ciudadana, el cumplimiento normativo y, sobre todo, la prevención de pérdidas de datos que afectan a la comunidad. Establecer canales de comunicación abiertos para escuchar las dudas y considerar los comentarios del personal no es un gesto de buena voluntad; es una parte estratégica de esta fase de soporte.

En conjunto, cuando la documentación ordenada, la formación continua y una gestión del cambio sensible se integran, dejan de ser requisitos aislados. Se convierten en los pilares para algo mucho más valioso y duradero: construir una auténtica cultura de seguridad en la Municipalidad de Chorrillos, donde proteger la información sea una responsabilidad compartida y entendida por todos.

Metodología PDCA del SGSI

Ciertamente, todo SGSI se sostiene sobre un motor fundamental: el ciclo de mejora continua PDCA (Planificar, Hacer, Verificar, Actuar). Este no es solo un modelo teórico; es la herramienta que permite al sistema respirar, aprender y adaptarse constantemente frente a nuevas amenazas. Para una municipalidad, aplicarlo es lo que transforma un proyecto en un proceso vivo.

Veamos cómo se traduce esto en la práctica del día a día en Chorrillos:

Planificar: Aquí es donde todo comienza con una visión clara. Como ya hemos visto, en esta fase se define el alcance del sistema, se establecen los objetivos de seguridad y se redacta la política que guiará todo el esfuerzo. Pero más allá de los documentos, se planifica cómo se alcanzarán esas metas. Por ejemplo, la Municipalidad determinará de manera concreta cómo garantizará la confidencialidad de los datos de los vecinos, estableciendo objetivos medibles y diseñando los procedimientos que los harán realidad.

Hacer: Llega el momento de poner manos a la obra. En esta fase se implementan todos los controles y procesos que se diseñaron. Es la ejecución tangible: se cifran las bases de datos sensibles, se aseguran las copias de respaldo, se despliegan firewalls en la red municipal y, crucialmente, se ponen en marcha los planes de tratamiento de riesgos. Es donde la teoría se convierte en acción protectora.

Verificar: Un sistema que no se mide, no se puede mejorar. Esta fase, la "C" del ciclo (del inglés Check), consiste en monitorear y evaluar rigurosamente el desempeño del SGSI. Para la Municipalidad de Chorrillos, esto significa realizar auditorías internas periódicas, ejecutar pruebas de penetración controladas o revisar indicadores clave, como el número y tipo de incidentes detectados. Es el momento de hacerse preguntas difíciles: ¿Estamos funcionando como esperábamos? ¿Los controles son efectivos?

Actuar: Esta es la fase que cierra el círculo y lo impulsa hacia adelante. Con base en los hallazgos de la verificación, se toman decisiones. Si se identifica una brecha—digamos, un procedimiento de acceso débil—, la Municipalidad actualiza ese procedimiento o implementa una nueva tecnología. No se trata de buscar culpables, sino de incorporar lecciones aprendidas. Aquí es donde se aplican las acciones correctivas y las mejoras, asegurando que el SGSI no se estanque.

La verdadera potencia del PDCA es que garantiza que el SGSI de Chorrillos nunca sea estático o un mero "proyecto de un año". Con cada iteración del ciclo, el gobierno municipal puede reasignar recursos de manera más inteligente, reforzar políticas donde haga falta y capacitar al personal en las áreas que realmente lo necesitan. Lo que se logra, en definitiva, es un enfoque de seguridad dinámico, resiliente y sostenible en el tiempo, que crece y se fortalece junto con la institución.

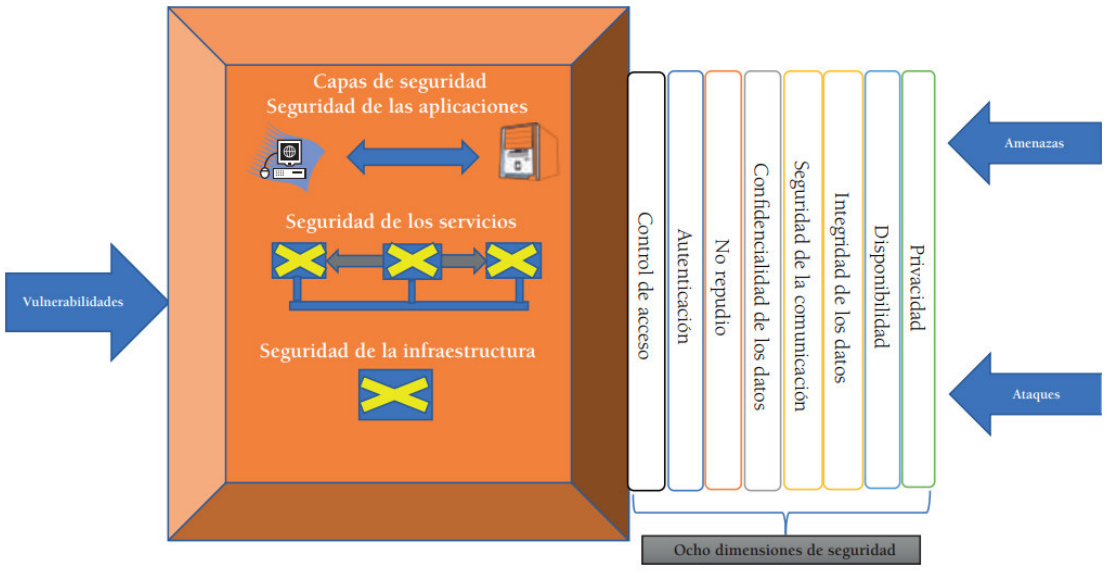
Modelo de clasificación de activos tecnológicos de la unión internacional de telecomunicaciones (ITU)

La Unión Internacional de Telecomunicaciones (ITU, por sus siglas en inglés) propone un modelo muy útil denominado arquitectura de seguridad para sistemas de comunicaciones de extremo a extremo. Este marco, que puedes ver representado en la imagen a continuación, se desarrolló siguiendo la Recomendación UIT-T X.805.

Lo valioso de este modelo es que define de forma clara y estructurada los elementos clave de seguridad que deben considerarse en una arquitectura. No se trata solo de proteger un punto aislado, sino de asegurar la protección a lo largo de toda la ruta que sigue la información, desde su origen hasta su destino final. En esencia, nos da una visión integral para garantizar que cada eslabón de la comunicación esté debidamente resguardado

Figura 3

Arquitectura de seguridad de la información



Nota. Elaboración propia.

Según lo que señala Valencia Duque (2021), las tecnologías de la información y las comunicaciones son, sin duda, claves para la productividad y competitividad de cualquier organización. Pero hay un lado delicado: también son vulnerables a diversas amenazas que, de materializarse, se convierten en riesgos reales.

Lamentablemente, estas amenazas pueden traer consecuencias serias, como pérdida de datos, interrupciones en los servicios o impactos financieros. Incluso, en casos más extremos, pueden afectar la reputación de una empresa o tener consecuencias mucho más graves, como poner en riesgo vidas humanas.

Por eso, el estudio destaca algo fundamental: implementar controles adecuados de seguridad de la información no es solo técnico, es una necesidad. Se trata de protegernos, de mitigar esos riesgos antes de que sea tarde.

Información y activos tecnológicos

La información es, en esencia, el cimiento para generar conocimiento. Y ese

conocimiento es precisamente lo que nos permite tomar decisiones acertadas en todos los niveles de una organización. Por eso, garantizar un adecuado nivel de seguridad de la información no es un tema secundario; es algo fundamental para que todo funcione bien, ya sea a nivel estratégico, táctico o en el día a día.

El proceso de gestionar esa información puede hacerse de manera manual, claro. Pero lo más común hoy es apoyarse en las Tecnologías de la Información y la Comunicación (TIC). Esta opción, que implica usar diversos activos tecnológicos, busca sobre todo eficiencia y efectividad en el manejo de los datos.

Ahora, aquí surge un desafío práctico: las organizaciones suelen tener una gran cantidad y variedad de estos activos tecnológicos. Identificarlos y clasificarlos puede volverse una tarea enorme, especialmente en las empresas más grandes. Imagina tener que organizar terabytes de datos electrónicos, archivos físicos interminables y miles de dispositivos y personas que forman parte del ecosistema tecnológico (ISACA, 2012). Por eso, se necesitan esquemas conceptuales que nos den una visión global y clara. Afortunadamente, existen varios modelos para abordar este reto, como los propuestos por Microsoft, la Unión Internacional de Telecomunicaciones, IBM, la norma ISO/IEC 27005, Magerit y la norma UNE 71504:2008.

Como bien señala la Dirección General de Modernización Administrativa (2012), las organizaciones enfrentan de forma constante diversas amenazas —ya sean naturales, tecnológicas o sociales— que pueden poner en riesgo sus objetivos. Cuando alguna de estas amenazas se materializa y nos impacta, entonces hablamos de "riesgo". Este término describe, justamente, la probabilidad de que ocurran eventos adversos y los efectos que podrían tener.

Para manejar esta realidad, las organizaciones han desarrollado el concepto de seguridad, entendido como un proceso continuo para mantener niveles de riesgo que sean aceptables. Ese nivel aceptable no es igual para todos; varía según cada organización. Y dado que es imposible eliminar todos los riesgos, la clave está en aprender a gestionarlos:

controlándolos, reduciéndolos o transformándolos. En ese sentido, es importante entender que la seguridad nunca puede ser absoluta.

En el ámbito específico de las TIC, la seguridad se refiere a la capacidad de estos sistemas para resistir, con un nivel de confianza adecuado, tanto accidentes como acciones malintencionadas. ¿El objetivo? Proteger la disponibilidad, autenticidad, integridad y confidencialidad de los datos que almacenan o transmiten, así como de los servicios que ofrecen (Dirección General de Modernización Administrativa, 2012).

Finalmente, la norma ISO/IEC 27000 define la seguridad de la información de manera muy clara: se trata de la protección de la confidencialidad, la integridad y la disponibilidad de la información. Tres pilares que, en conjunto, nos permiten resguardar lo que es verdaderamente valioso.

III. MÉTODO

3.1 Tipo de investigación

Esta investigación adopta un enfoque claramente tecnológico, ya que ofrece rasgos que la conectan de lleno con la innovación. Podría decirse, incluso, que se presenta como una herramienta fundamental para impulsar avances concretos en este ámbito.

Como bien señala Sampieri (2019), "la investigación tecnológica tiene como objetivo utilizar el conocimiento para transformar una realidad específica". ¿Y cómo funciona este enfoque? Se trata de un paradigma donde la investigación y la transformación avanzan de la mano. En otras palabras, primero necesitamos comprender a fondo aquello que estudiamos para, luego, poder intervenir de manera informada en una situación real. El proceso consiste justamente en modificar esa realidad paso a paso, acercándola progresivamente al resultado que buscamos

Diseño de investigación

Esta investigación-acción se basa en el método de la indagación introspectiva colectiva. ¿En qué consiste? Básicamente, la emprenden los propios participantes inmersos en una situación social, con un objetivo claro: mejorar tanto la racionalidad como la justicia de sus prácticas, ya sean sociales o educativas.

Como bien apunta O'Hanlon (2019), la investigación-acción parte de una idea importante: reconoce que tanto el investigador como los participantes tienen perspectivas y pensamientos distintos, los cuales inevitablemente influyen en el rumbo de la investigación. Esto es clave.

De hecho, la validez y autenticidad de este tipo de trabajo dependen, en gran medida, de que todos los involucrados sean conscientes de sus propios intereses y valores personales. ¿Por qué? Porque son precisamente estos factores los que van dando forma, paso a paso, al compromiso asumido en el proceso.

Escenario de estudio

Podemos entender la seguridad como un proceso continuo, algo vivo que requiere supervisión constante y un manejo cuidadoso. La norma ISO 27009 nos ofrece, justamente, una metodología diseñada para proteger tres pilares clave de la información: su confidencialidad, integridad y disponibilidad.

En este contexto, el área de Seguridad de la Municipalidad Distrital de Chorrillos tiene un objetivo claro y vital: aplicar esta metodología para definir su estrategia de seguridad de la información. La meta es resguardar de manera efectiva todos los datos e información institucional, y para ello se apoyará en el conocido modelo de mejora continua PHVA (Planificar, Hacer, Verificar y Actuar).

¿Cómo funciona este camino? Todo comienza con la descripción del Sistema de Gestión de la Seguridad de la Información (SGSI). En esta primera etapa, que corresponde a Planificar, se analizan y definen a fondo los escenarios y la planificación necesaria.

Luego, el modelo avanza hacia la puesta en marcha. Esta fase de Hacer abarca desde la implementación hasta la ejecución real de los controles y aplicaciones que se hayan definido.

Una vez que el SGSI está en funcionamiento, llega el momento de Verificar. Aquí se monitorea y revisa de cerca su desempeño. Finalmente, con esos aprendizajes, se pasa a Actuar, identificando e implementando las mejoras necesarias para que el sistema siga evolucionando y fortaleciéndose.

Participantes

Para llevar a cabo esta pesquisa, se eligió como sujetos a siete líderes del sector de amparo digital dentro de la Comuna Local de Chorrillos. Este conjunto de sujetos fue apartado puntualmente porque sus empleados manejan saberes en varios trucos y modos para manejar

los datos del centro, asegurando de ese modo su intimidad por medio del plan de defensa organizado.

Tal como indican Baptista et al. (2017), una colectividad se establece como ese conjunto de seres vivos que comparten un rasgo igual y que es materia de averiguación. Dicho de otro modo, estos expertos forman, en esta circunstancia, el bloque apropiado para inspeccionar las ocurrencias atadas al manejo del resguardo digital en el organismo.

3.2 Población y muestra

La estructura de este estudio se clasifica como observacional-vinculante. ¿Qué quiere decir esto realmente? Fundamentalmente, que persigue dos metas distintas: primero, intenta pintar un cuadro minucioso de cómo están hoy las cosas en cuanto a proteger datos dentro del Ayuntamiento de Chorrillos; y luego, examinar si hay algún lazo entre usar el estándar ISO/IEC 27009 y ver mejoras reales en el cuidado de la información que maneja la entidad. Tal como indican Hernández et al. (2014), en este modelo el que investiga no mueve las piezas, sino que simplemente mira y anota las cosas tal cual aparecen en su ambiente natural. Es similar a capturar una imagen de lo que sucede para entenderlo mejor.

Por un lado, la parte observacional nos dejará conseguir un panorama nítido y en detalle de todos los elementos que tocan la custodia digital local, y de cómo el ISO/IEC 27009 podría hacer más firmes las rutinas ya establecidas. Por el otro lado, la pieza vinculante busca algo importante: fijar si en verdad existe un nexo notorio entre poner en marcha esa pauta y los frutos conseguidos. Dicho de otra forma, deseamos averiguar si ponerla en práctica resulta en un amparo superior para los datos y una disminución palpable de los peligros. Universo y subconjunto.

Población

Según lo explica Gómez (2013), el grupo se interpreta como "la suma completa de piezas de examen del bloque a revisar, o sea, el cúmulo de personas, cacharros, trozos o sucesos donde cabe aparecer un rasgo apto para ser mirado" (p. 80).

Dentro del marco de esta indagación, enfocamos nuestra atención en algo de estudio bastante específico: las pifias ligadas a estar a salvo con la información dentro del Municipio de Chorrillos. Esto abarca, por poner un ejemplo, fallos al tratar con papeles del ente, escapes de datos privados y demás peligros que surgen de puntos débiles en la máquina.

Por este motivo, la gente para esta averiguación estará hecha del conjunto completo de percances anotados en el Sistema de Manejo de Resguardo de Datos (SGSI) durante un ciclo mensual. La mirada se llevará a cabo tomando en cuenta las notas de los días de lunes hasta el sábado, permitiéndonos notar con más agudeza el modo de actuar y cuán a menudo pasan estos sucesos en la semana laboral.

Muestra

Según Ortega et al. (2012), "cualquier pedacito del todo, mirando desde los números, puede tener azar o no tenerlo" (p. 52). Además, Hernández (2011) indica que "si el grupo grande es menos de cincuenta (50) piececitas, el grupo grande es igual al pedacito" (p. 69).

Puesto que la gente a la que se preguntará es poca y se puede manejar, el conteo de ese pedacito se hará pensando en la gente que aparezca en el tiempo ya fijado. Para el estudio, se elegirá como pedacito el número de gente entrevistada de la Comuna de Chorrillos, a ellas se les verá qué tan bien resuelven y cómo siguen las cosas. En esta situación, se usarán dos maneras de medir principales: si se puede acceder al dato electrónico y si ese dato electrónico se mantiene en secreto, esto dejará ver qué tan bien funciona el sistema para cuidar la información puesto en marcha.

El pedacito se verá al usar la cuenta matemática que se debe, porque el grupo grande es chiquito en verdad. Esta cuenta dejará que los datos para mirar se vean de forma correcta.

$$n = \frac{Z^2.N.p.q}{i^2(N-1) + Z^2.p.q}$$

Dónde:

n: Tamaño de la muestra

N (población): Tamaño de la población 7 entrevistas

Z= Valor de distribución (1.96)

p= Prevalencia esperada (p=0.05)

3.3 Operacionalización de variables

Tabla 1

Matriz de operacionalización cualitativa

TIPO	VARIABLE	DEFINICIÓN OPERACIONAL	DIMENSIÓN	INDICADORES	DESCRIPCIÓN
Variable Independiente	Aplicación de la norma ISO/IEC 27009	La aplicación de la norma ISO/IEC 27009 se refiere al proceso de implementación de los controles y directrices establecidos en la norma ISO/IEC 27009 en la organización, para establecer un sistema de gestión de seguridad de la información. Esto incluye la identificación y evaluación de riesgos, así como la creación de políticas y procedimientos que aseguren la confidencialidad, integridad y disponibilidad de los datos manejados en la Municipalidad de Chorrillos.			
Variable Dependiente	Prevención de riesgos del sistema de información	Los riesgos del sistema de información se refieren a las amenazas potenciales que podrían comprometer la confidencialidad, integridad y disponibilidad de la información procesada por los sistemas informáticos de la Municipalidad de Chorrillos. Esto incluye el análisis de vulnerabilidades, la probabilidad de ocurrencia de amenazas y sus impactos en los activos informáticos, con el fin de desarrollar estrategias de mitigación.	Porcentaje de interrupciones del sistema:	Disponibilidad del Sistema de Información	Cuando un usuario está convencido de que el nivel de prioridad de un incidente debe superar directrices normales
			Porcentaje de accesos no autorizados detectados:	Confidencialidad del Sistema de Información	Se mide cuando una incidencia es escalada al grupo de trabajo incorrecto

Nota. Aunque la estructura de la guía institucional emplea el título “Operacionalización de variables”, en la presente investigación se precisa que, por su enfoque cualitativo, se trabaja con categorías de análisis y no con variables estadísticas.

DIMENSIÓN	INDICADOR	DESCRIPCIÓN	TÉCNICA	INSTRUMENTO	UNIDAD DE MEDIDA	FÓRMULA
Porcentaje de interrupciones del sistema:	Disponibilidad del Sistema de Información	Cuando un usuario está convencido de que el nivel de prioridad de un incidente debe superar directrices normales	Instrumento de Recolección de Datos	Entrevista	Unidad	$DISP = \frac{NIR}{NTI}$
Porcentaje de accesos no autorizados detectados:	Confidencialidad del Sistema de Información	Se mide cuando una incidencia es escalada al grupo de trabajo incorrecto	Instrumento de Recolección de Datos	Entrevista	Unidad	$CONFIA = \frac{RA}{RR}$

Fuente: Elaboración Propia

3.4 Instrumentos

Para juntar los datos que hacen falta, usaremos formas de estudio numéricas, como cuestionarios y charlas arregladas. Estas se pondrán en marcha en dos grupos importantes: primero, en los trabajadores del Municipio de Chorrillos que se encargan del cuidado de los datos; y luego, en quienes usan las ayudas del municipio por medios electrónicos. Con estos aparatos intentaremos, en verdad, dos maneras de ver que se juntan bien. De un lado, lograr una imagen clara y total de cómo anda la guarda de los sistemas ahora. Del otro, saber directamente las ideas y lo que sienten tanto los de dentro como los de fuera, sobre todo al hablar de cuidar la información y qué tan bien funcionan las cosas que ya se pusieron. Así, podremos mezclar lo de las máquinas con lo de las personas, lo que se pensó con lo que pasó

3.4.1 Encuestas

Los sondeos se moldearán a partir de un listado de preguntas fijo que contendrá interrogantes de respuesta limitada y extensa, lo cual dejará conseguir cifras medibles y entendimientos sobre los puntos principales del resguardo de datos. Las dudas tendrán como fin saber las ideas de la gente acerca de qué tan seguro se ven los aparatos, los tropiezos que hallan al manejar la custodia, y qué tan bien funcionan las reglas puestas, sobre todo tocante al estándar ISO/IEC 27009.

