UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Aplicación de la norma internacional ISO 27035:2016 para la gestión de incidentes de seguridad de la información en la Empresa LISERME S.R.L., Arequipa 2022 .

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniero de Sistemas

AUTOR:

Limache Ynquilla, Anuar Mauro (ORCID: 0000-0002-9184-2099)

ASESOR:

Dr. Agreda Gamboa, Everson David (ORCID: 0000-0003-1252-9692)

LÍNEA DE INVESTIGACIÓN:

Sistemas de Información y Comunicaciones

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA - PERÚ

2022

Dedicatoria

A la memoria de mi padre, que, hasta sus últimos momentos, no dejo de preocuparse por los demás, el hombre más noble, amable e increíble que he podido conocer, un excelente padre, No hay un día que pase que no me acuerde de ti, Te amo, papá.

A mi madre y hermano, quienes, durante los últimos meses, me han alentado atentamente con su atención más plena y verdadera, a pesar de mi mal carácter, siempre tratando de acercarse y apoyarme para realizar mi trabajo con sinceridad y autoconfianza.

A personas amadas que partieron hace poco, en especial a mis abuelas que me criaron y quienes fueron las personas más fuertes que he conocido, cuyo amor por mí no conoció límites y quienes me enseñaron el valor del trabajo duro.

Agradecimiento

Aquellos a quienes están ahí en los peores momentos con su tiempo, aliento y apoyo constante y se mantuvieron ahí. Gracias por todo.

A la pequeñita que apareció en mi vida sin haberlo planeado, que se sienta a mi lado día con día, a pesar de que en este último tiempo continuamente se presenten situaciones que conducen al miedo, odio y a la desesperación, pero está ahí para hacerme entender que siempre tiene que predominar la esperanza, bondad y la paz. Gracias por todo.

Índice de contenidos

Pág.

Índice de tablas

Pág.

Índice de figuras

Pág.

Resumen

Esta investigación titulada, aplicación de la Norma internacional ISO 27035:2016 para la Gestión de incidentes de seguridad de la información en la Empresa LISERME S.R.L., Arequipa 2022, plantea como problema principal: ¿De qué manera la aplicación de la norma internacional ISO 27035:2016 influye en la gestión de incidentes de seguridad de la información en la empresa LISERME S.R.L., Arequipa 2022?, tiene como objetivo mejorar la gestión de incidentes de seguridad de la información en la empresa LISERME S.R.L. de la ciudad de Arequipa mediante la aplicación de la Norma internacional ISO 27035:2016 en el año 2022, plantea como hipótesis que: La Aplicación de la Norma internacional ISO 27035:2016 en el año 2022 mejorará significativamente la gestión de incidentes de seguridad de la información en la empresa LISERME S.R.L., Arequipa 2022. El tipo de investigación es aplicada y el nivel de investigación es una investigación pre experimental. También, se utilizaron como indicadores; Tiempo Promedio de respuesta de Incidentes atendidos, porcentaje de respuesta de incidentes atendidos, porcentaje de reincidencia de incidentes, nivel de satisfacción del personal. Se obtuvieron las muestras, las cuales fueron evaluadas en un periodo establecido. El desarrollo de la solución fue bajo la norma ISO 25035:2016. Como conclusiones se puede decir que, para el primer indicador, tiempo de promedio de respuesta de incidente atendidos, tuvo un descenso de 44.25 minutos a 13.91 minutos, para el segundo indicador, porcentaje de respuesta de incidentes se incrementó a 94.82%, para el tercer indicador, porcentaje de reincidencia de incidentes tuvo un descenso de 20.43% a 4.65%, para el cuarto indicador, nivel de satisfacción del personal de TI se incrementó a 86.67%, lo cual ha permitido validar y resulta favorable la aplicación de la norma internacional ISO 27035:2016 satisfactoriamente.

Palabras clave: Gestión de incidentes, Norma, Seguridad de la Información.

Abstract

This research entitled, application of the international standard ISO 27035:2016 for the management of information security incidents in the company LISERME S.R.L., Arequipa 2022, poses as main problem: How the application of the international standard ISO 27035:2016 influences the management of information security incidents in the company LISERME S.R.L., Arequipa 2022, aims to improve the management of information security incidents in the company LISERME S.R.L. in the city of Arequipa through the application of the international standard ISO 27035:2016 in the year 2022, hypothesizes that: The Application of the International Standard ISO 27035:2016 in the year 2022 will significantly improve the management of information security incidents in the company LISERME S.R.L., Arequipa 2022. The type of research is applied and the level of research is pre-experimental research. Also, were used as indicators; Average response time of incidents attended, percentage of response of incidents attended, percentage of recurrence of incidents, level of staff satisfaction. Samples were obtained, which were evaluated in an established period. The development of the solution was under the ISO 25035:2016 standard. As conclusions it can be said that, for the first indicator, average response time of incident attended, had a decrease from 44.25 minutes to 13.91 minutes, for the second indicator, percentage of incident response increased to 94.82%, for the third indicator, percentage of incident recurrence had a decrease from 20.43% to 4.65%, for the fourth indicator, level of IT staff satisfaction increased to 86.67%, which has allowed validating and is favorable the application of the international standard ISO 27035:2016 satisfactorily.