3.4.2 Entrevistas

Las charlas formales se llevarán a cabo con los guardianes del secreto digital en el ayuntamiento, y también con sabios en manejar la protección de datos dentro del ámbito gubernamental. Dichas conversaciones ayudarán a meterse más a fondo en cómo funciona la protección ahora, señalar qué anda bien y qué no en aplicar la regla ISO/IEC 27009, y recoger puntos de vista entendidos sobre maneras excelentes de hacer más fuerte el resguardo de la información en el gobierno local

Tabla 2

Matriz de Instrumentos

VARIABLE	INDICADOR	TÉCNICA	INSTRUMENTO	FUENTE
Planificación y Control del Proceso de Cotización	disponibilidad del sistema de información	Entrevista	Guía de Entrevista	Guía de Entrevista y Ficha de Observación elaborados por el investigador de acuerdo a las características y al objetivo.
		Observación	Ficha de Observación	
	confidencialidad del sistema de información	Entrevista	Guía de Entrevista	Guía de Entrevista y Ficha de Observación elaborados por el investigador de acuerdo a las características y al objetivo.
		Observación	Ficha de Observación	

Nota. Aunque la estructura de la guía institucional emplea el título "Operacionalización de variables", en la presente investigación se precisa que, por su enfoque cualitativo, se trabaja con categorías de análisis y no con variables estadísticas.

3.5 Procedimientos

El procedimiento de recolección de datos se llevará a cabo en varias fases:

Fase 1: Diseño y validación de instrumentos: En esta etapa se dibujarán los papeles de preguntas de los sondeos y las hojitas para las charlas, tomando como base las metas del estudio. Los artilugios pasarán una prueba de expertos en resguardo de datos para asegurar que son apropiados y concuerdan bien.

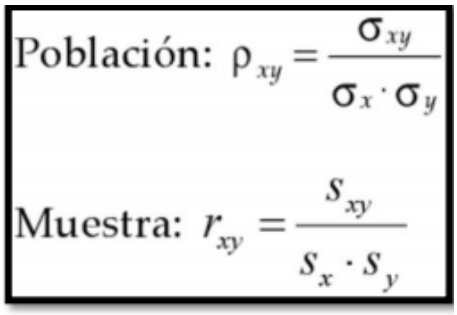
Fase 2: Aplicación de encuestas y entrevistas: Tras confirmar que los aparejos sirven, se seguirá adelante con entregar las formas al grupo de la alcaldía y a quienes usan lo que ofrece el gobierno, además de charlar de manera fija con los encargados del cuidado de datos.

Fase 3: Procesamiento de los datos: Los números que juntamos se pondrán en orden y se moverán con unos aparatos de cuenta para mirar lo que sale. Sobre las historias que nos cuenten, se les dará un código y se buscarán sus ideas principales al examinarlas.

Método de Test – Retest

Este proceso se aplica a diversos grupos de personas después de realizar la medición inicial. Si los resultados obtenidos son consistentes, se considera que el instrumento es fiable. Sin embargo, si el intervalo de tiempo entre las pruebas es largo, esto podría generar confusión al interpretar la fiabilidad del proceso. Por otro lado, si el periodo es breve, los participantes pueden recordar sus respuestas de la primera aplicación, lo que podría influir en los resultados de la segunda medición.

Coeficiente de correlación de Pearson



Donde:

Pxy= Coeficiente de correlación de Pearson de la población

Rxy= Coeficiente de correlación de Pearson Muestra

0xy= Sxy= covarianza de x e y

0x= Sx= Desviación típica de la variable x

0= Sy= Desviación típica de la variable y

La confiabilidad en mención menciona tres niveles de resultado adecuados al valor predeterminado del p-valor de contraste (sig.)

según las siguientes condiciones

Escala	Nivel
0.00 < sig. <0.20	Muy bajo
0.20 ≤ sig. < 0.40	Bajo
0.40 ≤ sig. < 0.60	Regular
0.60 ≤ sig. < 0.80	Aceptable
0.80 ≤ sig. < 1.00	Elevado

Fuente: Cayetano

Si sig. Está junto a 1, se puede decir que el instrumento es fiable.

Si sig. Está por debajo a 0.6, el instrumento presenta una varianza heterogénea en sus ítems.

3.6 Análisis de datos

La investigación respetó los principios de consentimiento informado, confidencialidad, privacidad de los participantes y uso académico de la información. La participación fue voluntaria y la información recolectada fue utilizada únicamente con fines académicos.

No se divulgaron nombres, cargos específicos ni datos sensibles que pudieran comprometer la seguridad institucional o la identidad de los participantes. Asimismo, se respetó la integridad de las respuestas obtenidas, evitando alterar su sentido durante el proceso de análisis.

Los resultados fueron presentados de manera agregada, priorizando la interpretación académica y la protección de la información municipal. Además, se mantuvo reserva sobre aspectos técnicos o administrativos que pudieran afectar la seguridad de los sistemas de información de la Municipalidad Distrital de Chorrillos.

3.7 Consideraciones éticas

Se garantizará que todo el proceso de recolección de datos respete los principios éticos de la investigación, como el consentimiento informado, la confidencialidad de los datos y el respeto por la privacidad de los participantes. Además, se asegurará que los resultados de la investigación sean utilizados únicamente con fines académicos y que no se identifiquen individualmente a los participantes en la difusión de los resultados.

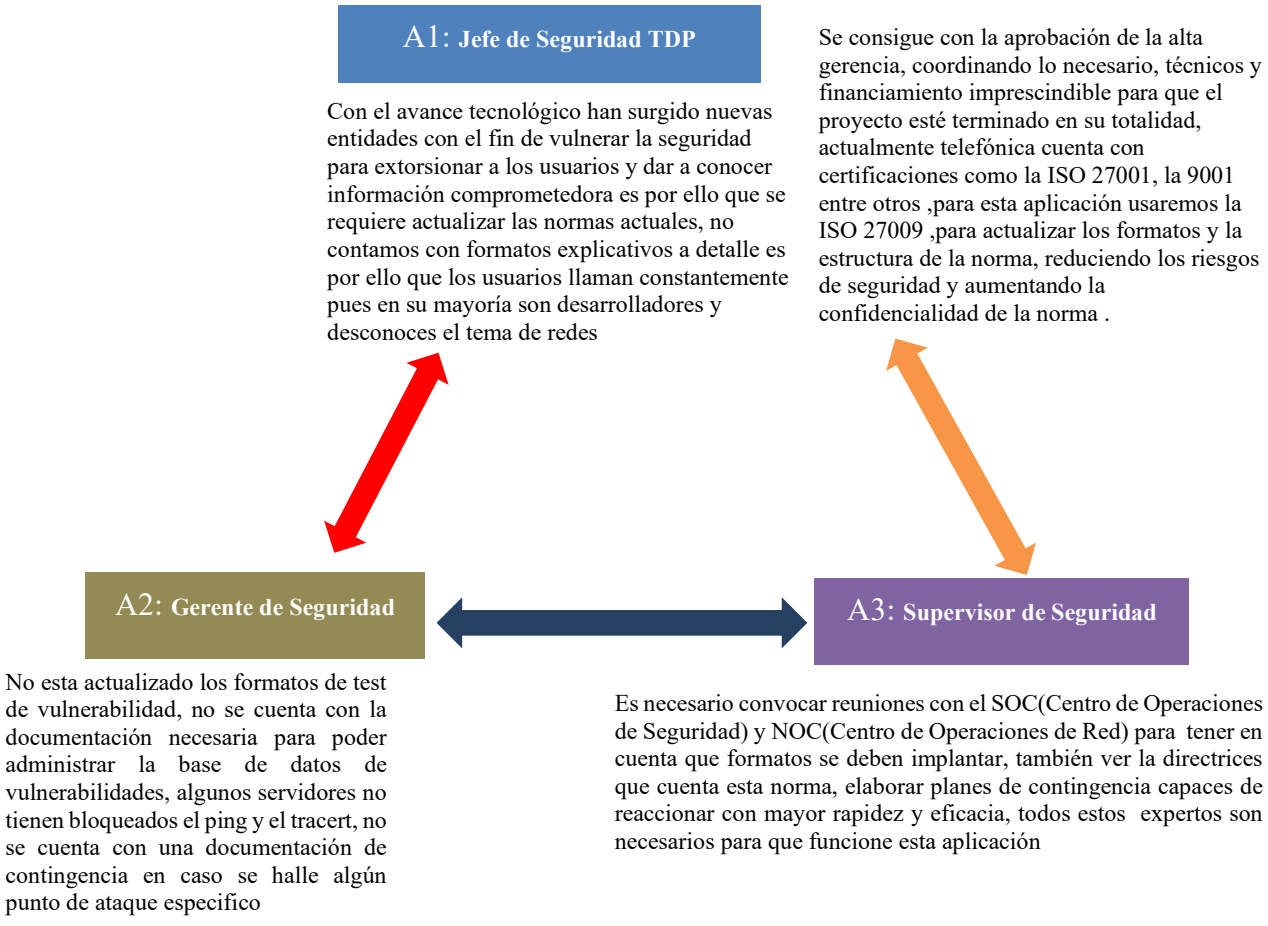
IV. RESULTADOS

Para describir los resultados, esta investigación ha empleado distintas técnicas de recolección de datos: la entrevista en profundidad con preguntas semiestructuradas, el análisis documental y la observación participante. La combinación de estos enfoques nos ha permitido alcanzar los objetivos planteados y, a la vez, estructurar y contrastar las respuestas proporcionadas por los expertos consultados.

A continuación, a través de la triangulación de estos datos, se ilustra el camino que nos ha llevado hasta la conclusión final. Se trata, en esencia, de contrastar las diferentes perspectivas obtenidas —lo dicho en las entrevistas, lo documentado y lo observado— para construir una visión más completa, sólida y fundamentada.

Figura 4

Triangulación de la observación de la unidad de estudio.



De acuerdo con lo presentado se puede concluir que la aplicación de una norma ISO 27009 se tienen que tener el apoyo de las partes involucradas tanto de la alta gerencia, hasta los técnicos encargados, identificando los posibles riesgos de seguridad y los procesos de información de la seguridad.

Los entrevistados, tanto el Jefe como el Gerente, cuentan con una amplia trayectoria de más de 10 años en distintas organizaciones.

En el caso del Gerente de Seguridad, actual responsable del equipo de seguridad de la información, es ampliamente reconocido por sus sólidos conocimientos técnicos y su especialización en Cloud Computing y Ethical Hacking. Su perspectiva es clara: para aplicar la norma, es fundamental contar con una planificación correcta y con suficiente antelación. Esto incluye, según señaló, *"tanto el plan, la documentación como la implementación del sistema de calidad"*.

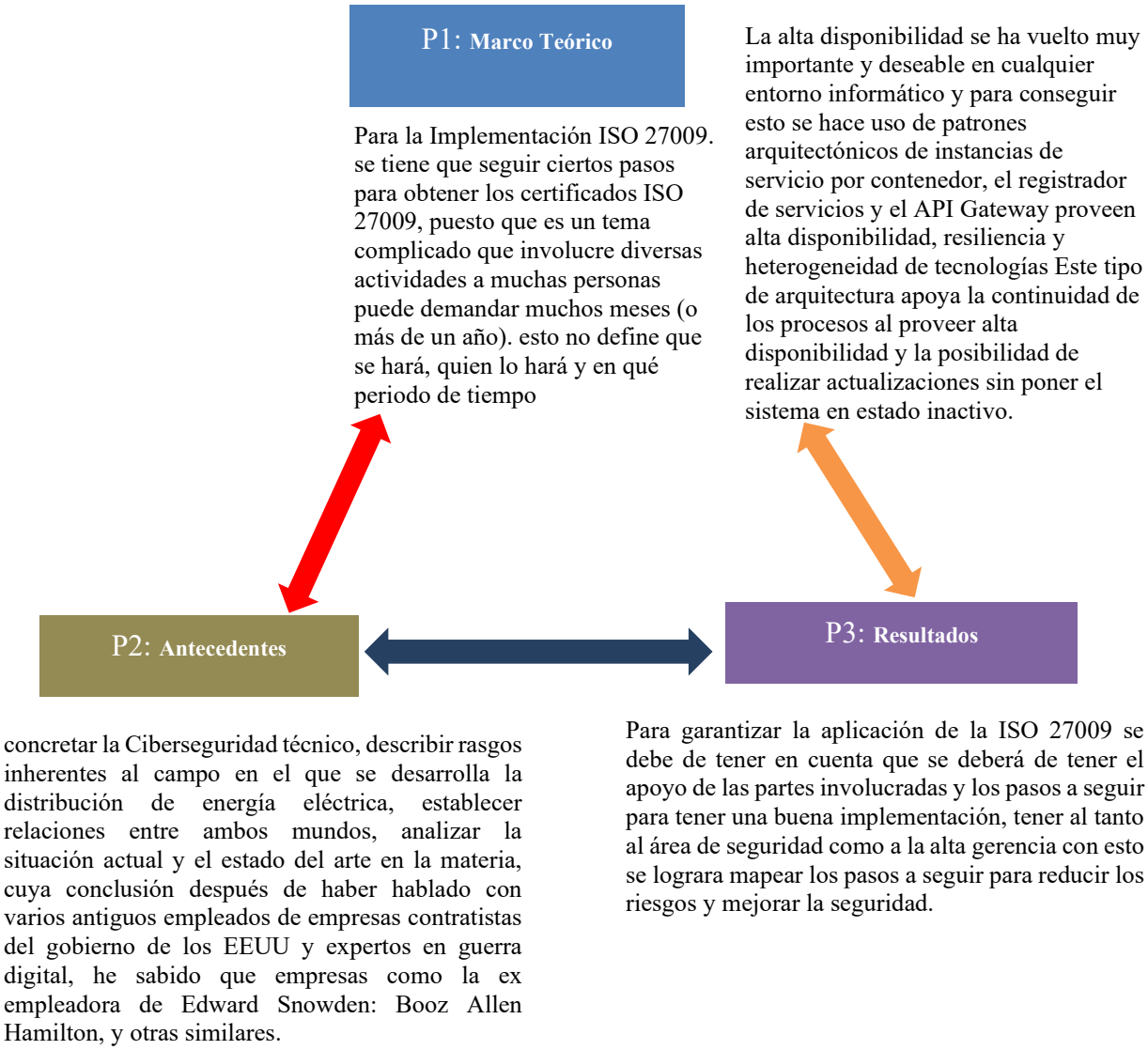
Por su parte, el Jefe de Seguridad enfatizó la importancia de conocer el punto de partida. Nos manifestó que, para aplicar la norma ISO, *"es imprescindible elaborar un diagnóstico de la situación actual de la empresa"*. Esta información inicial es clave, ya que permite analizar la viabilidad de cumplir con los requisitos necesarios para la certificación. Una vez evaluado el estado inicial, la empresa debe plantear un plan de implementación documentado que, en sus palabras, *"exhorta identificar y describir los procesos imprescindibles para que el sistema logre cumplir con todos los requisitos que el estándar ISO solicite"*.

Finalmente, el Supervisor, profesional especializado en ethical hacking y responsable del área de seguridad de la información en Telefónica del Perú, aportó una visión orientada a

la gestión dinámica del riesgo. Nos compartió que el entorno actual es cambiante y los riesgos de seguridad pueden presentar alteraciones repentinas. *"Las amenazas son constantes —señaló—, se detectan vulnerabilidades continuamente y los incidentes de seguridad pueden ocurrir con repercusiones de suma importancia"*. Su observación subraya la necesidad de adaptación y vigilancia continua dentro de cualquier estrategia de seguridad.

Figura 5

Triangulación de antecedentes, marco teórico y los resultados.

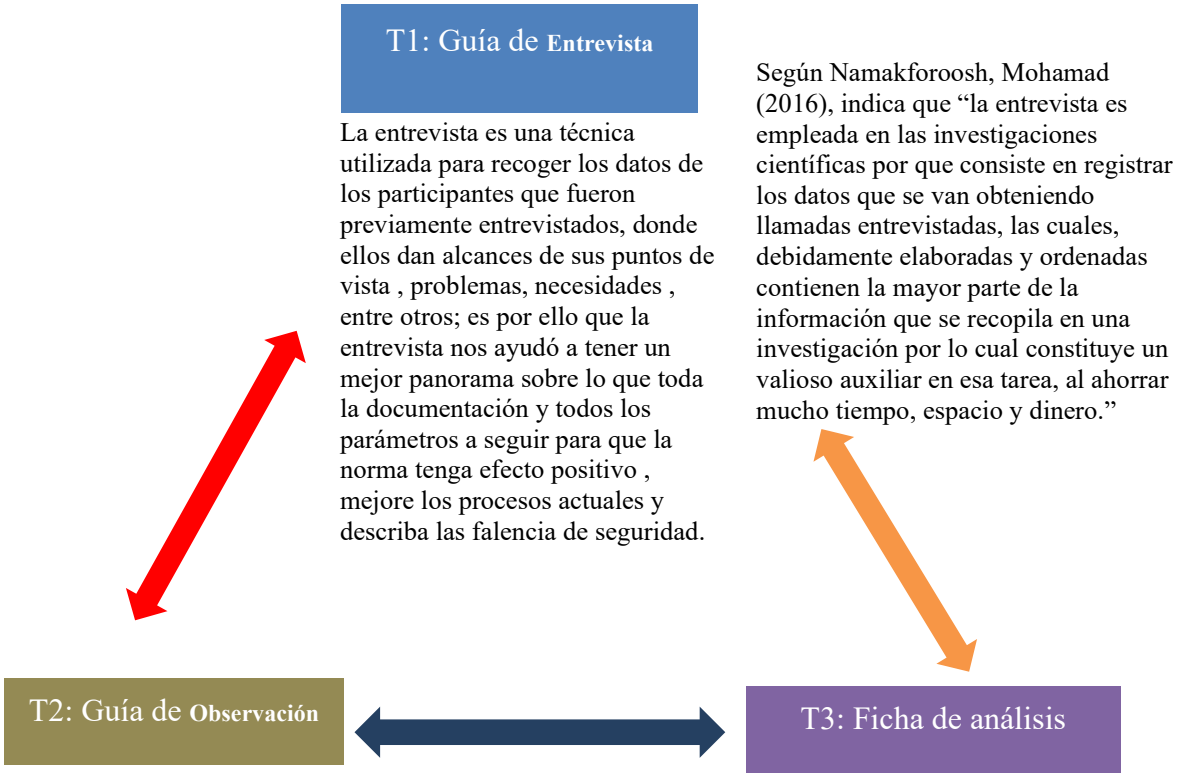


De acuerdo con lo expuesto se puede concluir que se deben de seguir los pasos necesarios para la aplicación de la ISO 27009 para la mejora de la seguridad de la información

es necesario tener en cuenta que se reducirán los riesgos informáticos y se mejorar la seguridad de la información, se obtendrá documentación más robusta y con mejor detalle de las vulnerabilidades, esto se reflejará con la reducción de la interrupción de los usuarios que de acuerdo con los expuesto se puede concluir lo necesario que resulta una implementación de la norma ISO 27009 que controle la seguridad. Es importante indicar que la aplicación ISO 27009 disminuirá estos posibles problemas de seguridad y agilizará sus procesos.

Figura 6

Triangulación de las técnicas de investigación utilizadas.



P1, ¿Cómo aplicar la norma ISO 27009 para prevenir riesgos del sistema de información en una empresa de telecomunicaciones?

E1: que la cúpula se una con firmeza, el estándar pide como condición, la causa se debe a los humanos, recursos monetarios y el equipo preciso para acabar la obra. dicho entorno trae consigo bastantes peligros de resguardo, mostrando una mudanza donde los embates son abundantes, las faltas de cuidado son halladas y los tropiezos ocurren con efectos. el libreto debe sumar el reparto de deberes, el calendario de labores y los plazos finales para lograr las metas (Vigilancia y manejo).

E2: Para que la norma ISO tome forma es necesario mirar el reloj, el mapa y el orden del plan, significando un trabajo pesado, por lo que afecta bastante el uso de las ayudas, acelerando la marcha y grados de contento, de los trabajadores, para el examen, del resguardo de los datos hay que considerar que toca revisar las maneras y los peligros juntados a las maneras del negocio en sí y el alrededor.

E3: El aire inquieto que traen las sombras de cuidado nos regalan vueltas sin fin, con peligros siempre ahí, huecos hallados a cada rato, y sucesos de guardia llegando con efectos grandes, sea para mirar el sitio en el que está.

P2. ¿Cómo elaborar el diagnostico de una empresa de telecomunicaciones para aplicar la norma ISO 27009?

E1: Para lograr una buena determinación, existen ciertas acciones que es bueno considerar, antes que nada toca señalar la firmeza de los datos presentes como los cuidados al secreto electrónico que se usen para evitar que entren sin permiso a los archivos, después de eso se revisan los modos de esos papeles.

E2: La medida de lo seguro en datos sugiere un mirar de conjunto y con metas claras, puesto en marcha sobre las bases firmes de prueba, estudio, juntar y de fiscalización, el modo de medir lo seguro se puede contar así, la medida con el fijar las metas

E3: Cabe señalar que la averiguación y la sugerencia: el vistazo inicial a las máquinas de datos, hecho a través de la red mundial y las saberes traídas por el grupo de labor servirá para juntar detalles acerca de la estructura de los aparatos de paso como cortafuegos.

P3. ¿Cómo implementar la norma ISO 27009 en una empresa de telecomunicaciones?

E1: Para poner en marcha la regla es bueno mirar las partes flojas antes de armar un plan para arreglar los tanteos de entrada que traen consigo correr el esquema de pasos hechos a mano o con máquinas que hacen parar a las máquinas.

E2: La estructuración acerca de las alturas de plenitud pedidas, sopesar los peligros, mirar las salvaguardas y poder fijar un diseño de azar, para arrancar la faena en los pasos esenciales para el grupo por lo tanto el llevar a cabo el diseño para poner la regla, el conjunto responsable debe tener en mente las pautas de tanteo y metas vistas (Organización de los pasos), igualmente hará falta un puñado de consejos para poder meter un diseño de perfeccionamiento.

E3: Si el negocio desea poner en marcha la regla ISO, puede ser mucha información saber dónde iniciar por esta razón, se necesita contar con un buen motivo para hacer ver a los jefes que aplican la regla ISO, según la hoja de ruta de peligros.

P4. ¿Qué riesgos existe al implementar la norma ISO 27009 en una empresa de

telecomunicaciones?

E1: Las empresas juntan una pila de peligros parecidos y guardan otros propios de su estructura. Hay ciertas pautas o inventarios que nos pueden echar una mano para comprobar si esos riesgos comunes que tienen casi todas las agrupaciones

E2: Para mirar los peligros toca escudriñar las paradas y poder fijar un mapa de peligro, para arrancar a mover el mapa del ente, después para el diseño de faenas se estudia el mirar profundo bueno de resguardo de datos es por esa causa que se aconseja la inspección activa

E3: Las compañías, buscando esquivar el surgimiento de peligros no vistos que podrían tocar cualquier percance de amparo, tienen que armar un mapa de peligros, sobre todo porque toca los datos y las estructuras, las respuestas para los problemas de protección son bastante más que poner aparatos como cortafuegos y accesos, y los programas contra virus.

P5. ¿Qué documentos y formatos se usan para implementar la norma ISO 27009?

E1: La pauta para la forma pide nombrar y contar los pasos requeridos para que el aparato cumpla todas las normas ISO, esto debe llevar quién hace qué, un mapa de faenas y fechas tope para terminar.

E2: El papeleo de lo que se logra da luz al asunto, un mapa para el hacer, un punto de partida para mirar el progreso y un cuaderno de lo ya hecho para luego mirar, si bien hay que saltarse el apuntar lo que estorbe.

E3: La guía del estándar señala los ingresos que se requieren y los resultados que salen de cada una de las labores de la empresa fijando el orden y cómo se tocan todas las tareas. Su forma debe seguir la regla del estándar y también tendrá una plantilla fija para apuntar la

información útil y debe escribirse antes de que se haga el mirar y arreglar de los peligros y el papel con lo visto y ahí se juntan todas las cosas halladas.

P6. ¿Cuáles son las estrategias del seguimiento y control?

E1: El modo de Vigilar y Gobernar la Tarea fija el grupo de pasos que se harán para asegurar la buena marcha de las faenas del encargo, por lo cual es clave entender la destreza del aparato y saber las probables fallas que podrían brotar.

E2: Tener un aparato de mirar y mandar que esté activo, que garantice un buen nivel en lo que se hace, con papeles puestos para chequearlo, por eso necesita revisiones a las formas, para mirar su firmeza y que encaje con el resto de papeles y a las guías de faena con el fin de mirar que sirvan bien

E3: Los planes se arman para que cada lado muestre algo para hacer crecer el programa de datos empleando una estructura clara junto al cronograma de revisión, hace falta saber qué tan importantes son los pasos y los sectores a revisar, y también hay que mirar las notas sacadas de las inspecciones pasadas, es igual de importante fijar las reglas usadas al momento de la fiscalización.

V. DISCUSIÓN DE RESULTADOS

Al cotejar los números que salieron con los papeles que revisamos —que son tesis, revistas y cosas de antes—, se pudo alcanzar la meta central de este estudio: poner en marcha la regla ISO/IEC 27009.

Recopilando lo que dijeron los tres sabios que charlamos, para usar esa regla y cuidar los peligros en el aparato de datos de una compañía de llamadas, hay que tener en cuenta estos puntos clave:

La gente de arriba debe quererlo y mostrarlo

Poner esto en práctica necesita que los jefes de verdad se esfuercen y se dejen ver. Ese empujón es algo que no puede faltar, pues todo el asunto se apoya mucho en que se den suficientes personas, máquinas y plata para terminar bien.

Ver cómo están las cosas y armar un plan ordenado

Es vital empezar mirando con lupa cómo anda la seguridad de la compañía justo ahora. Esa revisión debe sopesar los modos de trabajar, los peligros que hay y dónde operan. Con eso en mano, hay que crear un papel con el plan de montaje que contenga:

* Decir bien quién hace cada cosa.
* Un calendario fijo de tareas.
* Tiempos tope para lograr las metas.
* Formas de vigilar y chequear.

Esa fase de pensar y arreglar es un trabajo grande que pega directo en cómo se usa la plata y en lo que hacen los que trabajan allí.

Ponerle ojo a lo que siempre se mueve y cambia

El tema de la seguridad en las comunicaciones cambia sin parar y tiene peligros que aparecen siempre, fallas que se encuentran a cada rato y problemas que pueden ser serios. Por eso, la regla no se usa una sola vez; pide una vuelta de mejorar siempre.

Escribir todo, revisar y seguir vigilando

Un punto central es anotar cada paso y crear el papel que pide la regla. Luego, toca hacer miradas de vez en cuando y poner frenos para bajar las debilidades. Mirar que todo siga las reglas y ajustarse a lo nuevo son trozos fijos del hacer.

Forma de ver bien las cosas

Para hacer una mirada fuerte se sugiere lo siguiente:

* Notar cómo están ahora el cuidado y el resguardo de lo digital.
* Calcular los frenos puestos contra lo que dice la ley y si sirven de verdad.
* Ver las máquinas y programas (lo físico y lo lógico), tocando el cielo con la nube y las barreras de entrada como muros de fuego.
* Estudiar qué sabe hacer el grupo de gente a cargo.
* Hacer un primer vistazo a los sistemas de datos, usando lo que el propio equipo ya sabe bien.

Al final, esta mirada a la información segura —que mira el todo y busca metas claras—, junto con el plan de un modo seguro para hablar, sirvieron como bases muy importantes para armar esta investigación.

VI. CONCLUSIONES

Tomando como base los cachivaches empleados en esta tarea, arribamos a un primer dictamen sin dobleces: la escritura de cosas es de suma importancia. Aquello que se anota pone en vista el asunto del encargo, funciona cual mapa para la faena y crea un punto de partida para mirar el progreso. Aparte, deja un rastro de oro para cuando se requiera mirar atrás. Eso sí, es sabio no escribir hasta el hartazgo; hay que enfocarse en lo que de veras importa.

La forma de los moldes puede empezar pronto y marchar junto a los tiempos de armar el plan y ver la pulcritud. Todas estas piezas se hacen iguales con su papel oficial para que luego sea más sencillo meterlas en práctica. Los toques finales al escrito y arreglar cualquier tropiezo se juntan, como si fuera cosa de magia, con el chequeo del escudo protector del sistema. En este trajín, es vital lograr que las maneras de contar se abran a que quienes están metidos puedan meter su cuchara al mirar, cambiarle el traje y apuntar sus propios deberes.

Por otro lado, para acertar con el examen debemos seguir un puñado de senderos. De inicio, toca señalar cómo anda el cuidado de lo secreto digital, poniendo ojo en las cercas que se ponen para que nadie indeseado entre. Después, se sopesan los modos de pasar datos que se necesitan para que la máquina cumpla todo lo que pide la regla del ISO.

Este cuadro de visión ha empujado una alta petición de maneras de arreglar y entendidos listos para hacer ligas más firmes y menos dóciles. Aquí es vital sacar una creencia falsa: el pensamiento que las estructuras locales son de forma natural más a salvo que aquellas estructuras que viven en el cielo. Siendo cierto, el meterse a la fuerza sin permiso a los cuartos de máquinas del cielo es algo que pasa muy poco. Las fallas de seguridad más pesadas por lo general suceden tras las barreras de fuego de las compañías, muchas veces atadas a lo que hacen sus propios trabajadores. Los datos en el cielo, al estar puestos por partes en muchos aparatos y sitios, en vez de en solo un aparato cercano, pueden dar puntos buenos de aguante. Pagar atención a las reglas y textos de cuidado es forzoso, y los grupos tienen que vigilar

cualquier movida rara o entrada sin permiso, poniendo medidas de cuidado, avisos y notificaciones para cuidar aquella información que ven más querida y privada, como fichas de quienes usan, claves secretas o números del dinero.

El tercer punto final trata sobre el poner en práctica. Para usar la regla bien, debemos mirar y tomar en cuenta los puntos flojos antes de armar un mapa de lo que haremos. Los exámenes de meterse a la fuerza, que meten métodos hechos a mano o por máquinas para revisar aparatos, programas, redes y cosas, son importantes para ver por dónde se podrían abrir huecos. El orden de estos pasos sigue un camino claro de fases, hecho solo para el cuidado de la data. Por último, un Mapa de Ponerse Mejor sin parar nos deja crear ideas de qué hacer si algo malo pasa para tratar los peligros que salen en el trabajo y arreglarlos en el momento.

Finalmente, la manera de Vigilar y Gobernar arregla la pila de pasos para mirar que el trabajo se haga bien. Es necesario saber qué tan bueno anda el sistema y pensar en sus tropiezos probables. La forma ideal de hacer esto es con revisiones de casa. Se necesita que los jefes de arriba miren todo el quehacer y confirmen que se hicieron las cosas que se dijeron para arreglar en esas revisiones. Luego de ver lo que se encontró, hay que poner cosas para que no pasen problemas luego y tapar los huecos a los que quieren entrar, así se termina la vuelta de hacerse mejor.

VII. RECOMENDACIONES

Primera recomendación

Para aplicar la norma con éxito, el punto de partida siempre debe ser un diagnóstico claro de la seguridad actual. Esto nos permite entender qué protocolos ya están en marcha y cuáles necesitan ajustarse. Luego, durante la implementación, es fundamental tener un inventario completo y actualizado de los activos, tanto lógicos como físicos.

También es clave documentar todos los procesos; esto no es solo un trámite, sino la evidencia que nos muestra qué está funcionando, qué podemos mejorar y qué quizás debemos replantear. Por último, pero no menos importante, está el monitoreo y control continuo de las vulnerabilidades. Esta vigilancia constante es, en gran medida, lo que nos ayudará a prevenir intrusiones de personas ajenas a la organización.

Segunda recomendación

Un diagnóstico eficiente en una empresa requiere, en primer lugar, identificar la situación actual de la seguridad. Esto evita redundancias y nos da una base sólida para avanzar. El siguiente paso es evaluar todos los procesos de seguridad con ojo crítico, para discernir cuáles han quedado obsoletos y cuáles nuevos deben integrarse.

Aquí el factor humano es esencial: el personal responsable debe contar con experiencia previa o, en su defecto, con una capacitación sólida y continua. Por otro lado, la infraestructura lógica y física debe tener un soporte permanente que permita revisar y parchar vulneraciones de forma ágil. Implementar políticas de seguridad claras es otro pilar para reducir riesgos de manera proactiva.

Para la implementación en sí, se necesita un plan de riesgos bien definido que evalúe las amenazas potenciales. Una vez listo este plan, se procede a implementar siguiendo las directrices de la norma ISO. En esta fase, una planificación meticulosa de todos los procesos

es lo que nos permitirá, más adelante, diseñar un plan de mejora continua. Este ciclo es justamente lo que hace que la seguridad de la información se vuelva más robusta y resiliente con el tiempo.

VIII. REFERENCIAS

AL-Dosari, K., & Fetais, N. (2023). Risk-management framework and information-security systems for small and medium enterprises (SMEs): A meta-analysis approach. Electronics, 12(17), 3629. https://doi.org/10.3390/electronics12173629

Congreso de la República del Perú. (2011). Ley N.° 29733, Ley de Protección de Datos Personales. https://www.leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf

Cotos López, A. E., & Chombo Quezada, E. M. (2025). Propuesta de sistema de gestión basado en ISO 27001 para mejorar la seguridad de información en la Municipalidad Provincial del Santa. [Tesis de licenciatura, Universidad Nacional del Santa]. Repositorio Institucional de la Universidad Nacional del Santa. https://repositorio.uns.edu.pe/handle/20.500.14278/5255

Díaz-Bravo, L., Torruco-García, U., Martínez-Hernández, M., & Varela-Ruiz, M. (2013). La entrevista, recurso flexible y dinámico. Investigación en Educación Médica, 2(7), 162–167. https://doi.org/10.1016/S2007-5057(13)72706-6

García, S. B., Coral, M. Á. V., Rodríguez, I. E. C., & Rodríguez, D. L. (2021). Políticas basadas en la ISO 27001:2013 y su influencia en la gestión de seguridad de la información en municipalidades de Perú. Enfoque UTE, 12(2), 69–79. https://doi.org/10.29019/enfoqueute.743

Guizado Castillo, J. M. (2024). SGSI según ISO/IEC 27001:2022 y su incidencia en la protección de información en una municipalidad distrital, Lima 2023. [Tesis de maestría, Universidad César Vallejo]. Repositorio Institucional de la Universidad César Vallejo. https://hdl.handle.net/20.500.12692/135503

Hernández-Sampieri, R., & Mendoza Torres, C. P. (2018). Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta (1.ª ed.). McGraw-Hill Education.

Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2025). Cybersecurity in local governments: A systematic review and framework of key challenges. Urban Governance, 5(1), 1–19. https://doi.org/10.1016/j.ugj.2024.12.010

International Organization for Standardization, & International Electrotechnical Commission. (2020). ISO/IEC 27009:2020 Information security, cybersecurity and privacy protection—Sector-specific application of ISO/IEC 27001—Requirements. International Organization for Standardization.

International Organization for Standardization, & International Electrotechnical Commission. (2022a). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection—Information security management systems—Requirements. International Organization for Standardization.

International Organization for Standardization, & International Electrotechnical Commission. (2022b). ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection—Information security controls. International Organization for Standardization.

International Organization for Standardization, & International Electrotechnical Commission. (2022c). ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection—Guidance on managing information security risks. International Organization for Standardization.

Islam, M. S., & Karlsson, F. (2021). The public sector cloud service procurement in Sweden: An exploratory study of use and information security challenges. International Journal of Public Administration in the Digital Age, 8(1), 1–22. https://doi.org/10.4018/IJPADA.302906

Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2023). The ISO/IEC 27001 information security management standard: How to extract value from data in the IT sector. Sustainability, 15(7), 5828. https://doi.org/10.3390/su15075828

Krippendorff, K. (2019). Content analysis: An introduction to its methodology (4th ed.). SAGE Publications.

Limaymanta Ortiz, M. J. (2022). Auditoría basada en la norma ISO 27001 para la mejora de los controles de seguridad de la información en la Gerencia de Informática y Tecnología en una municipalidad peruana [Tesis de licenciatura, Universidad César Vallejo]. Repositorio Institucional de la Universidad César Vallejo. https://hdl.handle.net/20.500.12692/108918

Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic inquiry. SAGE Publications.

Magnusson, L., Iqbal, S., Elm, P., & Dalipi, F. (2025). Information security governance in the public sector: Investigations, approaches, measures, and trends. International Journal of Information Security, 24, Article 177. https://doi.org/10.1007/s10207-025-01097-x

Mayring, P. (2014). Qualitative content analysis: Theoretical foundation, basic procedures and software solution. Social Science Open Access Repository. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-395173

National Institute of Standards and Technology. (2012). Guide for conducting risk assessments (Special Publication 800-30, Revision 1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-30r1

Otzen, T., & Manterola, C. (2017). Técnicas de muestreo sobre una población a estudio. International Journal of Morphology, 35(1), 227–232. https://doi.org/10.4067/S0717-95022017000100037

Presidencia del Consejo de Ministros. (2018). Decreto Legislativo N.° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital. Diario Oficial El Peruano. https://busquedas.elperuano.pe/dispositivo/NL/1691026-1

Sánchez-Zurdo, J., & San-Martín, J. (2024). A country risk assessment from the perspective of cybersecurity in local entities. Applied Sciences, 14(24), 12036. https://doi.org/10.3390/app142412036

IX. ANEXOS

ANEXO A. MATRIZ DE CONSISTENCIA

MATRIZ DE CONSISTENCIA

Título:

Aplicación de la norma ISO/IEC 27009 para la prevención de riesgos del sistema de información en la Municipalidad Distrital de Chorrillos

Problemas	***Objetivos***	***Supuestos de investigación***	***Categorías***	***Subcategorías***	***Metodología***
Problema general: ¿De qué manera la aplicación de la norma ISO/IEC 27009 contribuye a la prevención de riesgos del sistema de información en la Municipalidad Distrital de Chorrillos?	Objetivo general: Analizar de qué manera la aplicación de la norma ISO/IEC 27009 contribuye a la prevención de riesgos del sistema de información en la Municipalidad Distrital de Chorrillos.	Supuesto general: La aplicación de lineamientos basados en la norma ISO/IEC 27009 contribuye a organizar controles de seguridad de la información y a fortalecer la prevención de riesgos del sistema de información en la Municipalidad Distrital de Chorrillos.	Aplicación de la norma ISO/IEC 27009. Prevención de riesgos del sistema de información.	Diagnóstico institucional. Implementación de controles. Adaptación al contexto municipal. Seguimiento y mejora continua. Disponibilidad. Confidencialidad. Gestión de incidentes. Protección de activos de información.	Tipo: aplicada. Enfoque: cualitativo. Alcance: descriptivo-interpretativo. Diseño: no experimental y transversal. Técnica: entrevista. Instrumento: guía de entrevista semiestructurada. Muestra: 10 participantes. Análisis: análisis de contenido cualitativo.
Problema específico 1: ¿De qué manera la aplicación de la norma ISO/IEC 27009 contribuye a fortalecer la disponibilidad del sistema de información en la Municipalidad Distrital de Chorrillos?	Objetivo específico 1: Analizar de qué manera la aplicación de la norma ISO/IEC 27009 contribuye a fortalecer la disponibilidad del sistema de información en la Municipalidad Distrital de Chorrillos.	Supuesto específico 1: La aplicación de la norma ISO/IEC 27009 contribuye a fortalecer la disponibilidad del sistema de información mediante controles orientados a la continuidad operativa, respaldo de información,	Prevención de riesgos del sistema de información. Aplicación de la norma ISO/IEC 27009.	Disponibilidad del sistema de información. Gestión de incidentes. Seguimiento y mejora continua.	Participantes: responsables, especialistas o trabajadores vinculados con seguridad de la información, administración de sistemas, soporte tecnológico, gestión de incidentes y protección de activos de información.

		gestión de incidentes y recuperación ante fallas.			
Problema específico 2: ¿De qué manera la aplicación de la norma ISO/IEC 27009 contribuye a fortalecer la confidencialidad del sistema de información en la Municipalidad Distrital de Chorrillos?	Objetivo específico 2: Analizar de qué manera la aplicación de la norma ISO/IEC 27009 contribuye a fortalecer la confidencialidad del sistema de información en la Municipalidad Distrital de Chorrillos.	Supuesto específico 2: La aplicación de la norma ISO/IEC 27009 contribuye a fortalecer la confidencialidad de la información mediante controles de acceso, protección de datos sensibles, trazabilidad de operaciones y gestión de permisos.	Prevención de riesgos del sistema de información. Aplicación de la norma ISO/IEC 27009.	Confidencialidad de la información. Protección de activos de información. Implementación de controles. Adaptación al contexto municipal.	Procesamiento: transcripción de entrevistas, codificación, organización por categorías, identificación de patrones y síntesis interpretativa.

Nota. Elaboración propia.

ANEXO B. GUÍA DE ENTREVISTA SEMIESTRUCTURADA

GUÍA DE ENTREVISTA SEMIESTRUCTURADA

1. ¿Cómo considera que debe aplicarse la norma ISO/IEC 27009 para prevenir riesgos del sistema de información en la Municipalidad Distrital de Chorrillos?

2. ¿Cómo debería elaborarse el diagnóstico institucional de la Municipalidad Distrital de Chorrillos para aplicar la norma ISO/IEC 27009?

a. ¿Cómo se deberían identificar los posibles riesgos de seguridad de la información?
b. ¿Cómo se deberían identificar los procesos vinculados con la seguridad de la información?
c. ¿Cómo se debería determinar la competencia del personal para aplicar la norma ISO/IEC 27009?
d. ¿Cómo se debería evaluar la infraestructura relacionada con la seguridad de la información?
e. ¿Cómo se deberían identificar las políticas de seguridad existentes?