Keywords: Incident management, Standard, Information Security.

I. INTRODUCCIÓN

La economía mundial se encuentra en medio de una rápida transformación, como la Internet, economía digital, tecnología móvil y tendencias de gestión de la información a gran escala que han provocado una ola de innovación y está ocasiona que se afecten no solo las empresas especializadas en tecnología. Hoy en día, somos testigos de grandes tendencias tecnológicas que están transformando la sociedad, los pequeños negocios y la economía. Las empresas ya sean grandes, mediana y pequeñas ahora se ven afectadas en gran medida, si no totalmente, por la aparición de tendencias de tecnología de la información, como la nube, las redes sociales.

La mayoría de las empresas confían demasiado en los sistemas, desde el correo electrónico de los empleados, gestión de redes, base de datos, gestión empresarial, CRM, ERP, hasta sistemas de inteligencia de negocios. Incluso las pequeñas empresas no especializadas en tecnología necesitan un sistema, estándares, políticas y buenas prácticas que ayuden en sus diferentes tareas de manera eficaz, ocasionando una serie de inconvenientes tecnológicos que al no contar con una buena gestión de incidentes se viene solucionando empíricamente o dando una solución temporal esto hace que tarde o temprano sea incontrolable.

A nivel internacional, (WeLiveSecurity, 2021 pág. 6), en su reporte, *"ESET Security Report 2021"*, sostiene que, Según el estudio realizado para la ESR 2021, las principales preocupaciones de seguridad de las empresas en Latinoamérica son los códigos maliciosos 64%, seguidos del robo de información 60% y el acceso no autorizado a los sistemas 56%.

(Sundaram, 2022), el artículo, *"Siete tendencias tecnológicas que impulsarán los negocios en 2022"*, sostiene que, Hay un cambio posterior a lo ocurrido, con la pandemia ocasionando que se acelere la economía y la rápida transformación a lo digital, además del seguimiento, se requiere de la confianza de los clientes que valoran las marcas que pueden garantizar, entre otras cosas, la seguridad de su información, privacidad y datos personales que las personas encontrarán para El acceso de pago a estos beneficios se está convirtiendo en una de las grandes tendencia tecnológicas.

A nivel nacional, (INEI, 2018), en su libro, *"Perú: Tecnologías de Información y Comunicación en las Empresas"*, sostiene que, los resultados recolectados de la encuesta económica elaborada anualmente, examina a las grandes, medianas y pequeñas empresas que realizaron actividades económicas en 2019. Durante este período se registraron 100.627 empresas, de las cuales 94.1% de empresas utilizaron telefonía móvil, 93.8% empresas utilizaron ordenadores, 92.2% utilizan el Internet, 84.6% teléfonos fijos, 17.4% usan intranet, 15.1% PDA y 7,.4% extranet.

A nivel nacional, (INDECOPI, 2013), en su norma, "*NORMA TÉCNICA PERUANA NTP-ISO/IEC 27035:2013",* sostiene que, las empresas que cuentan con seguridad de datos a pesar de contar con políticas y buenas prácticas, no quiere decir que se garantice que la seguridad esté completamente sin vulnerabilidades, esto puede ocasionar que la seguridad sea ineficaz y pueda llevar a que existan o se generen eventos de seguridad, la preparación insuficiente en las empresas puede ocasionar ante dichos eventos de seguridad de la información sea menos eficaz, además que el nivel de impacto sea mayor tanto directo como indirectos en las operaciones de las empresas.

En este contexto, una empresa especializada en fabricación de productos metálicos en la ciudad de Arequipa, la cual es una pequeña empresa, poniendo a disposición su instrucción, experiencia, cualidades y recursos para atender las demandas del mercado en el sector industrial a nivel nacional.

Las empresas que fabrican productos metálicos para uso estructural se están expandiendo constantemente en los últimos años, mejorando continuamente; aun así, se presentan algunas deficiencias en sus procesos como es la situación con las brechas de seguridad de datos en sus diferentes servicios que ofrece, ya que algunos están localizados en distintos puntos.

Los empleados no cuentan con una capacitación adecuada para los incidentes de seguridad que se presentan, con las constantes actualizaciones tecnológicas, los niveles de competencia entre empresas son cada vez mayores, eso significa que es aún más importante que sus empleados estén

capacitados con el conocimiento y las habilidades que necesitan para trabajar de manera segura y eficiente. El aprendizaje constante para estar preparados y seguir el ritmo de la transformación digital que estamos viviendo es necesario para el éxito.

Ignorar la importancia de la gestión eficaz de incidentes, reducir el impacto si ocurren y fortalecer sus defensas contra amenazas futuras. Puede afectar seriamente la capacidad y la calidad del servicio de una organización para atraer y retener buenos clientes.

La creciente complejidad y la prevalencia de las amenazas finalmente han llamado la atención de no solo las empresas que cuentan con mayor presupuesto. Los incidentes de seguridad son inevitables, prepárese para ello es lo más acertado, con un programa adecuado de respuesta a incidentes.