3. ¿Cómo debería implementarse la norma ISO/IEC 27009 en la Municipalidad Distrital de Chorrillos?

4. ¿Qué riesgos podrían presentarse durante la implementación de la norma ISO/IEC 27009 en la Municipalidad Distrital de Chorrillos?

a. ¿Cómo se debería elaborar un plan de riesgos?
b. ¿En qué debería consistir la ejecución del plan de riesgos?
c. ¿Cómo se deberían planificar los procesos de ejecución de la norma ISO/IEC 27009?
d. ¿Cómo se debería elaborar un plan de mejora?

5. ¿Qué documentos y formatos considera necesarios para implementar la norma ISO/IEC 27009?

a. ¿Qué formatos deberían diseñarse para implementar la norma ISO/IEC 27009?

b. ¿Cómo debería ejecutarse la estandarización de la norma ISO/IEC 27009?

c. ¿Qué mecanismos de información son más pertinentes para aplicar la norma ISO/IEC 27009?

6. ¿Qué estrategias de seguimiento y control deberían aplicarse?

a. ¿Qué tipo de auditorías deberían realizarse?

b. ¿Cómo deberían determinarse las acciones correctivas?

c. ¿Cómo deberían determinarse las acciones preventivas?

ANEXO C. VALIDACIÓN Y CONFIABILIDAD CUALITATIVA DEL INSTRUMENTO

VALIDACIÓN Y CONFIABILIDAD DE INSTRUMENTO

Validación del instrumento

La validación del instrumento se realizó mediante juicio de expertos, con la finalidad de evaluar la claridad, pertinencia, coherencia y suficiencia de las preguntas incluidas en la guía de entrevista semiestructurada.

Para este proceso, se consultó a especialistas vinculados con seguridad de la información, gestión de riesgos, metodología de la investigación y normas de la familia ISO/IEC 27000. Los expertos revisaron la correspondencia entre las preguntas del instrumento, el problema de investigación, los objetivos, los supuestos de investigación, las categorías y subcategorías del estudio.

La validación permitió verificar que las preguntas fueran adecuadas para recoger información relevante sobre la aplicación de la norma ISO/IEC 27009 en el contexto de la Municipalidad Distrital de Chorrillos. Asimismo, permitió confirmar que el instrumento abordara aspectos vinculados con el diagnóstico institucional, disponibilidad, confidencialidad, gestión de riesgos, documentación, implementación de controles, seguimiento y mejora continua.

Las observaciones formuladas por los expertos fueron consideradas para mejorar la redacción de las preguntas, evitar ambigüedades y asegurar la coherencia del instrumento con el enfoque cualitativo de la investigación.

Alineación con los objetivos de la investigación

Las preguntas de la guía de entrevista semiestructurada fueron elaboradas en correspondencia con el objetivo general y los objetivos específicos de la investigación. En ese sentido, el instrumento permitió recoger información sobre la forma en que la aplicación de la

norma ISO/IEC 27009 contribuye a la prevención de riesgos del sistema de información en la Municipalidad Distrital de Chorrillos.

Asimismo, las preguntas permitieron abordar las dimensiones centrales del estudio: disponibilidad del sistema de información, confidencialidad de la información, gestión de riesgos, diagnóstico institucional, implementación de controles, documentación, seguimiento y mejora continua. Esta alineación permitió garantizar que la información recolectada fuera pertinente para el análisis cualitativo posterior.

Aplicación piloto del instrumento

De manera complementaria, se realizó una aplicación piloto de la guía de entrevista con un grupo reducido de participantes con características similares a la muestra del estudio. Esta aplicación permitió verificar la claridad de las preguntas, la comprensión de los términos utilizados y la pertinencia de la secuencia temática del instrumento.

A partir de la aplicación piloto, se realizaron ajustes de redacción en algunas preguntas, con la finalidad de facilitar su comprensión y mejorar la calidad de la información recolectada.

Confiabilidad del instrumento

La confiabilidad del instrumento se sustentó en la aplicación uniforme de la guía de entrevista semiestructurada a los diez participantes del estudio. Para ello, se mantuvo la misma estructura de preguntas, el mismo orden temático y los mismos criterios de registro durante el proceso de recolección de información.

Asimismo, la confiabilidad se fortaleció mediante la identificación de los entrevistados con códigos alfanuméricos del E1 al E10, el registro ordenado de las respuestas y la organización de la información en una matriz de desgravación de entrevistas. Posteriormente, las respuestas fueron revisadas y codificadas de acuerdo con las categorías y subcategorías de análisis.

Debido a que la investigación tiene enfoque cualitativo y utiliza como instrumento una

guía de entrevista semiestructurada, no se aplicó alfa de Cronbach ni pruebas estadísticas de consistencia interna, ya que dichos procedimientos corresponden principalmente a instrumentos cuantitativos con escalas de medición.

Criterios de confiabilidad cualitativa

Para fortalecer la confiabilidad del proceso de recolección y análisis de información, se consideraron los siguientes criterios:

Credibilidad: se aseguró mediante la correspondencia entre las preguntas de la entrevista, los objetivos de investigación y las respuestas proporcionadas por los participantes.

Consistencia: se garantizó mediante la aplicación de la misma guía de entrevista a todos los participantes, manteniendo el orden temático y los criterios de registro de información.

Confirmabilidad: se fortaleció mediante la conservación de las respuestas organizadas en la matriz de desgravación de entrevistas, permitiendo verificar la trazabilidad entre la información recolectada y los hallazgos presentados.

Transferibilidad: se favoreció mediante la descripción del contexto institucional, los criterios de selección de los participantes y las categorías de análisis utilizadas en la investigación.

Resultado de la validación y confiabilidad

Luego de la revisión realizada por los expertos y de la organización metodológica del instrumento, la guía de entrevista semiestructurada fue considerada aplicable para la recolección de información cualitativa. El instrumento permitió recoger datos pertinentes sobre la aplicación de la norma ISO/IEC 27009 y su contribución a la prevención de riesgos del sistema de información en la Municipalidad Distrital de Chorrillos.

En consecuencia, el instrumento fue considerado válido y confiable para los fines de la presente investigación cualitativa.

ANEXO D. MATRIZ DE ANÁLISIS CATEGORIAL

Categoría	*Pregunta*	*Síntesis de respuestas de entrevistados E1–E10*	*Análisis del investigador*
Implementación de la norma	¿Cómo considera que debe aplicarse la norma ISO/IEC 27009 para prevenir riesgos del sistema de información en la Municipalidad Distrital de Chorrillos?	Los entrevistados coinciden en que la implementación debe iniciar con el compromiso de la alta dirección, la asignación de recursos, el diagnóstico institucional y el establecimiento de lineamientos de seguridad de la información. También destacan la necesidad de identificar activos críticos, evaluar riesgos, aplicar controles, capacitar al personal, realizar monitoreo continuo y ejecutar auditorías periódicas.	La aplicación de la norma ISO/IEC 27009 requiere una gestión estructurada de la seguridad de la información. La participación de la alta dirección, el diagnóstico inicial, la capacitación y la mejora continua constituyen condiciones necesarias para fortalecer la prevención de riesgos en los sistemas de información municipales.
Diagnóstico institucional	¿Cómo debería elaborarse el diagnóstico institucional de la Municipalidad Distrital de Chorrillos para aplicar la norma ISO/IEC 27009?	Los entrevistados señalan que el diagnóstico debe incluir la evaluación de la infraestructura tecnológica, la revisión de políticas de seguridad existentes, el análisis de procesos institucionales, la identificación de activos críticos, la revisión documental, la evaluación de controles de acceso y la elaboración de un informe de brechas.	El diagnóstico institucional permite establecer una línea base sobre el estado actual de la seguridad de la información. Este proceso facilita la identificación de vulnerabilidades, brechas normativas y necesidades prioritarias para orientar la implementación de la norma en el contexto municipal.
Gestión de riesgos	¿Cómo se deberían identificar los posibles riesgos de seguridad de la información?	Los entrevistados mencionan el uso de metodologías de análisis de riesgos, auditorías de seguridad, pruebas de penetración, revisión de configuraciones, análisis de incidentes previos, evaluación de controles de acceso, identificación de riesgos internos y externos, y uso de herramientas de análisis de vulnerabilidades.	La identificación de riesgos constituye una etapa esencial para prevenir incidentes de seguridad. El uso combinado de auditorías, análisis de vulnerabilidades, revisión de incidentes y evaluación de controles permite priorizar amenazas y establecer medidas de mitigación.
Procesos de información	¿Cómo se deberían identificar los procesos vinculados con la seguridad de la información?	Los entrevistados indican que es necesario mapear los flujos de información entre áreas, documentar cómo se generan, procesan, almacenan, transmiten y eliminan los datos, identificar sistemas que gestionan información sensible y analizar el ciclo de vida de los datos.	El mapeo de procesos de información permite reconocer puntos críticos donde pueden producirse filtraciones, accesos indebidos o fallas de disponibilidad. Este análisis facilita la definición de controles adecuados para proteger la información durante todo su ciclo de vida.
Competencias del personal	¿Cómo se debería determinar la competencia del personal para aplicar la norma ISO/IEC 27009?	Los entrevistados coinciden en que debe evaluarse la experiencia del personal en seguridad de la información, su participación en proyectos tecnológicos, sus certificaciones, conocimientos técnicos, desempeño en gestión de	La competencia del personal es un factor crítico para la implementación de la norma. La capacitación, actualización tecnológica y cultura de seguridad permiten reducir errores humanos y fortalecer la aplicación efectiva de

		incidentes y necesidad de capacitación continua.	controles institucionales.
Infraestructura tecnológica	¿Cómo se debería evaluar la infraestructura relacionada con la seguridad de la información?	Los entrevistados recomiendan evaluar servidores, redes, sistemas de almacenamiento, mecanismos de respaldo, aplicaciones institucionales, dispositivos del personal, sistemas de acceso remoto, autenticación, firewalls, sistemas de detección de intrusos y cumplimiento de estándares tecnológicos.	La evaluación de la infraestructura tecnológica permite determinar si los recursos existentes son suficientes para proteger la información municipal. También permite identificar debilidades técnicas que podrían comprometer la disponibilidad, integridad o confidencialidad de los sistemas de información.
Políticas de seguridad	¿Cómo se deberían identificar las políticas de seguridad existentes?	Los entrevistados señalan que se deben revisar las normas internas, políticas de control de accesos, políticas de respaldo, uso de dispositivos tecnológicos, protocolos de respuesta ante incidentes y documentación institucional relacionada con protección de la información.	Las políticas de seguridad son necesarias para establecer responsabilidades, procedimientos y criterios homogéneos de protección de la información. Su revisión permite identificar vacíos normativos y proponer nuevas directrices alineadas con la ISO/IEC 27009.
Implementación de la norma	¿Cómo debería implementarse la norma ISO/IEC 27009 en la Municipalidad Distrital de Chorrillos?	La implementación debe iniciar con un diagnóstico de sistemas y procesos, pruebas de seguridad controladas, identificación de vulnerabilidades, elaboración de un plan de acción, definición de políticas, protocolos de respuesta, mecanismos de monitoreo continuo y participación de las áreas municipales.	La implementación de la norma debe asumirse como un proceso integral y progresivo. No se limita a controles técnicos, sino que requiere planificación, gestión de riesgos, cultura organizacional, continuidad operativa y participación de la alta dirección.
Riesgos institucionales	¿Qué riesgos podrían presentarse durante la implementación de la norma ISO/IEC 27009 en la Municipalidad Distrital de Chorrillos?	Los entrevistados identifican riesgos como resistencia al cambio, falta de capacitación, limitaciones tecnológicas, escasez de recursos, falta de apoyo de la alta dirección, procesos poco documentados, ausencia de personal especializado, errores humanos, ataques cibernéticos y falta de continuidad en los programas de seguridad.	La implementación de la norma enfrenta riesgos organizacionales, humanos y tecnológicos. Estos riesgos deben ser anticipados mediante planificación, asignación de recursos, capacitación, gestión del cambio y seguimiento institucional permanente.
Plan de riesgos	¿Cómo se debería elaborar un plan de riesgos?	Los entrevistados indican que el plan debe partir de la evaluación de riesgos, definir opciones de tratamiento, establecer acciones concretas, asignar responsables, plazos, recursos, controles, indicadores, presupuesto y mecanismos de revisión periódica.	El plan de riesgos permite ordenar la respuesta institucional frente a amenazas identificadas. Su utilidad depende de que sea documentado, aprobado por la alta dirección, comunicado a las áreas involucradas y revisado de manera continua.
Ejecución del plan de riesgos	¿En qué debería consistir la ejecución del plan de riesgos?	Los entrevistados señalan que la ejecución implica poner en marcha controles técnicos, organizativos y legales,	La ejecución del plan de riesgos convierte la planificación en acciones concretas. Para ser efectiva,

		capacitar al personal, documentar acciones, monitorear avances, gestionar incidentes y comunicar los progresos a la organización.	requiere control de cambios, documentación de evidencias, seguimiento de responsables y verificación del funcionamiento de los controles implementados.
Planificación de la implementación	¿Cómo se deberían planificar los procesos de ejecución de la norma ISO/IEC 27009?	Los entrevistados indican que se debe definir el alcance del SGSI, elaborar cronogramas, asignar responsables, establecer hitos, planificar recursos, comunicación, riesgos del proyecto, criterios de calidad y mecanismos de control de cambios.	La planificación de la implementación permite organizar los recursos y actividades necesarias para aplicar la norma. Una planificación formal reduce improvisaciones, facilita el seguimiento y mejora la sostenibilidad del proceso.
Plan de mejora	¿Cómo se debería elaborar un plan de mejora?	Los entrevistados señalan que el plan de mejora debe partir de auditorías, incidentes, no conformidades, indicadores y revisión por la dirección. Debe incluir análisis de causa raíz, acciones correctivas, acciones preventivas, responsables, plazos, recursos, seguimiento y verificación de eficacia.	El plan de mejora permite mantener la continuidad del sistema de gestión de seguridad de la información. Su aplicación fortalece el ciclo de mejora continua y evita que los problemas identificados se repitan.
Documentación de seguridad	¿Qué documentos y formatos considera necesarios para implementar la norma ISO/IEC 27009?	Los entrevistados mencionan el manual del SGSI, política de seguridad de la información, procedimientos documentados, plan de tratamiento de riesgos, plan de continuidad, declaración de aplicabilidad, inventarios de activos, registros de auditoría, reportes de incidentes y matriz de requisitos legales.	La documentación es fundamental para estandarizar la implementación de la norma. Además, permite demostrar trazabilidad, cumplimiento normativo y continuidad en la gestión de seguridad de la información.
Formatos necesarios	¿Qué formatos deberían diseñarse para implementar la norma ISO/IEC 27009?	Los entrevistados proponen formatos de control de documentos, inventario de activos, evaluación de riesgos, declaración de aplicabilidad, reporte de incidentes, auditoría interna, acciones correctivas y preventivas, asistencia a capacitaciones, revisión por la dirección y actas de reunión.	Los formatos facilitan la sistematización de los procesos de seguridad de la información. Su uso permite registrar evidencias, controlar acciones, hacer seguimiento y respaldar auditorías internas o externas.
Estandarización	¿Cómo debería ejecutarse la estandarización de la norma ISO/IEC 27009?	Los entrevistados señalan que la estandarización requiere procedimientos claros, capacitación, supervisión, uso uniforme de registros, auditorías internas, control documental, herramientas tecnológicas, revisión por la dirección y mejora continua.	La estandarización permite que los controles y procedimientos se conviertan en prácticas institucionales permanentes. Para ser efectiva, debe integrarse a la cultura organizacional y mantenerse mediante seguimiento y actualización documental.
Mecanismos de información	¿Qué mecanismos de información son más pertinentes para aplicar la norma ISO/IEC 27009?	Los entrevistados mencionan intranet, correo institucional, reuniones de comité, reuniones de área, afiches, boletines electrónicos, tableros de control, campañas de concienciación,	Los mecanismos de información favorecen la comunicación, sensibilización y seguimiento de la implementación. Una comunicación clara permite

		cursos de formación, buzones de sugerencias e informes de gestión.	fortalecer la cultura de seguridad y mejorar la participación del personal municipal.
Seguimiento y control	¿Qué estrategias de seguimiento y control deberían aplicarse?	Los entrevistados destacan el uso del ciclo PHVA, monitoreo técnico, revisión de indicadores, gestión de incidentes, auditorías internas, revisión por la dirección, gestión de no conformidades, seguimiento del plan de riesgos, revisión documental y retroalimentación de partes interesadas.	El seguimiento y control permiten verificar la eficacia de los controles implementados. Estas estrategias fortalecen la mejora continua y ayudan a corregir desviaciones en la gestión de seguridad de la información.
Auditorías	¿Qué tipo de auditorías deberían realizarse?	Los entrevistados mencionan auditorías internas, auditorías externas de certificación, auditorías de seguimiento, auditorías específicas, auditorías de cumplimiento legal, auditorías de proveedores, auditorías técnicas, pruebas de penetración y autoevaluaciones.	Las auditorías permiten comprobar el cumplimiento de la norma y detectar oportunidades de mejora. Su planificación periódica contribuye a mantener la eficacia del sistema de gestión de seguridad de la información.
Acciones correctivas	¿Cómo deberían determinarse las acciones correctivas?	Los entrevistados señalan que las acciones correctivas deben partir de la identificación de no conformidades, descripción objetiva del hallazgo, análisis de causa raíz, definición de acciones específicas, asignación de responsables, plazos, implementación, verificación de eficacia y documentación.	Las acciones correctivas permiten eliminar las causas de problemas detectados. Su adecuada gestión evita la repetición de fallas y fortalece el control institucional sobre los procesos de seguridad.
Acciones preventivas	¿Cómo deberían determinarse las acciones preventivas?	Los entrevistados indican que las acciones preventivas se determinan mediante análisis proactivo de riesgos, revisión de tendencias, lecciones aprendidas, cambios normativos o tecnológicos, sugerencias del personal y evaluación de amenazas antes de que ocurran incidentes.	Las acciones preventivas permiten anticipar riesgos y reducir la probabilidad de incidentes. Su aplicación contribuye a una gestión de seguridad más proactiva, alineada con la mejora continua y la prevención de vulnerabilidades.

ANEXO E. DIRECTIVA DE SEGURIDAD EN SISTEMAS INFORMÁTICOS

DIRECTIVA DE SEGURIDAD EN SISTEMAS INFORMÁTICOS DE LA MUNICIPALIDAD DISTRITAL DE CHORRILLOS

Finalidad

Establecer lineamientos básicos para la protección de los sistemas informáticos, activos de información, datos institucionales y servicios digitales de la Municipalidad Distrital de Chorrillos, con el propósito de prevenir riesgos que puedan afectar la disponibilidad, confidencialidad e integridad de la información municipal**.**

1. Objetivo

Regular el uso, acceso, administración, respaldo, protección y monitoreo de los sistemas informáticos de la Municipalidad Distrital de Chorrillos, tomando como referencia los lineamientos de seguridad de la información establecidos en la familia de normas ISO/IEC 27000 y, de manera específica, la adaptación de controles prevista en la norma ISO/IEC 27009.

2. Alcance

La presente directiva es aplicable a todos los órganos, unidades orgánicas, servidores, funcionarios, trabajadores, practicantes, proveedores y terceros que accedan, administren o utilicen sistemas informáticos, redes, bases de datos, plataformas digitales, equipos tecnológicos o información institucional de la Municipalidad Distrital de Chorrillos.

3. Base normativa

La presente directiva se sustenta en los principios de seguridad de la información, protección de datos personales, gobierno digital y gestión de riesgos tecnológicos. Asimismo,

considera como referencia técnica los lineamientos de la familia ISO/IEC 27000, especialmente las normas ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27009, en cuanto orientan la implementación, adaptación y mejora de controles de seguridad de la información.

4. Definiciones básicas

Término	Definición
Seguridad de la información	Conjunto de medidas orientadas a proteger la confidencialidad, integridad y disponibilidad de la información.
Sistema informático	Conjunto de aplicaciones, equipos, redes, bases de datos y recursos tecnológicos utilizados para procesar información institucional.
Activo de información	Información, sistema, base de datos, documento, equipo o recurso que posee valor para la institución.
Riesgo de seguridad	Posibilidad de que una amenaza aproveche una vulnerabilidad y afecte los sistemas o la información municipal.
Confidencialidad	Propiedad que garantiza que la información sea accesible solo para personas autorizadas.
Disponibilidad	Propiedad que asegura que la información y los sistemas estén accesibles cuando sean requeridos.
Integridad	Propiedad que garantiza que la información no sea alterada de forma no autorizada.
Incidente de seguridad	Evento que compromete o puede comprometer la seguridad de la información o de los sistemas informáticos.

5. Disposiciones generales

5.1. La Municipalidad Distrital de Chorrillos debe promover una cultura institucional de seguridad de la información, orientada a la prevención de riesgos, protección de datos y continuidad de los servicios digitales.

5.2. Todo usuario que acceda a sistemas informáticos municipales es responsable del uso adecuado de las credenciales, información, equipos y recursos tecnológicos asignados.

5.3. Los accesos a los sistemas informáticos deben otorgarse según las funciones del usuario, aplicando el principio de mínimo privilegio.

5.4. La información institucional debe ser protegida frente a accesos no autorizados, pérdida, modificación indebida, divulgación no permitida, interrupción del servicio o uso inadecuado.

5.5. Las unidades orgánicas deben comunicar oportunamente al área responsable de

tecnologías de información cualquier incidente, anomalía, pérdida de información, falla de sistema o sospecha de acceso no autorizado.

5.6. La implementación de controles de seguridad debe realizarse de manera progresiva, considerando la criticidad de los activos de información, los riesgos identificados y la disponibilidad de recursos institucionales.

6. Responsabilidades

6.1 Alta dirección municipal

La alta dirección municipal es responsable de promover, aprobar y respaldar las políticas, directivas, recursos y acciones necesarias para fortalecer la seguridad de la información y la prevención de riesgos en los sistemas informáticos institucionales.

6.2 Área de tecnologías de información

El área de tecnologías de información es responsable de administrar los sistemas informáticos, implementar controles técnicos, gestionar accesos, supervisar respaldos, monitorear incidentes, mantener la infraestructura tecnológica y proponer mejoras en materia de seguridad de la información.

6.3 Unidades orgánicas

Las unidades orgánicas son responsables de utilizar adecuadamente los sistemas informáticos, proteger la información bajo su administración, reportar incidentes y cumplir las disposiciones establecidas en la presente directiva.

6.4 Usuarios internos

Los usuarios internos son responsables de custodiar sus credenciales, utilizar los sistemas únicamente para fines institucionales, evitar la divulgación de información reservada y comunicar cualquier evento que pueda afectar la seguridad de la información.

6.5 Proveedores o terceros

Los proveedores o terceros que accedan a información, sistemas o infraestructura tecnológica municipal deben cumplir las condiciones de seguridad establecidas por la institución y mantener la confidencialidad de la información a la que tengan acceso.

7. Control de acceso a sistemas informáticos

7.1. Todo acceso a sistemas informáticos debe ser autorizado por el responsable correspondiente y registrado por el área de tecnologías de información.

7.2. Las cuentas de usuario deben ser personales e intransferibles.

7.3. Está prohibido compartir contraseñas, credenciales, tokens, accesos remotos o cuentas institucionales.

7.4. Los permisos deben asignarse de acuerdo con las funciones del usuario y deben revisarse periódicamente.

7.5. Cuando un trabajador cambie de área, suspenda funciones o culmine su vínculo con la institución, sus accesos deben ser modificados, suspendidos o eliminados oportunamente.

7.6. Se recomienda implementar mecanismos de autenticación robusta, especialmente en sistemas críticos o con acceso a información sensible.

7.7. La creación, modificación, bloqueo, reactivación, reseteo de clave o baja de cuentas de usuario deberá realizarse mediante el Formulario de creación, modificación y baja de cuenta de usuario, el cual forma parte de la presente directiva como formato complementario.

8. Uso de contraseñas

8.1. Las contraseñas deben mantenerse en reserva y no deben ser compartidas bajo ninguna circunstancia.

8.2. Las contraseñas deben tener una longitud y complejidad suficiente para reducir el riesgo de accesos no autorizados.

8.3. Los usuarios deben evitar utilizar contraseñas personales, repetidas, evidentes o asociadas a datos fácilmente identificables.

8.4. Las contraseñas deben cambiarse periódicamente o cuando exista sospecha de compromiso.

8.5. El área de tecnologías de información debe promover buenas prácticas de gestión de contraseñas.

9. Protección de información institucional

9.1. La información municipal debe clasificarse según su nivel de sensibilidad, criticidad y uso institucional.

92. La información sensible, reservada o confidencial debe ser protegida mediante controles de acceso, resguardo documental, cifrado cuando corresponda y mecanismos de trazabilidad.

9.3. Está prohibida la copia, extracción, modificación, eliminación o divulgación no autorizada de información institucional.

9.4. Los documentos digitales y físicos que contengan información sensible deben ser almacenados en repositorios seguros.

9.5. La información de ciudadanos, contribuyentes, proveedores, trabajadores y usuarios debe ser tratada con reserva y conforme a los principios de protección de datos personales.

10. Respaldo y recuperación de información

10.1. El área de tecnologías de información debe establecer procedimientos para el respaldo periódico de la información crítica.

10.2. Los respaldos deben realizarse con una frecuencia definida según la criticidad de los sistemas y datos institucionales.

10.3. Los medios de respaldo deben almacenarse en condiciones seguras, evitando accesos no autorizados, deterioro, pérdida o alteración.

10.4. Se deben realizar pruebas periódicas de restauración para verificar la eficacia de los respaldos.

10.5. Los procedimientos de respaldo y recuperación deben documentarse y mantenerse actualizados.

11. Gestión de incidentes de seguridad

11.1. Todo incidente de seguridad de la información debe ser reportado de manera inmediata al área de tecnologías de información.

11.2. Se consideran incidentes de seguridad los accesos no autorizados, pérdida de información, fallas críticas, infección por malware, alteración de datos, interrupciones no programadas, uso indebido de credenciales o cualquier evento que comprometa la seguridad de la información.

11.3. El área de tecnologías de información debe registrar, analizar, atender y cerrar los incidentes reportados.

11.4. Los incidentes deben documentarse indicando fecha, descripción, sistema afectado, usuario reportante, acciones realizadas, responsable y resultado de la atención.

11.5. Los incidentes recurrentes deben ser analizados para determinar causas y proponer acciones correctivas o preventivas.

12. Uso de equipos y recursos tecnológicos

12.1. Los equipos informáticos asignados por la municipalidad deben utilizarse

únicamente para fines institucionales.

12.2. Está prohibida la instalación de software no autorizado en equipos institucionales.

12.3. Los usuarios deben evitar conectar dispositivos externos no autorizados o de procedencia desconocida.

12.4. Los equipos deben contar con mecanismos básicos de protección, tales como antivirus, actualizaciones de seguridad y configuración adecuada.

12.5. El área de tecnologías de información debe realizar mantenimiento preventivo y correctivo de los equipos institucionales.

13. Seguridad en redes y comunicaciones

13.1. La red institucional debe ser administrada por el área de tecnologías de información.

13.2. El acceso a la red debe ser controlado y monitoreado, especialmente cuando se trate de sistemas críticos o información sensible.

13.3. El uso de redes inalámbricas debe contar con mecanismos de autenticación y cifrado adecuados.

13.4. El acceso remoto a sistemas municipales debe ser autorizado, registrado y protegido mediante controles de seguridad.

13.5. Se deben implementar mecanismos de monitoreo para detectar accesos sospechosos, anomalías o intentos de intrusión.

14. Continuidad operativa

14.1. La municipalidad debe identificar los sistemas y procesos críticos que requieren continuidad operativa.

14.2. El área de tecnologías de información debe proponer medidas para reducir interrupciones en los servicios digitales.

14.3. Se deben definir procedimientos mínimos de contingencia para responder ante

fallas tecnológicas, interrupciones de servicio, pérdida de información o incidentes graves.

14.4. Los planes de continuidad deben ser revisados y actualizados periódicamente.

14.5. La continuidad operativa debe considerar servicios críticos como recaudación, gestión documental, atención ciudadana, catastro, licencias, trámite documentario y otros sistemas institucionales relevantes.

15. Capacitación y sensibilización

15.1. La municipalidad debe promover actividades de capacitación y sensibilización sobre seguridad de la información.

15.2. Las capacitaciones deben abordar temas como uso seguro de contraseñas, protección de datos, reporte de incidentes, riesgos de ingeniería social, uso adecuado de equipos y buenas prácticas digitales.

15.3. El personal que administre sistemas críticos debe recibir formación específica en seguridad de la información, gestión de riesgos y continuidad operativa.

15.4. La sensibilización debe ser permanente y orientada a fortalecer la cultura institucional de protección de la información.

16. Auditoría, seguimiento y mejora continua

16.1. La municipalidad debe realizar revisiones periódicas del cumplimiento de la presente directiva.

16.2. El área de tecnologías de información debe informar sobre incidentes, riesgos identificados, acciones correctivas, respaldos, controles implementados y necesidades de mejora.

16.3. Se deben establecer indicadores básicos para evaluar la seguridad de la información, tales como incidentes reportados, tiempo de atención, cumplimiento de respaldos, revisión de accesos y actualización de sistemas.

16.4. Las desviaciones, incumplimientos o debilidades detectadas deben generar

acciones correctivas o preventivas.

16.5. La directiva debe revisarse periódicamente para mantener su vigencia frente a cambios tecnológicos, normativos e institucionales.

17. Prohibiciones

Queda prohibido:

a) Compartir credenciales de acceso a sistemas institucionales.

b) Acceder a información para fines distintos a las funciones asignadas.

c) Divulgar información institucional sensible sin autorización.

d) Instalar software no autorizado en equipos municipales.

e) Desactivar mecanismos de seguridad sin autorización del área competente.

f) Copiar, extraer o eliminar información institucional sin autorización.

g) Utilizar equipos o sistemas municipales para fines personales, comerciales o ajenos a la institución.

h) Omitir el reporte de incidentes de seguridad de la información.

i) Conectar dispositivos externos no autorizados a equipos o redes municipales.

j) Modificar configuraciones de seguridad sin autorización.

18. Medidas frente al incumplimiento

El incumplimiento de las disposiciones establecidas en la presente directiva será comunicado al área correspondiente para la evaluación de las acciones administrativas que correspondan, de acuerdo con la normativa interna aplicable y la gravedad del caso.

Cuando el incumplimiento pueda comprometer información sensible, datos personales, continuidad operativa o seguridad institucional, el área de tecnologías de información deberá adoptar medidas inmediatas de contención, mitigación y recuperación.

19. Disposición final

La presente directiva constituye un documento de orientación institucional para fortalecer la seguridad de los sistemas informáticos de la Municipalidad Distrital de Chorrillos. Su aplicación contribuye a prevenir riesgos, proteger la información municipal, mejorar la continuidad de los servicios digitales y promover una cultura de seguridad alineada con los principios de la norma ISO/IEC 27009.

Municipalidad de Chorrillos	FORMULARIO DE CUENTA DE USUARIO	Código:	FCU-01-OGTD
		Versión 1.0	Aprobación:
		SOLICITUD Nº	

SOLICITUD DE CREACIÓN, MODIFICACION Y BAJA DE CUENTA DE USUARIO

I. DATOS GENERALES

Fecha:	/ /												
Motivo de Solicitud:		Creación		Modificación		Baja		Bloqueo		Reactivación		Reseteo Clave	

II. DATOS DEL JEFE / GERENTE / SUBGERENTE SOLICITANTE

Apellidos y Nombres		DNI:	
Oficina/Gerencia / Subgerencia		Teléfono/ Anexo	
Cargo	Correo		

III. DATOS DEL USUARIO BENEFICIARIO DE LOS SERVICIOS:

Apellidos y Nombres		DNI:	
Oficina / Gerencia / Subgerencia		Teléfono/ Anexo	
Cargo / Rol / Servicio	Correo		
Modalidad	D. L. 276	D. L. 1057	Contrato	Orden de Servicio

IV. ACCESOS A LOS SISTEMAS:

SISTEMA DE GAT

- ☐ Módulos de Sistema de Caja
- ☐ Arbitrios Municipales
- ☐ Centro de Gestión de Ingresos
- ☐ Clona Declaraciones Juradas
- ☐ Compensación de Cuenta
- ☐ Notificaciones Tributarias
- ☐ Descargo de Cuenta Corriente
- ☐ Eliminar Intereses por campaña
- ☐ Emisión de Liquidaciones
- ☐ Fiscalización Tributaria
- ☐ Fraccionamiento Tributario
- ☐ Genera Recibo Tributo
- ☐ Gestión de Valores
- ☐ Impuesto Predial
- ☐ Tablas del Impuesto Predial
- ☐ Multas Administrativas
- ☐ Ejecutoria Coactiva
- ☐ Notificaciones Coactivas
- ☐ Coactivo Amnistía (Sin Interés)
- ☐ Pagos Manuales – descargos
- ☐ Información Gerencial
- ☐ Consulta – Caja
- ☐ Consultas Tributarias
- ☐ Consulta en General
- ☐ Consulta de ingresos por Centro de Costo

- ☐ Consultas
- ☐ Operaciones → PERMISOS
- ☐ Otros

- ☐ Colas
- ☐ Registro de Visitas

SISTEMA DE GESTION DOCUMENTAL

- ☐ Asistente o secretaria
- ☐ Especialista
- ☐ Visualización Mesa de Partes (**)

SISTEMA DE GDU

- ☐ Parámetros Urbanistico
- ☐ Licencia de Edificación
- ☐ Conformidad de Obra
- ☐ Autorización de Anuncios y Aviso Publicitario
- ☐ Constancia de Posesión

- ☐ Administrador
- ☐ Consulta → PERMISOS

SISTEMA DE GDET

- ☐ Licencia de Funcionamiento
- ☐ Certificado ITSE

- ☐ Administrador
- ☐ Consulta → PERMISOS

SISTEMA SIAF

- ☐ Módulo de Conciliación de cuentas de Enlace
- ☐ Módulo de Conciliación de operaciones SIAF
- ☐ Módulo Contable
- ☐ Módulo de Deuda Pública
- ☐ Módulo de Control de Pago de Planillas
- ☐ Módulo de Procesos Presupuestario
- ☐ Módulo de Administrativo
- ☐ Otros

PLATAFORMA DE INTEROPERABILIDAD DEL ESTADO (PIDE)

- ☐ Consulta Reniec
- ☐ Consulta Sunat
- ☐ Consulta Vehicular Sunarp
- ☐ Consulta Sunarp Titularidad
- ☐ Otros

☐ **ACCESO A LA RED INTERNA**

(Es el controlador principal de dominio, encargado de dar los accesos a la red y almacenar las cuentas de los usuarios; se encuentran protegido por un perimetro definido de seguridad)

☐ **CORREO INSTITUCIONAL**

(**+) Para Validar este acceso, debe tener la autorización de la Oficina de Gestión Documentaria y Atención al Ciudadano via email.
La confidencialidad de los datos de la Cuenta de Usuario y contraseña es de exclusiva responsabilidad del Usuario, así como todas las actividades realizadas en el sistema de Información con en nombre de Usuario y contraseña.
Por tal motivo, declaró bajo juramento que toda la información proporcionada es veraz, en caso contrario, me someto al procedimiento y a las sanciones previstas en la Ley Nº 27444, Ley del Procedimiento Administrativo General. Finalmente, se rubrican la firma en señal de fe y consentimiento de que las actividades sean susceptibles de ser auditadas en cualquier momento.

Chorrillos, _____de _____del 2,02__

_____
Jefe/Gerente /Subgerente
(Firma Digital)

Nota. Elaboración propia, tomando como referencia los lineamientos de seguridad de la información aplicables a la gestión municipal y la adaptación de controles prevista en la norma ISO/IEC 27009

ANEXO F. MATRIZ DE DESGRAVACIÓN DE ENTREVISTA

MATRIZ DE DESGRAVACIÓN DE ENTREVISTA

"Aplicación de la norma ISO/IEC 27009 para prevenir riesgos del sistema de información en la Municipalidad de Chorrillos"

1, ¿Cómo aplicar la norma ISO/IEC 27009 para prevenir riesgos del sistema de información en la Municipalidad de Chorrillos?

E1: El compromiso de la alta dirección municipal es fundamental no solo por ser un requisito normativo, sino porque de este depende la asignación de recursos humanos, técnicos y financieros esenciales para ejecutar proyectos de manera exitosa. En un entorno dinámico como Chorrillos, los riesgos en seguridad como amenazas constantes, vulnerabilidades detectadas en servicios públicos o incidentes con impacto en la ciudadanía exigen una gestión proactiva y adaptativa.

Para implementar la norma ISO, la municipalidad debe iniciar con un diagnóstico integral de su situación actual, evaluando procesos administrativos, sistemas de información y protocolos de protección de datos. Este análisis permitirá determinar la viabilidad de cumplir los requisitos de la norma elegida y establecer prioridades acordes a las necesidades locales. Una vez identificado el punto de partida, se requiere un plan de implementación documentado, alineado con la realidad institucional de la Municipalidad de Chorrillos. Este plan debe detallar los procesos clave (ej. atención al ciudadano, gestión documental, ciberseguridad), asignar responsabilidades a áreas específicas (como TI, Gerencia Municipal, como también planeamiento y presupuesto), definir cronogramas realistas y establecer mecanismos de seguimiento para garantizar el avance hacia los objetivos. La transparencia en la ejecución, junto con la capacitación del personal y la optimización de recursos, será clave para obtener la

certificación ISO y fortalecer la confianza ciudadana mediante servicios más eficientes y seguros.

E2: Para aplicar la norma ISO/IEC 27009 en la Municipalidad de Chorrillos, es fundamental iniciar con un diagnóstico institucional que permita identificar de manera precisa los activos de información críticos, las amenazas potenciales y las vulnerabilidades presentes en los sistemas informáticos municipales. Este análisis debe servir como base para definir controles específicos y alineados con las necesidades del sector público, garantizando la protección de datos ciudadanos y la continuidad de los servicios municipales. Asimismo, la norma facilita la integración de requisitos adicionales a los establecidos en ISO/IEC 27001, adaptándolos al contexto gubernamental y asegurando la coherencia con marcos regulatorios nacionales. Con ello, se logra establecer un sistema de gestión de seguridad de la información robusto, capaz de prevenir riesgos, mitigar incidentes y fortalecer la confianza de la comunidad en la gestión digital de la municipalidad.

E3: Resulta esencial establecer un marco de políticas de seguridad claras que definan responsabilidades y lineamientos para el manejo de la información. Estas políticas deben complementarse con procedimientos operativos que regulen el acceso, uso y protección de los datos municipales, asegurando que cada área cumpla con estándares homogéneos. Asimismo, es necesario implementar controles tecnológicos como sistemas de autenticación, cifrado y monitoreo continuo, que garanticen la confidencialidad, integridad y disponibilidad de la información crítica. La norma permite adaptar los requisitos de ISO/IEC 27001 a un contexto específico, en este caso el sector público, fortaleciendo la gestión de riesgos y la resiliencia institucional. Con ello, se previenen incidentes de seguridad, se asegura la continuidad de los servicios digitales y se refuerza la confianza de los ciudadanos en la administración municipal.

E4: Es clave conformar un equipo especializado que asuma la responsabilidad de la gestión de la seguridad de la información y supervise de manera integral la implementación de

los controles definidos. Este grupo debe estar compuesto por profesionales con competencias técnicas y normativas, capaces de coordinar acciones entre las distintas áreas municipales. Su labor incluye monitorear riesgos, evaluar la eficacia de las medidas aplicadas y garantizar la actualización constante de políticas y procedimientos. Además, el equipo debe promover la cultura de seguridad en todos los niveles de la organización, asegurando que los funcionarios comprendan la importancia de proteger los datos ciudadanos. Con esta estructura, se fortalece la capacidad institucional para prevenir incidentes, responder de forma oportuna y mantener la confianza de la comunidad en los servicios digitales municipales.

E5: La capacitación del personal es fundamental para garantizar la protección de la información institucional. Es necesario diseñar programas de formación continua que aborden tanto aspectos técnicos como normativos, asegurando que los funcionarios comprendan la relevancia de la confidencialidad, integridad y disponibilidad de los datos municipales. Estas capacitaciones deben incluir simulaciones de incidentes, buenas prácticas en el manejo de contraseñas y protocolos de respuesta ante riesgos. Además, la sensibilización debe extenderse a todos los niveles de la organización, fomentando una cultura de seguridad que trascienda lo meramente tecnológico. Con ello, se fortalece la capacidad institucional para prevenir vulnerabilidades y se refuerza la confianza de los ciudadanos en la gestión digital de la municipalidad.

E6: Es recomendable implementar metodologías de gestión de riesgos que permitan identificar, evaluar y priorizar los riesgos más críticos que afectan a los sistemas municipales. Estas metodologías deben incluir un análisis sistemático de amenazas, vulnerabilidades y posibles impactos sobre los servicios digitales y la información ciudadana. Con base en estos resultados, se pueden diseñar planes de acción que asignen recursos de manera eficiente y establezcan controles específicos para mitigar los riesgos más relevantes.

E7: Para aplicar la norma ISO/IEC 27009 en la Municipalidad de Chorrillos, la implementación debe contemplar herramientas de monitoreo y detección de incidentes que permitan identificar amenazas en tiempo real y actuar de manera inmediata. Estas soluciones tecnológicas, como sistemas de gestión de eventos de seguridad (SIEM) o plataformas de análisis de tráfico, facilitan la detección temprana de anomalías y posibles ataques. Además, es importante establecer protocolos claros de respuesta que definan responsabilidades y tiempos de acción ante incidentes detectados. El monitoreo continuo no solo fortalece la capacidad de prevención, sino que también contribuye a la mejora constante de los controles de seguridad. Con ello, la municipalidad asegura la protección de la información institucional y la continuidad de los servicios digitales que brindan confianza a la ciudadanía.

E8: Para aplicar la norma es importante integrarla de manera coherente con los procesos administrativos y tecnológicos ya existentes. Esto implica revisar y adaptar los flujos de trabajo municipales para que las prácticas de seguridad de la información no se perciban como actividades aisladas, sino como parte natural de la gestión institucional. La integración debe abarcar desde la gestión documental y los trámites digitales hasta los sistemas de atención ciudadana, asegurando que cada área cumpla con estándares homogéneos de protección. Asimismo, se deben establecer mecanismos de coordinación entre las unidades administrativas y el área de TI para garantizar la aplicación efectiva de los controles.

E9: Resulta esencial establecer indicadores de seguridad que permitan medir de manera objetiva el nivel de protección de la información institucional. Estos indicadores deben abarcar aspectos como el número de incidentes detectados, el tiempo de respuesta ante amenazas, el grado de cumplimiento de políticas y la efectividad de los controles implementados. Al contar con métricas claras, la municipalidad puede evaluar periódicamente su desempeño y detectar áreas de mejora en la gestión de la seguridad. Además, los indicadores facilitan la toma de

decisiones estratégicas y la asignación adecuada de recursos para fortalecer la resiliencia digital.

E10: Para aplicar la norma ISO/IEC 27009 en la Municipalidad de Chorrillos, es indispensable realizar auditorías periódicas que verifiquen el cumplimiento de los controles y políticas de seguridad establecidos. Estas auditorías deben evaluar tanto los procesos administrativos como los tecnológicos, identificando brechas y oportunidades de mejora en la protección de la información institucional. Además, permiten validar la eficacia de las medidas implementadas y asegurar que se mantengan alineadas con los requisitos normativos y legales vigentes. El proceso de auditoría debe incluir informes claros y recomendaciones prácticas que orienten a la municipalidad hacia la mejora continua.

2. ¿Cómo elaborar el diagnóstico de la Municipalidad de Chorrillos para aplicar la norma ISO 27009?

E1: Para realizar un diagnóstico integral en materia de seguridad de la información, la municipalidad debe seguir pasos clave. Primero, evaluar las medidas actuales de protección de datos, como protocolos para resguardar la privacidad digital en trámites municipales (ej. registros ciudadanos, plataformas de pago) y evitar accesos no autorizados a sistemas críticos (gestión catastral, bases de datos de contribuyentes). Luego, se deben analizar los procesos internos para garantizar que cumplan con los requisitos de la norma ISO seleccionada, priorizando áreas sensibles como la gestión documental o la ciberseguridad en servicios públicos. Esta necesidad ha incrementado la demanda de expertos en protección de datos que fortalezcan sistemas municipales y reduzcan vulnerabilidades.

E2: Para elaborar el diagnóstico de la Municipalidad de Chorrillos en el marco de la norma ISO 27009, es fundamental revisar las políticas de seguridad existentes y evaluar su nivel de cumplimiento con los estándares internacionales. Este análisis debe incluir la

identificación de activos de información críticos, como registros ciudadanos, sistemas de recaudación y plataformas digitales de atención. Asimismo, se requiere examinar los controles de acceso, la gestión documental y los mecanismos de protección de datos personales frente a posibles vulnerabilidades. El diagnóstico debe contemplar también la alineación con la normativa nacional de protección de datos y la capacidad de respuesta ante incidentes de seguridad.

E3: Se deben analizar de manera detallada los procesos institucionales que utilizan información digital. Esto implica revisar cómo se gestionan los datos en trámites ciudadanos, plataformas de recaudación y sistemas de catastro, identificando posibles vulnerabilidades. Es necesario evaluar la eficacia de los controles de acceso, la trazabilidad de la información y la protección frente a incidentes de seguridad.

E4: Se recomienda realizar entrevistas con el personal del área de tecnologías de información. Estas entrevistas permiten identificar prácticas actuales de seguridad, conocer la percepción de riesgos y evaluar el nivel de cumplimiento de las políticas internas. Además, facilitan la detección de brechas en la gestión de accesos, protección de datos y continuidad de servicios digitales. Es importante complementar estas entrevistas con la revisión documental y el análisis de procesos críticos, como la recaudación tributaria y la gestión catastral. De esta manera, se obtiene una visión integral que combina la experiencia del personal con los requisitos normativos, generando insumos valiosos para definir un plan de acción estratégico.

E5: Para elaborar el diagnóstico de la Municipalidad de Chorrillos en el marco de la norma ISO 27009, la revisión de la documentación institucional resulta esencial para identificar posibles brechas en la gestión de la seguridad de la información. Este proceso debe abarcar políticas internas, manuales de procedimientos, registros de incidentes y protocolos de acceso a sistemas críticos. Al analizar estos documentos, se pueden detectar inconsistencias entre las

prácticas actuales y los estándares internacionales de seguridad. Asimismo, la revisión permite evaluar la trazabilidad de los procesos y la protección de datos personales en trámites digitales.

E6: Se deben evaluar de manera rigurosa los controles de acceso a los sistemas informáticos. Este análisis debe considerar la gestión de credenciales, la implementación de autenticación multifactor y la segregación de funciones en áreas críticas. Asimismo, es necesario revisar los permisos otorgados a usuarios internos y externos, verificando que se ajusten al principio de mínimo privilegio. La evaluación debe incluir pruebas de resistencia frente a intentos de intrusión y auditorías periódicas de accesos.

E7: Es necesario analizar los procedimientos de respaldo y recuperación de información. Este análisis debe incluir la revisión de las políticas de copias de seguridad, la frecuencia con que se realizan y la seguridad de los medios utilizados para almacenarlas. Asimismo, se debe evaluar la eficacia de los planes de recuperación ante desastres y su capacidad para garantizar la continuidad de los servicios municipales. Es importante verificar que los procedimientos estén documentados, probados periódicamente y alineados con los estándares internacionales de seguridad.

E8: El proceso debe incluir un análisis de riesgos preliminar que permita identificar amenazas potenciales y evaluar su impacto en los activos de información. Este análisis debe considerar tanto riesgos internos, como fallas en procesos o accesos indebidos, como externos, tales como ciberataques o desastres naturales. Es fundamental clasificar los riesgos según su probabilidad y nivel de impacto, priorizando aquellos que afectan servicios críticos como la recaudación tributaria y la gestión catastral. Asimismo, se deben revisar las medidas de mitigación existentes y determinar si cumplen con los estándares internacionales de seguridad.

E9: Se deben identificar de manera precisa los activos críticos de información que sostienen la operación institucional. Esto incluye bases de datos de contribuyentes, sistemas de gestión catastral, plataformas de recaudación y registros ciudadanos digitales. La identificación

debe considerar tanto el valor estratégico de cada activo como su nivel de exposición frente a amenazas internas y externas. Asimismo, es necesario clasificar estos activos según su importancia para la continuidad de los servicios municipales y el cumplimiento de la normativa vigente.

E10: Para elaborar el diagnóstico de la Municipalidad de Chorrillos en el marco de la norma ISO 27009, finalmente se debe elaborar un informe que resuma de manera clara las debilidades y fortalezas del sistema actual de seguridad de la información. Este documento debe incluir los hallazgos obtenidos en la revisión de políticas, procesos, controles de acceso y gestión de riesgos. Asimismo, debe destacar las áreas que cumplen con los estándares internacionales y aquellas que requieren mejoras urgentes.

a) ¿Cómo identificar los posibles riesgos de seguridad?

E1: La identificación de riesgos de seguridad requiere aplicar metodologías que evalúen tanto el impacto como la probabilidad de amenazas, utilizando herramientas como el análisis FODA o el análisis de escenarios. Estas técnicas permiten anticipar vulnerabilidades y priorizar acciones preventivas. Además, es fundamental complementar el enfoque con pruebas de penetración que simulen ataques reales y revelen debilidades técnicas. Las auditorías periódicas, por su parte, garantizan el cumplimiento de estándares y la detección temprana de fallas.

E2: La identificación de riesgos de seguridad puede lograrse mediante auditorías especializadas en los sistemas informáticos, que permiten evaluar su nivel de protección y cumplimiento normativo. Estas auditorías analizan configuraciones, accesos y controles internos para detectar posibles debilidades. Asimismo, facilitan la verificación de políticas de seguridad y la eficacia de los mecanismos de defensa implementados.

E3: La identificación de riesgos de seguridad puede realizarse mediante pruebas de penetración, diseñadas para simular ataques reales y evaluar la resistencia de los sistemas. Estas pruebas permiten descubrir vulnerabilidades técnicas que podrían ser explotadas por actores maliciosos. Además, ofrecen información valiosa para priorizar medidas correctivas y fortalecer la infraestructura crítica. Al ejecutarse de manera controlada y periódica, garantizan un proceso de mejora continua en la protección informática.

E4: La identificación de riesgos de seguridad también puede lograrse mediante el análisis de incidentes ocurridos anteriormente, lo que permite aprender de experiencias pasadas. Este enfoque facilita reconocer patrones de ataque y vulnerabilidades recurrentes en la infraestructura tecnológica. Además, ayuda a evaluar la eficacia de las medidas de respuesta implementadas y a detectar posibles brechas en los protocolos de seguridad.

E5: La identificación de riesgos de seguridad puede realizarse evaluando los controles de acceso existentes, verificando su eficacia frente a posibles intentos de intrusión. Este análisis permite detectar configuraciones débiles, permisos excesivos o fallas en la gestión de credenciales. Asimismo, facilita la revisión de políticas de autenticación y autorización para garantizar que se apliquen de manera adecuada.

E6: La identificación de riesgos de seguridad puede lograrse mediante la detección de posibles fallas en la infraestructura tecnológica, evaluando su capacidad de respuesta ante incidentes. Este análisis permite reconocer debilidades en servidores, redes y dispositivos críticos que podrían comprometer la operación. Asimismo, facilita la revisión de configuraciones y la verificación del cumplimiento de estándares de seguridad.

E7: La identificación de riesgos de seguridad también implica considerar los riesgos internos asociados al factor humano, dado que los errores o malas prácticas pueden comprometer la protección de la información. Este análisis permite detectar conductas inseguras, falta de capacitación o incumplimiento de políticas organizacionales.

E8: La identificación de riesgos de seguridad requiere analizar los riesgos externos, entre ellos los ataques cibernéticos que representan una amenaza constante para las organizaciones. Este enfoque permite evaluar la exposición frente a malware, phishing, ransomware y otras técnicas de intrusión. Asimismo, facilita la implementación de medidas preventivas y planes de respuesta ante incidentes.

E9: La identificación de riesgos de seguridad puede realizarse revisando las configuraciones de seguridad de servidores y redes, asegurando que estén alineadas con las mejores prácticas. Este análisis permite detectar parámetros inadecuados, accesos no autorizados o servicios expuestos que incrementan la vulnerabilidad. Asimismo, facilita la verificación de actualizaciones, parches y protocolos de comunicación seguros.

E10: La identificación de riesgos de seguridad puede realizarse utilizando herramientas especializadas de análisis de vulnerabilidades, capaces de detectar fallas técnicas en sistemas y aplicaciones. Estas soluciones permiten evaluar configuraciones, parches y niveles de exposición frente a amenazas externas. Asimismo, generan reportes detallados que facilitan la priorización de medidas correctivas y la optimización de controles de seguridad.

b) ¿Cómo identificar los procesos de información de seguridad?

E1: Es necesario realizar un mapeo exhaustivo de todos los flujos de datos que circulan entre áreas y sistemas. Este análisis debe incluir la documentación detallada de los procesos vinculados al manejo de información sensible, como datos personales de ciudadanos o registros financieros. Posteriormente, se evalúa cómo se protegen dichos datos en cada etapa de su ciclo de vida: recolección, almacenamiento, transmisión, uso y eliminación.

E2: Es fundamental comenzar con el reconocimiento de los flujos de información entre las distintas áreas y dependencias. Este análisis debe permitir visualizar cómo se generan, transmiten y almacenan los datos, especialmente aquellos de carácter sensible.

E3: Es necesario documentar de manera precisa cómo se genera, procesa y almacena la información en cada área. Este análisis debe incluir la clasificación de los datos según su nivel de sensibilidad, así como la identificación de los sistemas y responsables que intervienen en su gestión.

E4: Resulta esencial analizar de manera detallada los sistemas que gestionan datos sensibles. Este estudio debe incluir la revisión de las plataformas tecnológicas, bases de datos y aplicaciones utilizadas para almacenar y procesar información crítica. A partir de ello, se documentan los procedimientos de acceso, transmisión y protección de los datos, verificando la existencia de controles adecuados.

E5: Es indispensable evaluar los mecanismos de protección que se aplican sobre los datos sensibles. Este análisis debe considerar tanto las medidas tecnológicas como cifrado, autenticación y control de accesos como las políticas y procedimientos internos que regulan el uso de la información. A partir de ello, se documenta cómo se asegura la integridad, disponibilidad y confidencialidad de los datos en cada etapa de su ciclo de vida.

E6: Es necesario revisar cuidadosamente los procedimientos de intercambio de información entre las diferentes áreas. Este análisis permite detectar cómo circulan los datos, qué canales se utilizan y qué controles existen para garantizar su integridad y confidencialidad. A partir de ello, se documentan los responsables y las políticas aplicadas en cada etapa del flujo de información.

E7: Es fundamental analizar el ciclo de vida completo de los datos. Este estudio debe abarcar desde su creación y recolección, pasando por el procesamiento y almacenamiento, hasta su transmisión y eventual eliminación. En cada etapa se deben documentar los responsables, los sistemas utilizados y los controles de seguridad aplicados para garantizar la integridad y confidencialidad de la información.

E8: Es clave reconocer los puntos críticos donde puede existir riesgo de filtración de datos. Este análisis debe abarcar tanto los sistemas tecnológicos como los procedimientos administrativos que manejan información sensible. A partir de ello, se documentan los flujos de datos y se evalúan los controles aplicados en cada etapa, verificando su eficacia frente a posibles amenazas.

E9: Es esencial evaluar la seguridad de los sistemas de almacenamiento de datos. Este análisis debe considerar la infraestructura tecnológica utilizada, verificando si cuenta con mecanismos de cifrado, redundancia y control de accesos adecuados. Asimismo, se deben documentar los procedimientos de respaldo y recuperación, asegurando la disponibilidad y continuidad de la información en caso de incidentes.

E10: Es necesario documentar de manera integral todos los procedimientos relacionados con la gestión de la información. Este trabajo debe incluir la descripción de cómo se generan, procesan, transmiten, almacenan y eliminan los datos, especialmente aquellos de carácter sensible.

c) ¿Cómo determinar la competencia del personal para aplicar la norma ISO 27009?

E1: Se determina mediante la evaluación integral de su experiencia previa en gestión de seguridad de la información, la verificación de certificaciones y capacitaciones específicas en la norma, así como la actualización constante en mejores prácticas y estándares internacionales. Además, se consideran sus habilidades técnicas en análisis de riesgos, continuidad de negocio y cumplimiento normativo, junto con la capacidad de aplicar metodologías de auditoría y mejora continua. Es clave validar la participación en proyectos relacionados con seguridad y la adaptación a entornos regulados.

E2: Puede determinarse mediante un análisis sistemático de su experiencia en el área de TI, evaluando proyectos previos relacionados con seguridad de la información y continuidad operativa. Es fundamental verificar que los profesionales cuenten con conocimientos prácticos en gestión de riesgos, cumplimiento normativo y adaptación de controles de seguridad a distintos sectores.

E3: Se fortalece mediante la implementación de programas de capacitación estructurados y continuos, orientados a desarrollar conocimientos específicos en gestión de seguridad de la información. Estos programas deben incluir formación en la norma, actualización en estándares internacionales y prácticas de cumplimiento regulatorio. Asimismo, es importante incorporar talleres prácticos que permitan aplicar controles de seguridad en escenarios reales y fomentar la cultura de mejora continua.

E4: Se asegura mediante evaluaciones periódicas que permitan medir sus conocimientos, habilidades y desempeño en la gestión de la seguridad de la información. Estas evaluaciones deben incluir pruebas técnicas, revisión de certificaciones y análisis de la experiencia práctica en proyectos relacionados con continuidad y cumplimiento normativo.

E5: Se puede garantizar promoviendo certificaciones profesionales en seguridad informática que validen sus conocimientos y habilidades técnicas. Estas certificaciones permiten demostrar dominio en gestión de riesgos, cumplimiento normativo y aplicación de controles de seguridad en distintos entornos.

E6: Puede evaluarse analizando su desempeño en la gestión de incidentes de seguridad, verificando la eficacia de sus respuestas y la correcta aplicación de protocolos establecidos. Es fundamental medir la capacidad de identificar, contener y resolver incidentes, así como documentar las lecciones aprendidas para fortalecer la resiliencia organizacional.

E7: Se puede fortalecer mediante la realización de talleres de formación enfocados en buenas prácticas de seguridad de la información. Estos espacios permiten que los colaboradores

adquieran conocimientos prácticos sobre gestión de riesgos, cumplimiento normativo y aplicación de controles específicos.

E8: Se fortalece fomentando una cultura de seguridad dentro de la institución, donde cada miembro asuma la protección de la información como una responsabilidad compartida. Este enfoque implica promover valores, actitudes y comportamientos alineados con las mejores prácticas de seguridad, integrando la norma en las actividades cotidianas.

E9: Se puede garantizar implementando programas de actualización tecnológica que mantengan a los profesionales al día con las herramientas, plataformas y tendencias más recientes en seguridad de la información. Estos programas deben incluir capacitaciones en nuevas soluciones de gestión de riesgos, continuidad operativa y cumplimiento normativo.

E10: La competencia del personal para aplicar la norma ISO/IEC 27009 se asegura supervisando de manera constante el cumplimiento de los procedimientos de seguridad establecidos en la organización. Esta supervisión permite verificar que las prácticas implementadas estén alineadas con los requisitos normativos y que se apliquen de forma consistente en todos los niveles. Además, facilita la detección temprana de desviaciones o incumplimientos, generando acciones correctivas oportunas.

d) ¿Cómo determinar la infraestructura del proceso de seguridad de la Información?

E1: Debe definirse considerando su capacidad para sostener de manera integral las medidas establecidas en la norma ISO/IEC 27009. Esto implica analizar la robustez de servidores, redes y aplicaciones, así como la confiabilidad de los dispositivos de almacenamiento y las políticas de respaldo implementadas. Además, es esencial evaluar la escalabilidad y redundancia de los sistemas para garantizar continuidad operativa frente a incidentes.

E2: Puede determinarse mediante un análisis exhaustivo de las redes institucionales, evaluando su nivel de protección y capacidad de respuesta frente a amenazas. Este examen debe incluir la revisión de configuraciones, segmentación, controles de acceso y mecanismos de detección de intrusiones.

E3: Debe evaluarse revisando de manera integral los sistemas de almacenamiento de datos, garantizando su confiabilidad y protección frente a riesgos. Es necesario analizar la capacidad de los repositorios para asegurar la integridad, disponibilidad y confidencialidad de la información crítica.

E4: Debe verificarse asegurando la existencia y eficacia de sistemas de respaldo que garanticen la continuidad operativa. Es fundamental evaluar la periodicidad de las copias de seguridad, su integridad y la capacidad de recuperación ante incidentes. Asimismo, se debe revisar la redundancia de los repositorios y la protección de los datos respaldados mediante cifrado y controles de acceso.

E5: La infraestructura del proceso de seguridad de la información debe evaluarse considerando el uso de firewalls y sistemas de detección de intrusos como elementos clave de protección. Es fundamental analizar la correcta configuración de estos dispositivos, asegurando que bloqueen accesos no autorizados y monitoreen actividades sospechosas en tiempo real.

E6: Debe evaluarse mediante un análisis detallado de las aplicaciones institucionales, verificando que cumplan con estándares de protección y buenas prácticas. Es esencial revisar la gestión de accesos, la implementación de autenticación robusta y la protección contra vulnerabilidades comunes. Asimismo, se debe garantizar que las aplicaciones cuenten con actualizaciones periódicas y pruebas de seguridad que validen su resistencia frente a ataques.

E7: Revisando la protección de los dispositivos utilizados por el personal, asegurando que cuenten con medidas de seguridad adecuadas. Es fundamental verificar la implementación de antivirus, sistemas de cifrado y controles de acceso que reduzcan riesgos de vulnerabilidad.

Asimismo, se debe garantizar la actualización constante de software y parches de seguridad para prevenir incidentes.

E8: Debe evaluarse considerando la protección de los sistemas de acceso remoto, dado que representan un punto crítico de exposición. Es esencial verificar la implementación de mecanismos de autenticación robusta, cifrado de comunicaciones y controles de acceso diferenciados. Asimismo, se debe revisar la configuración de VPNs, firewalls y sistemas de monitoreo que garanticen la detección temprana de intentos de intrusión.

E9: Analizando los mecanismos de autenticación utilizados, ya que constituyen la primera línea de defensa contra accesos no autorizados. Es fundamental revisar la robustez de las credenciales, la implementación de autenticación multifactor y la gestión segura de contraseñas. Asimismo, se debe verificar la integración de certificados digitales y protocolos de validación confiables.

E10: Debe evaluarse verificando el cumplimiento de los estándares de seguridad tecnológica, asegurando la alineación con normas internacionales reconocidas. Es esencial revisar la implementación de controles técnicos, políticas organizacionales y procedimientos que garanticen la protección integral de los activos. Asimismo, se debe analizar la actualización constante de sistemas y la adopción de buenas prácticas que refuercen la resiliencia frente a amenazas.

e) ¿Cómo identificar las políticas de seguridad?

E1: Es necesario realizar un análisis exhaustivo de las normas ya establecidas, verificando su coherencia con los principios de la ISO/IEC 27009. Este proceso implica revisar la documentación vigente, evaluar su aplicabilidad en los distintos procesos institucionales y detectar posibles vacíos o inconsistencias.

E2: Requiere un análisis detallado de las normas internas vigentes en la organización. Este proceso implica revisar cómo dichas políticas regulan el acceso, la gestión y la protección de la información dentro de los sistemas tecnológicos. Además, se debe evaluar su nivel de cumplimiento frente a estándares internacionales y buenas prácticas de seguridad.

E3: Requiere evaluar si las normas internas vigentes cumplen con los requisitos establecidos por la ISO/IEC 27009. Este análisis implica revisar la documentación existente y contrastarla con los lineamientos de la norma para determinar su grado de conformidad. A partir de esta comparación, se pueden detectar brechas o áreas de mejora que demanden ajustes específicos.

E4: Implica reconocer posibles vacíos normativos dentro de la organización, revisando cuidadosamente las directrices existentes y su alcance real. Este análisis permite detectar áreas donde las políticas no ofrecen cobertura suficiente frente a riesgos o estándares internacionales. Una vez identificados dichos vacíos, se deben proponer ajustes o nuevas políticas que fortalezcan la gestión de la información.

E5: Puede realizarse proponiendo la creación de nuevas directrices que respondan a las necesidades actuales de la organización. Este enfoque permite cubrir áreas que no están contempladas en las normas vigentes y fortalecer la protección de la información crítica.

E6: Revisando de manera específica las políticas de control de accesos implementadas en la organización. Este análisis permite verificar si las normas actuales regulan adecuadamente la gestión de credenciales, permisos y niveles de autorización. Asimismo, se evalúa su efectividad frente a riesgos como accesos no autorizados o uso indebido de información crítica.

E7: Puede realizarse mediante el análisis de las políticas de respaldo de información que la organización tiene implementadas. Este proceso permite verificar si los mecanismos actuales garantizan la disponibilidad y recuperación de datos ante incidentes o fallas.

E8: Evaluando las políticas de uso de dispositivos tecnológicos dentro de la organización. Este análisis permite verificar si existen lineamientos claros sobre la utilización de equipos como computadoras, móviles y dispositivos externos, garantizando un manejo seguro de la información.

E9: Revisando los protocolos de respuesta ante incidentes establecidos en la organización. Este análisis permite evaluar si las medidas actuales garantizan una reacción rápida y efectiva frente a amenazas o vulnerabilidades.

E10: Documentando de manera sistemática todas las políticas institucionales relacionadas con la protección de la información. Este proceso asegura que las directrices existentes queden registradas de forma clara, accesible y actualizada para todos los miembros de la organización.

3. ¿Cómo implementar la norma ISO/IEC 27009 en la Municipalidad de Chorrillos?

Para implementar la norma ISO/IEC 27009 en la Municipalidad de Chorrillos es necesario concebir un plan integral que vaya más allá de la simple identificación de vulnerabilidades técnicas. En primer lugar, se debe realizar un diagnóstico exhaustivo de los sistemas municipales, evaluando tanto la infraestructura tecnológica como los procesos administrativos que gestionan información sensible de los ciudadanos. Este diagnóstico debe incluir pruebas de intrusión controladas en plataformas críticas —como sistemas de recaudación tributaria, bases de datos de vecinos y aplicaciones de atención ciudadana— con el fin de simular ataques manuales y automatizados que permitan medir la capacidad de resistencia de servidores, redes y dispositivos utilizados en la prestación de servicios públicos. Posteriormente, los hallazgos deben traducirse en un plan de acción que contemple medidas correctivas, políticas de seguridad, protocolos de respuesta ante incidentes y mecanismos de

monitoreo continuo. Es fundamental involucrar a las distintas áreas municipales en la construcción de una cultura de seguridad, capacitando al personal en buenas prácticas y asegurando que las decisiones tecnológicas estén alineadas con la normativa vigente. Asimismo, se recomienda establecer un comité de gestión de riesgos que supervise la implementación de controles, garantice la trazabilidad de las acciones y evalúe periódicamente la eficacia de las medidas adoptadas. Todo este proceso debe realizarse sin interrumpir las operaciones esenciales, como las plataformas de denuncias ciudadanas o los sistemas de alerta temprana, asegurando que la continuidad de los servicios esté protegida mientras se fortalece la resiliencia institucional frente a amenazas digitales.

4. ¿Qué riesgos existe al implementar la norma ISO/IEC 27009 en la Municipalidad de Chorrillos?

E1: Conlleva riesgos que deben gestionarse con precisión, ya que la estructura pública y la diversidad de procesos administrativos pueden generar vulnerabilidades específicas. Entre los principales riesgos se encuentran la resistencia al cambio cultural, la falta de capacitación del personal y la posible insuficiencia de recursos tecnológicos para cumplir con los controles exigidos. Asimismo, existe el peligro de accesos no autorizados debido a sistemas heredados o mal configurados, lo que podría derivar en delitos informáticos y pérdida de confianza ciudadana. Otro riesgo relevante es la dificultad para mantener la continuidad operativa durante la transición hacia un modelo más seguro, especialmente en áreas críticas como recaudación y gestión documental. Para mitigar estos desafíos, resulta indispensable contar con listas de verificación, planes de gestión de riesgos y protocolos claros de accesos denegados.

E2: Puede enfrentar como principal riesgo la resistencia al cambio por parte del personal, ya que la adopción de nuevas políticas de seguridad suele generar incertidumbre y rechazo inicial. Este obstáculo puede derivar en una baja adherencia a los procedimientos,

debilitando la efectividad del sistema de gestión de seguridad de la información. Además, la falta de compromiso y capacitación adecuada puede provocar errores en la aplicación de controles, exponiendo a la institución a vulnerabilidades críticas.

E3: La falta de conocimiento en seguridad de la información representa un riesgo significativo ya que limita la correcta aplicación de controles y procedimientos. Este desconocimiento puede generar errores en la gestión de accesos, en la protección de datos sensibles y en la respuesta ante incidentes, debilitando la confianza institucional. Además, la ausencia de capacitación adecuada incrementa la probabilidad de vulnerabilidades explotables por atacantes externos o internos.

E4: Puede verse afectada por limitaciones tecnológicas, ya que la infraestructura existente podría no estar preparada para cumplir con los requisitos de seguridad exigidos. Estas carencias incluyen sistemas obsoletos, falta de interoperabilidad entre plataformas y recursos insuficientes para garantizar la protección de datos sensibles.

E5: La falta de apoyo de la alta dirección constituye un riesgo crítico en la implementación de la norma ya que sin el respaldo de los líderes institucionales los proyectos de seguridad carecen de legitimidad y recursos suficientes. Esta ausencia de compromiso puede traducirse en una débil asignación presupuestal, escasa priorización de iniciativas y resistencia en los niveles operativos.

E6: La implementación de la norma puede verse comprometida por procesos institucionales poco documentados, lo que dificulta la trazabilidad y el control de las actividades relacionadas con la seguridad de la información. La ausencia de registros claros genera vacíos en la identificación de responsabilidades y en la aplicación de controles, aumentando la probabilidad de errores y vulnerabilidades.

E7: La falta de personal especializado en ciberseguridad representa un riesgo crítico para la implementación de la norma ya que limita la capacidad de diseñar, ejecutar y supervisar

controles efectivos de protección de la información. Esta carencia puede derivar en una gestión deficiente de incidentes, errores en la configuración de sistemas y una baja capacidad de respuesta frente a ataques informáticos.

E8: Enfrenta riesgos asociados a errores humanos, los cuales pueden manifestarse en configuraciones incorrectas, uso inadecuado de contraseñas o incumplimiento de procedimientos de seguridad. Estos fallos, muchas veces involuntarios, pueden abrir brechas que faciliten accesos no autorizados y comprometan la integridad de la información institucional.

E9: Puede verse amenazada por ataques cibernéticos durante el proceso de transición, ya que los sistemas suelen estar más vulnerables mientras se ajustan a nuevos controles y configuraciones. Estos ataques pueden aprovechar brechas temporales en la infraestructura tecnológica, comprometiendo datos sensibles y afectando la continuidad operativa.

E10: La falta de continuidad en los programas de seguridad constituye un riesgo importante para la implementación de la norma, ya que interrumpe el ciclo de mejora continua y debilita la eficacia de los controles establecidos. Cuando las iniciativas de seguridad se ejecutan de manera aislada o sin seguimiento, se generan brechas que pueden ser explotadas por atacantes y comprometer la información institucional.

a) ¿Cómo se realizaría un plan de riesgos?

E1: El plan de riesgos, también llamado plan de tratamiento de riesgos, se elabora a partir de los resultados de la evaluación de riesgos. Para cada riesgo identificado que supere el nivel de aceptación definido por la municipalidad, debemos decidir una opción de tratamiento: reducir (aplicar controles), retener (aceptar conscientemente), transferir (contratar un seguro o externalizar) o evitar (discontinuar la actividad).

E2: El plan debe detallar, para cada riesgo, las acciones concretas a realizar. Por ejemplo, si el riesgo es "acceso no autorizado a la base de datos tributaria por contraseñas débiles", la acción de tratamiento será "implementar una política de contraseñas seguras y autenticación de dos factores". Se asignará un responsable (ej. el jefe de TI), un plazo (ej. 3 meses) y los recursos necesarios (ej. compra de tokens de autenticación).

E3: El plan debe incluir también los controles que se implementarán, haciendo referencia al Anexo A de la ISO 27001 o a controles personalizados según la ISO 27009. Es importante justificar por qué se selecciona cada control y cómo contribuye a mitigar el riesgo específico. Esta justificación quedará reflejada en la Declaración de Aplicabilidad (SoA).

E4: El plan debe establecer prioridades. No todos los riesgos pueden tratarse al mismo tiempo. Priorizaremos aquellos con mayor nivel de riesgo (combinación de probabilidad e impacto) o aquellos que afectan a procesos críticos para la municipalidad. El plan debe reflejar un orden lógico de ejecución.

E5: El plan debe incluir un presupuesto estimado para cada acción. Esto es crucial para que la alta dirección pueda aprobar la asignación de recursos. El presupuesto debe considerar costos de software, hardware, consultoría, capacitación y horas de trabajo del personal.

E6: El plan debe definir los indicadores que permitirán hacer seguimiento a la ejecución de las acciones y a la efectividad de los controles. Por ejemplo, "número de usuarios con autenticación de dos factores implementada" o "reducción del porcentaje de contraseñas débiles detectadas en auditorías".

E7: El plan debe ser un documento vivo, que se revisará y actualizará periódicamente. A medida que se ejecutan las acciones, pueden surgir nuevos riesgos o cambios en el contexto que requieran ajustes. La gestión de riesgos es un proceso continuo, no un ejercicio de una sola vez.

E8: El plan debe ser comunicado a todas las áreas involucradas. Los responsables de cada acción deben conocer sus responsabilidades y los plazos. La comunicación asegura que no haya sorpresas y que todos remen en la misma dirección.

E9: El plan debe ser aprobado formalmente por la alta dirección, mediante una resolución o acuerdo de concejo. Esta aprobación le da el respaldo político necesario y lo convierte en un compromiso institucional, no solo del equipo de proyecto.

E10: Finalmente, el plan de riesgos se integrará al SGSI como un documento controlado. Se le asignará un código, una versión, y se establecerá su periodicidad de revisión (generalmente anual, o cuando ocurran cambios significativos). Su cumplimiento será auditado interna y externamente.

b) ¿En qué consiste la ejecución del plan de riesgos?

E1: La ejecución es la puesta en marcha de todas las acciones definidas en el plan. Es la fase más visible y operativa del proyecto. Se asignan los recursos aprobados, se adquieren las tecnologías necesarias, se redactan y aprueban las políticas, y se capacita al personal. Es un período de intensa actividad y cambio.

E2: Durante la ejecución, se implementan los controles técnicos. Esto implica la instalación y configuración de software de seguridad, la migración a sistemas más seguros, la segmentación de redes, la implementación de copias de seguridad automatizadas, etc. Cada implementación técnica debe seguir procedimientos de cambio controlados para no afectar la operación.

E3: Se implementan los controles organizativos y legales. Se publican las nuevas políticas, se actualizan los manuales de procedimientos, se modifican los contratos laborales para incluir cláusulas de confidencialidad, y se formalizan los acuerdos con proveedores exigiendo niveles de seguridad.

E4: Se ejecuta el plan de capacitación. Se llevan a cabo los talleres, las charlas y los cursos programados. Se entrega material de apoyo y se realizan evaluaciones para verificar la asimilación de los conocimientos. La formación no es un evento único, sino un proceso continuo durante toda la ejecución.

E5: Se establecen los mecanismos de monitoreo y reporte. Se configuran las herramientas de monitoreo, se definen los turnos de supervisión, y se ponen en marcha los procedimientos de respuesta a incidentes. La ejecución no termina hasta que estos mecanismos están operativos y el personal sabe cómo usarlos.

E6: Se documenta cada acción ejecutada. Se guardan las actas de reunión, los informes de configuración, las listas de asistencia a capacitaciones, las resoluciones de aprobación de políticas. Esta evidencia es fundamental para demostrar la conformidad en las auditorías.

E7: Se realiza un seguimiento cercano de la ejecución. El jefe de proyecto verifica que las acciones se estén completando según lo planificado, que no surjan desviaciones y que los recursos se estén utilizando adecuadamente. Cualquier problema se reporta al comité de dirección para tomar decisiones correctivas.

E8: Se gestionan los incidentes y problemas que puedan surgir durante la ejecución. Por ejemplo, si la implementación de un nuevo firewall causa problemas de conectividad, se debe activar el procedimiento de gestión de incidentes para resolverlo rápidamente y minimizar el impacto.

E9: Se comunican los avances a toda la organización. Se publican boletines informativos, se realizan reuniones de seguimiento con las áreas, se celebra cada hito alcanzado. Mantener informados a todos ayuda a mantener el compromiso y a reducir la resistencia al cambio.

E10: Al finalizar la ejecución de todas las acciones planificadas, se realiza una revisión para verificar que los riesgos han sido efectivamente tratados y que los controles operan según lo

esperado. Esta revisión puede incluir pruebas técnicas, encuestas al personal y auditorías internas. El resultado de esta revisión alimentará el siguiente ciclo de mejora.

c) ¿Cómo planificar los procesos de ejecución de la norma ISO/IEC 27009?

E1: La planificación de la ejecución comienza con la definición del alcance del SGSI. ¿Qué áreas, procesos y sistemas de la municipalidad estarán cubiertos por la certificación? Esta decisión estratégica debe tomarse en función de los objetivos del negocio, los requisitos legales y los riesgos identificados. Un alcance demasiado amplio puede ser inmanejable; demasiado reducido, puede no ser significativo.

E2: Se elabora un cronograma detallado del proyecto, utilizando herramientas como diagramas de Gantt. Se desglosa el trabajo en paquetes de actividades (WBS), se estima la duración de cada una, se identifican las dependencias entre ellas y se asignan fechas de inicio y fin. El cronograma debe ser realista y contar con márgenes para imprevistos.

E3: Se asignan responsables para cada actividad. No basta con decir "el área de TI hará esto". Hay que designar personas concretas, con nombres y apellidos, y asegurarse de que tienen disponibilidad y autoridad para llevar a cabo la tarea es una herramienta útil para esto.

E4: Se definen los hitos del proyecto. Los hitos son eventos significativos que marcan el avance, como "aprobación del diagnóstico", "finalización del plan de tratamiento de riesgos", "implementación del piloto", "aprobación de políticas". Los hitos ayudan a mantener el enfoque y a celebrar los logros.

E5: Se planifica la gestión de recursos. Esto incluye el presupuesto (ya aprobado), pero también los recursos humanos (¿se necesita contratar personal adicional o consultores?), los recursos tecnológicos (¿hay que comprar servidores o software?), y los recursos físicos (¿se necesita adecuar una sala para el centro de datos?).

E6: Se planifica la comunicación del proyecto. Se define qué información se comunicará, a quién, con qué frecuencia y a través de qué medios. Por ejemplo, informes semanales al comité de dirección, boletines mensuales a todo el personal, reuniones quincenales con los jefes de área.

E7: Se planifica la gestión de riesgos del propio proyecto. Identificaremos los riesgos que podrían afectar la ejecución del plan (como los mencionados en la pregunta 4) y definiremos acciones de contingencia para mitigarlos. Por ejemplo, si hay riesgo de rotación del personal clave, tendremos un plan de transferencia de conocimiento.

E8: Se planifica la gestión de la calidad. Definiremos los criterios de aceptación para cada entregable. Por ejemplo, una política estará "aprobada" cuando haya sido revisada por asesoría jurídica y firmada por el alcalde. Un control técnico estará "implementado" cuando pase una prueba de funcionamiento y seguridad.

E9: La planificación debe ser aprobada formalmente por el comité de dirección. Esta aprobación significa que la dirección se compromete a proporcionar los recursos necesarios y a apoyar la ejecución. El plan aprobado se convierte en la hoja de ruta oficial del proyecto.

E10: Finalmente, se establece un sistema de control de cambios del plan. Durante la ejecución, pueden surgir necesidades de ajustar fechas, recursos o actividades. Debe haber un procedimiento claro para proponer, evaluar y aprobar estos cambios, de manera que el plan se mantenga actualizado y realista

d) ¿Cómo se realizaría un plan de mejora?

E1: El plan de mejora nace de los resultados de la evaluación del desempeño del SGSI. Las principales fuentes de entrada son: los resultados de las auditorías internas, el análisis de incidentes y no conformidades, las revisiones por la dirección, los indicadores de desempeño (KPIs) y las sugerencias del personal.

E2: El plan debe basarse en el análisis de causa raíz. No basta con corregir un problema puntual; hay que entender por qué ocurrió para evitar que se repita. Por ejemplo, si se detectó que varios usuarios no cambiaron sus contraseñas, la causa raíz podría ser que la política no está automatizada o que la formación fue insuficiente.

E3: El plan de mejora incluye acciones correctivas (para eliminar las causas de no conformidades detectadas) y acciones preventivas (para eliminar las causas de posibles no conformidades futuras, basadas en el análisis de riesgos). También puede incluir acciones de mejora continua, que son iniciativas proactivas para optimizar el sistema, aunque no haya habido un problema previo.

E4: El plan debe priorizar las acciones de mejora en función de su impacto y urgencia. No se puede abordar todo a la vez. Las acciones que corrigen no conformidades graves o que previenen riesgos críticos tendrán prioridad sobre aquellas que son meramente cosméticas.

E5: Para cada acción de mejora, el plan debe definir: la descripción de la acción, el responsable de ejecutarla, los recursos necesarios, el plazo de ejecución y los indicadores que permitirán verificar su eficacia una vez implementada.

E6: El plan debe ser realista y factible. Debe considerar la capacidad operativa de la municipalidad. No tendría sentido proponer 50 acciones de mejora si solo hay personal para ejecutar 10 en el próximo año. La mejora es continua, no un estallido de actividad.

E7: El plan debe ser comunicado a las áreas involucradas. Los responsables de cada acción deben conocer su cometido y los plazos. La comunicación también ayuda a generar compromiso y a evitar malentendidos.

E8: Se debe hacer seguimiento a la ejecución del plan de mejora con la misma rigurosidad que al plan de riesgos. Reuniones periódicas de revisión, informes de avance, y actualización del estado de cada acción (pendiente, en progreso, completada, verificada).

E9: Una vez implementadas las acciones, se debe verificar su eficacia. ¿Realmente se resolvió el problema? ¿El indicador mejoró? ¿La no conformidad no ha vuelto a aparecer? Esta verificación es esencial para cerrar el ciclo de mejora y para demostrar que las acciones no fueron solo un parche.

E10: Finalmente, los resultados del plan de mejora deben ser presentados en la revisión por la dirección. La alta dirección evaluará si el sistema está mejorando conforme a lo esperado y tomará decisiones estratégicas para el siguiente período. Este ciclo de revisión y mejora es lo que garantiza la evolución y la sostenibilidad del SGSI en el tiempo.

5. ¿Qué documentos y formatos se usan para implementar la norma ISO/IEC 27009?

E1: La documentación del SGSI se estructura en varios niveles. En el nivel estratégico, el documento más importante es el **Manual del SGSI**, que describe el sistema, su alcance, la política de seguridad y los objetivos. Es la carta de presentación del sistema y debe ser aprobado por la alta dirección.

E2: En el nivel táctico, se encuentran los **procedimientos documentados obligatorios** que exige la ISO 27001: control de documentos, control de registros, auditorías internas, gestión de no conformidades y acciones correctivas, y gestión de incidentes. Además, se elaboran procedimientos específicos para cada área de control (gestión de activos, control de accesos, etc.).

E3: En el nivel operativo, tenemos los **planes y las instrucciones técnicas**. Por ejemplo, el Plan de Tratamiento de Riesgos, el Plan de Continuidad del Negocio, las instrucciones de configuración segura de servidores, o los guiones para la respuesta a incidentes.

E4: En el nivel de evidencia, se encuentran los **registros**. Son documentos que demuestran que las actividades se han realizado conforme a lo planificado. Ejemplos: actas de reunión del comité de seguridad, informes de auditoría, reportes de incidentes, listas de asistencia a capacitaciones, resultados de evaluaciones de riesgos.

E5: Un documento transversal crítico es la **Declaración de Aplicabilidad (SoA)**. Este documento lista todos los controles del Anexo A (y otros adicionales) y justifica, para cada uno, si se aplica o no en la municipalidad y por qué. El SoA es la columna vertebral de la implementación y es exhaustivamente revisado en las auditorías.

E6: También son necesarios los **inventarios**: Inventario de Activos de Información, Inventario de Software, Inventario de Hardware. Estos inventarios deben estar vivos y actualizarse constantemente.

E7: Se requieren **políticas de alto nivel** aprobadas por la dirección, como la Política de Seguridad de la Información, la Política de Uso Aceptable, la Política de Control de Accesos, y la Política de Copias de Seguridad. Cada política define los principios y responsabilidades generales en su ámbito.

E8: Para la gestión de riesgos, se utilizan documentos como la **Metodología de Gestión de Riesgos** (que describe el proceso a seguir) y el **Registro de Riesgos** (donde se listan y evalúan los riesgos identificados).

E9: Para la continuidad del negocio, se elaboran el **Análisis de Impacto en el Negocio (BIA)**, la **Estrategia de Continuidad** y los **Planes de Continuidad** específicos para cada proceso crítico.

E10: Para asegurar el cumplimiento normativo, se elabora la Matriz de Requisitos Legales y Regulatorios. Este documento identifica y centraliza todas las leyes aplicables (como la Ley de Protección de Datos Personales y normativas del sector público) y las obligaciones

contractuales, mapeando cada exigencia con los controles específicos del SGSI diseñados para satisfacerla.

a) ¿Qué formatos son los necesarios a diseñar para implementar la Norma ISO/IEC 27009?

E1: Es necesario diseñar un **Formato de Control de Documentos**, que es una plantilla para solicitar la creación, modificación o eliminación de un documento, con espacios para justificar el cambio y para las firmas de revisión y aprobación.

E2: Un **Formato de Inventario de Activos** es esencial. Debe incluir campos como: código del activo, nombre, descripción, propietario, ubicación, clasificación de la información (público, interno, confidencial, secreto), soporte (físico o digital), y valoración.

E3: Se necesita un **Formato de Evaluación de Riesgos**, con secciones para describir el riesgo, identificar activos, amenazas y vulnerabilidades, valorar la probabilidad e impacto, calcular el nivel de riesgo, y proponer opciones de tratamiento.

E4: Un **Formato de Declaración de Aplicabilidad (SoA)**, que liste todos los controles del Anexo A y permita marcar si son aplicables o no, con una columna para la justificación y otra para referenciar el documento donde se implementa el control.

E5: Un **Formato de Reporte de Incidentes de Seguridad**, que cualquier funcionario pueda llenar de manera sencilla. Debe incluir fecha y hora del incidente, descripción, persona que reporta, sistemas afectados, y acciones inmediatas tomadas.

E6: Un **Formato de Auditoría Interna**, que sirva como lista de verificación (checklist) para los auditores, con los requisitos a verificar, espacio para hallazgos, y para clasificar las no conformidades (mayores, menores, oportunidades de mejora).

E7: Un **Formato de Acciones Correctivas y Preventivas**, que permita documentar cada acción, su causa raíz, las actividades planeadas, el responsable, el plazo, y el seguimiento de su implementación y verificación de eficacia.

E8: Un **Formato de Control de Asistencia** para las capacitaciones y reuniones, que incluya tema, fecha, instructor, lista de participantes con firma, y evaluación de la actividad (si aplica).

E9: Un **Formato de Revisión por la Dirección**, que sirva de guía para la reunión anual de la alta dirección, con puntos a tratar como el estado de las acciones de períodos anteriores, cambios en el contexto, resultados de auditorías, y decisiones para la mejora.

E10: Finalmente, un **Formato de Acta de Reunión** estandarizado, que facilite la documentación de las decisiones tomadas en el comité de seguridad o en el equipo de proyecto, con campos para acuerdos, responsables y plazos.

b) ¿Cómo ejecutar la estandarización de la norma ISO/IEC 27009?

E1: La estandarización se logra cuando los procedimientos documentados se convierten en la forma habitual de trabajar. Para ello, es crucial que los documentos sean prácticos, estén redactados en un lenguaje claro y accesible, y sean conocidos por todos los que deben aplicarlos.

E2: La estandarización requiere formación. No basta con publicar los procedimientos; hay que enseñar a las personas cómo usarlos. Se deben realizar sesiones de capacitación práctica, donde los funcionarios practiquen la aplicación de los nuevos formatos y procedimientos en casos simulados.

E3: La estandarización se refuerza mediante la supervisión y el acompañamiento. En las primeras semanas de implementación, los responsables de cada proceso deben recibir apoyo cercano para resolver dudas y corregir desviaciones. Los jefes deben velar por el cumplimiento.

E4: La estandarización se evidencia en los registros. Cuando todos los reportes de incidentes se llenan en el mismo formato, con la misma calidad de información, y se archivan en el lugar designado, eso es señal de que el proceso se ha estandarizado.

E5: La estandarización se mantiene mediante auditorías internas. Los auditores verificarán si los procedimientos se están siguiendo en la práctica. Los hallazgos de auditoría señalarán las desviaciones que deben corregirse para volver al estándar.

E6: La estandarización implica también la gestión de cambios. Cuando sea necesario modificar un procedimiento estandarizado, el cambio debe hacerse siguiendo el procedimiento de control de documentos, y la nueva versión debe ser comunicada y desplegada de manera controlada.

E7: La estandarización se facilita con herramientas tecnológicas. Por ejemplo, un sistema de gestión documental que automatice los flujos de aprobación y asegure que todos accedan a la última versión de los documentos ayuda a mantener la estandarización.

E8: La estandarización debe ser auditada por la alta dirección. En las revisiones periódicas, la dirección debe preguntar: ¿se están siguiendo los procedimientos? ¿Hay desviaciones recurrentes? ¿Necesitamos ajustar el estándar porque no es práctico?

E9: La estandarización no es rigidez. Un proceso estandarizado debe ser también mejorable. Si se detecta que un procedimiento está causando cuellos de botella o no es efectivo, debe ser revisado y mejorado, y la nueva versión se convierte en el nuevo estándar.

E10: Finalmente, la estandarización se consolida cuando se integra en la cultura organizacional. Cuando un nuevo empleado llega a la municipalidad, aprende los procedimientos estandarizados como parte de su inducción, y cuando los funcionarios con más años los aplican de manera natural, podemos decir que la estandarización ha sido exitosa.

c) ¿Qué métodos de información son los más comunes usando la Norma ISO/IEC 27009?

E1: El método más formal es la **intranet o portal del empleado**, donde se publican todas las políticas, procedimientos y formatos del SGSI. Debe ser de fácil acceso y estar actualizado. Es el repositorio oficial de la documentación.

E2: El **correo electrónico institucional** es un método masivo y efectivo para comunicaciones rápidas: anuncios de nuevas políticas, recordatorios de buenas prácticas, alertas de seguridad, convocatorias a capacitaciones. Sin embargo, debe usarse con mesura para no saturar las bandejas de entrada.

E3: Las **reuniones periódicas** del comité de seguridad y las reuniones de área son fundamentales para la comunicación bidireccional. Permiten discutir problemas, aclarar dudas y tomar decisiones colegiadas. Las actas de estas reuniones son registros valiosos.

E4: Los **carteles y afiches** en lugares visibles (comedor, salas de espera, oficinas) son un método de concienciación pasiva pero efectivo. Mensajes como "Protege tu contraseña" o "¿Has visto algo sospechoso? Repórtalo" mantienen el tema presente en la mente de los funcionarios.

E5: Los **boletines electrónicos o newsletters** periódicos (mensuales o trimestrales) pueden resumir los avances del SGSI, compartir estadísticas de incidentes, destacar buenas prácticas y reconocer a los empleados que han contribuido a la seguridad.

E6: Los **tableros de control o dashboards** son un método de información para la alta dirección. Muestran de manera visual y resumida los indicadores clave (KPIs) del SGSI: número de incidentes, tiempo de respuesta, avance del plan de riesgos, etc.

E7: Las **campañas de concienciación** temáticas, como el "mes de la ciberseguridad", con actividades lúdicas, concursos, charlas de expertos invitados, son métodos que generan engagement y refuerzan la cultura de seguridad.

E8: Los **cursos de formación presenciales o virtuales** son el método más estructurado para transmitir conocimientos. Pueden ser obligatorios para ciertos roles y deben incluir evaluaciones para verificar el aprendizaje.

E9: El **buzón de sugerencias** y el **correo de contacto institucional** (seguridad@munichorrillos.gob.pe) se consolidan como canales oficiales de comunicación ascendente dentro de la organización. Estas herramientas estratégicas están diseñadas con el propósito de ofrecer a todos los empleados un espacio seguro y accesible para reportar problemas operativos, formular preguntas complejas o proponer mejoras innovadoras. Al garantizar un entorno de absoluta confidencialidad, se fomenta una cultura de transparencia, confianza y participación activa, permitiendo que la voz de cada colaborador contribuya directamente al fortalecimiento de los procesos internos y al bienestar colectivo.

E10: Finalmente, los **informes de gestión** que se presentan periódicamente a la alta dirección son un método de información consolidada que permite la toma de decisiones estratégicas. Estos informes deben ser claros, concisos y basados en datos objetivos.

6. ¿Cuáles son las estrategias del seguimiento y control?

E1: La estrategia principal es el ciclo **PHVA (Planificar-Hacer-Verificar-Actuar)** aplicado al sistema. El seguimiento y control corresponden a la fase "Verificar". Consiste en medir el desempeño del SGSI, compararlo con los objetivos planeados y detectar desviaciones para corregirlas.

E2: El seguimiento y control se basa en la **medición continua**. Esto incluye el monitoreo técnico en tiempo real (logs, intrusiones, disponibilidad), la revisión periódica de indicadores de gestión, y la realización de auditorías programadas.

E3: Una estrategia clave es la **gestión de incidentes**. Registrar, analizar y resolver incidentes de seguridad es una forma de controlar que los riesgos no se materialicen o de minimizar su impacto. El análisis de tendencias de incidentes también alimenta la mejora.

E4: Las **auditorías internas** son el corazón del seguimiento. Se programan con una frecuencia determinada (al menos anual) y cubren todos los requisitos de la norma y todos los procesos del SGSI. Los auditores internos deben ser independientes y competentes.

E5: La **revisión por la dirección** es el punto culminante del ciclo de control. Una o dos veces al año, la alta dirección analiza el desempeño global del sistema, revisa los resultados de las auditorías, evalúa el cumplimiento de objetivos y toma decisiones estratégicas para el siguiente período.

E6: El control también se ejerce a través de la **gestión de no conformidades**. Cada vez que se detecta un incumplimiento de los requisitos (ya sea en una auditoría, en una queja o en una revisión diaria), se abre una no conformidad y se inicia el proceso de acciones correctivas para eliminar su causa.

E7: Otra estrategia es el **seguimiento del plan de tratamiento de riesgos**. Verificar periódicamente que las acciones planificadas se están ejecutando y que los riesgos se están reduciendo según lo esperado. Si no es así, hay que reajustar el plan.

E8: El control también implica la **revisión de la documentación**. Verificar que los documentos sigan siendo adecuados, que las versiones estén controladas y que los registros se estén generando y archivando correctamente.

E9: Los **indicadores de desempeño (KPIs)** son herramientas fundamentales. Deben estar definidos, medirse periódicamente y analizarse. Por ejemplo: tiempo medio de respuesta a incidentes, porcentaje de sistemas con parches actualizados, índice de satisfacción de usuarios internos con la seguridad.

E10: Finalmente, el seguimiento y control incluye la **retroalimentación de las partes interesadas**. Escuchar a los empleados, a los ciudadanos (a través de quejas o sugerencias) y a los proveedores puede proporcionar información valiosa sobre el funcionamiento real del sistema que no siempre captan los indicadores formales.

a) ¿Qué tipo de auditorías hay que hacer?

E1: El primer tipo son las **auditorías internas de primera parte**. Las realiza la propia organización (o un externo contratado para ello) pero con personal que no tenga responsabilidad directa en las áreas auditadas. Su objetivo es verificar la conformidad y prepararse para la auditoría externa.

E2: Las **auditorías externas de certificación** son realizadas por una entidad de certificación acreditada. Estas auditorías tienen dos fases: la Fase 1 (revisión de la documentación y del diseño del sistema) y la Fase 2 (verificación in situ de la implementación y eficacia). Si son exitosas, otorgan el certificado.

E3: Después de la certificación, se realizan **auditorías de seguimiento** anuales (o semestrales) por parte de la entidad certificadora para verificar que el sistema se mantiene y mejora. Cada tres años se realiza una auditoría de recertificación.

E4: También pueden realizarse **auditorías específicas o de alcance reducido** para verificar un área particular o un proceso nuevo que se haya incorporado al SGSI, sin necesidad de auditar todo el sistema.

E5: Las **auditorías de cumplimiento legal** son recomendables para verificar que la municipalidad cumple con todas las leyes y regulaciones aplicables en materia de protección de datos, transparencia, etc. Pueden ser parte de las auditorías internas o realizarse por separado.

E6: Las **auditorías de proveedores** pueden ser necesarias si la municipalidad ha externalizado servicios críticos. Se audita a los proveedores para verificar que cumplen con los requisitos de seguridad contractuales.

E7: Las **auditorías técnicas** o pruebas de penetración (pentesting) son un tipo especial de auditoría que busca vulnerabilidades técnicas en los sistemas mediante ataques simulados. No son obligatorias por la norma, pero son altamente recomendables.

E8: Las **auto-evaluaciones** o revisiones por pares pueden ser una herramienta de control menos formal pero muy útil entre áreas de la municipalidad, fomentando la colaboración y el aprendizaje mutuo.

E9: Es importante planificar un **programa anual de auditorías** que defina qué auditorías se realizarán, con qué alcance, en qué fechas y con qué recursos. Este programa debe ser flexible para adaptarse a cambios imprevistos.

E10: Finalmente, todas las auditorías deben seguir un procedimiento estandarizado: planificación, preparación de listas de verificación, ejecución (reunión de apertura, recolección de evidencias, entrevistas), elaboración del informe de hallazgos, reunión de cierre, y seguimiento de las acciones correctivas derivadas.

b) ¿Cómo se determinan las acciones correctivas?

E1: Las acciones correctivas se determinan a partir de la identificación de una **no conformidad**. Una no conformidad es el incumplimiento de un requisito (de la norma, legal o propio). Puede detectarse en una auditoría, en una revisión diaria, o a través de una queja o incidente.

E2: El primer paso es **describir la no conformidad** de manera clara y objetiva, indicando dónde, cuándo y cómo se detectó. Esta descripción se registra en el Formato de Acciones Correctivas y Preventivas.

E3: El paso crítico es el **análisis de la causa raíz**. No basta con solucionar el síntoma. Hay que preguntarse "¿por qué?" repetidamente (técnica de los 5 porqués) hasta llegar a la causa fundamental del problema. Por ejemplo, si no se realizó una copia de seguridad, la causa raíz podría ser que el procedimiento no asignaba un responsable claro.

E4: Una vez identificada la causa raíz, se **definen las acciones** necesarias para eliminarla. Estas acciones deben ser específicas, medibles, asignadas a un responsable y con un plazo. Por ejemplo: "modificar el procedimiento de copias de seguridad para asignar la responsabilidad al administrador del sistema de turno, y comunicar el cambio mediante una reunión el día X".

E5: Las acciones propuestas deben ser **evaluadas por el responsable del proceso** afectado y aprobadas por la dirección del SGSI (por ejemplo, el oficial de seguridad o el comité). Se verifica que sean factibles y que no generen efectos secundarios no deseados.

E6: Se **implementan las acciones** según lo planificado. Durante la implementación, se debe dar seguimiento para asegurar que se avanza y que no surgen impedimentos. Cualquier desviación debe ser gestionada.

E7: Una vez implementadas, se debe **verificar la eficacia** de las acciones. ¿Realmente se eliminó la causa raíz? ¿La no conformidad ha dejado de ocurrir? Esta verificación puede incluir una nueva auditoría, una revisión documental o una prueba práctica. Si la acción no fue eficaz, debe reiniciarse el ciclo.

E8: Todo el proceso debe quedar **documentado** en el mismo formato: desde la detección de la no conformidad hasta la verificación de la eficacia. Esta documentación es evidencia para futuras auditorías.

E9: Las acciones correctivas exitosas pueden dar lugar a **cambios en el SGSI**. Por ejemplo, si la causa raíz era un procedimiento deficiente, la acción correctiva implicará su actualización. La nueva versión del procedimiento se integrará al sistema.

E10: Finalmente, se debe **analizar la tendencia** de las acciones correctivas. Si un mismo tipo de no conformidad aparece repetidamente, puede indicar un problema sistémico más profundo que requiere una acción preventiva o un rediseño del proceso.

c) ¿Cómo se determinan las acciones preventivas?

E1: Las acciones preventivas se determinan a partir del **análisis proactivo de riesgos**. Mientras que las acciones correctivas reaccionan ante problemas ocurridos, las preventivas anticipan problemas potenciales. La principal fuente de acciones preventivas es el proceso de gestión de riesgos.

E2: Cuando en la evaluación de riesgos identificamos un riesgo con una probabilidad de ocurrencia significativa, aunque aún no se haya materializado, podemos definir **acciones para reducir esa probabilidad** o para mitigar su impacto potencial. Esas son acciones preventivas.

E3: Otra fuente son las **tendencias detectadas en los indicadores**. Si observamos que el número de intentos de acceso no autorizado a un sistema está aumentando lentamente, aunque aún no haya habido un acceso exitoso, podemos implementar una acción preventiva (como reforzar la autenticación) antes de que ocurra un incidente.

E4: Las **lecciones aprendidas de otras organizaciones** también pueden motivar acciones preventivas. Si otra municipalidad ha sufrido un tipo de ataque, podemos analizar si somos vulnerables al mismo y tomar medidas para prevenirlo.

E5: Si otra municipalidad ha sufrido un tipo de ataque, podemos analizar si somos vulnerables al mismo y tomar medidas para prevenirlo. Por ejemplo, si en una municipalidad vecina se presentó un caso de ransomware que paralizó sus sistemas, en Chorrillos podemos implementar copias de seguridad offline y capacitación específica sobre ese tipo de amenaza antes de que ocurra un incidente similar.

E6: Las **sugerencias y recomendaciones del personal** también son una fuente valiosa de acciones preventivas. Los funcionarios que están en la operación diaria suelen identificar potenciales problemas antes de que se materialicen. Establecer un canal para que puedan reportar estas "casi fallas" o ideas de mejora es fundamental.

E7: Los **cambios en el contexto** (nuevas leyes, nuevas tecnologías, cambios en la estructura organizativa) pueden generar nuevos riesgos. Ante un cambio planificado, como la implementación de un nuevo sistema de trámite en línea, debemos realizar un análisis de riesgos previo y definir acciones preventivas para asegurar que el nuevo sistema sea seguro desde su diseño.

E8: Al igual que en las acciones correctivas, las preventivas deben ser **documentadas en el mismo formato**, incluyendo: la identificación del riesgo potencial, el análisis de su causa (¿por qué podría ocurrir?), la acción propuesta para prevenirlo, el responsable, el plazo, y luego el seguimiento y la verificación de su eficacia.

E9: Es importante que las acciones preventivas no se conviertan en una "cacería de fantasmas". Deben estar justificadas por un análisis razonable de probabilidad e impacto. No se puede pretender prevenir todos los riesgos imaginables; hay que priorizar aquellos con mayor potencial de daño

E10: Las acciones preventivas se determinan a partir del análisis proactivo de los riesgos y las vulnerabilidades. Se basan en la identificación de posibles amenazas antes de que ocurran incidentes.