Las oportunidades de desarrollo sostenible a través de la gestión eficaz de los incidentes de seguridad, son una buena y muy atractiva oportunidad para brindar buenos resultados tanto a la empresa como a sus empleados, Al asumir la responsabilidad de capacitar e invertir en sus empleados, atrae clientes potenciales al contar con estándares, políticas y mejores prácticas internacionales y reducir el tiempo de respuesta si se detecta incidente de seguridad, la mala respuesta a incidentes afecta negativamente las prácticas comerciales, incluido el flujo de trabajo, la generación de ingresos y la imagen pública.

Para mantener y optimizar de manera efectiva los servicios que ofrece la empresa, es necesario asegurar la operación de componentes funcionales como procesos, estándares, información, recursos humanos y aumentar la producción, así como crear ventajas competitivas y reducir la inactividad.

Este trabajo de investigación aborda el siguiente problema:

¿De qué manera la aplicación de la Norma ISO 27035:2016 influye en la gestión de incidentes de seguridad de la información en la empresa LISERME S.R.L., Arequipa 2022?

*Justificación***:** Para la empresa LISERME, esto mejorará las capacidades del departamento de tecnología de la información guiará para desarrollar un programa de respuestas adecuado, escalable y mejorará el flujo de trabajo y se podrá administrar la operación en caso de incidentes para reducir cualquier impacto adverso garantizando el cumplimiento de los requisitos de gestión de incidentes ISO 27035:2016, permitirá una buena gestión de los incidentes de seguridad, la optimización de los recursos existentes y la implementación de nuevos recursos en la empresa para lograr la mejora continua.

Objetivo general: Para el desarrollo de la investigación es, mejorar la gestión de incidentes de seguridad de la información en la empresa LISERME S.R.L. de la ciudad de Arequipa a través de la aplicación de la Norma internacional ISO 27035:2016 en el año 2022.

Objetivos específicos: Para el desarrollo de la investigación, mediante la aplicación de la Norma ISO 27035:2016, se reducirá el tiempo promedio de respuesta de incidentes atendidos en la empresa LISERME; mediante la aplicación de la Norma ISO 27035:2016, se incrementará el porcentaje de respuesta de incidentes atendidos en la empresa LISERME; mediante la aplicación de la Norma ISO 27035:2016, se reducirá el porcentaje de reincidencia de incidentes en la empresa LISERME; mediante la aplicación de la Norma ISO 27035:2016, se incrementará el nivel de satisfacción del personal del área de TI en la empresa LISERME.

En la investigación en estudio, se formuló la siguiente hipótesis:

“La Aplicación de la Norma internacional ISO 27035:2016 mejorará significativamente la Gestión de incidentes de seguridad de la información de la empresa LISERME S.R.L., Arequipa 2022”

II. MARCO TEÓRICO

Hay varios antecedentes importantes en el presente capítulo de investigación, Hay una serie de precedentes importantes para la consolidación del proyecto de investigación para la aplicación de la Norma ISO 27035:2016 gestión de incidentes, implementado para la empresa LISERME, empresa especializada en la fabricación de productos metálicos, además se detalla información acerca de la gestión de incidentes concretamente de seguridad de la información, entre otros conceptos que apoyaran el desarrollo del proyecto.

A nivel nacional, (INDECOPI, 2013), en su norma, "*NORMA TÉCNICA PERUANA NTP-ISO/IEC 27035:2013",* sostiene que, la seguridad de la información a pesar de contar con políticas, no quiere decir que se garantice que la seguridad esté completamente sin vulnerabilidades, esto puede ocasionar que la seguridad sea ineficaz y pueda llevar a que existan o se generen incidentes de seguridad de los datos, la preparación insuficiente en las empresas puede ocasionar ante dichos incidentes de seguridad de la información sea menos eficaz además que el nivel de impacto sea mayor tanto directo como indirectos en las operaciones.

A nivel internacional, (ISO, 2016), en su norma, ***"ISO/IEC 27035-1:2016(en)",*** sostiene que, los procesos y controles que tienen las organizaciones para la seguridad de la información no garantizan por sí mismos una protección completa. Es probable que a pesar de todo las vulnerabilidades permanezcan después de la implementación de controles, lo que puede debilitar la eficacia de la seguridad de la información además de fomentar la ocurrencia de fallas en la seguridad. Puede afectar directa o indirectamente el negocio de la organización. Además, es inevitable que aparezcan nuevas amenazas antes desconocidas. Por eso es importante que cualquier organización tenga que estructurar y planificar un programa sólido de seguridad de datos.

(Chicano Tejada, 2016), en su libro, *"Gestión de incidentes de seguridad informática",* sostiene que, el objetivo de la gestión de incidentes es emplear adecuadamente los instrumentos esenciales para aplicar los procedimientos

preventivos y correctivos de incidentes. Se inicia con establecer procesos correctos para la prevención de incidentes, la implementación de estas medidas será para impedir que ocurran incidentes, seguido de la detección y reporte de incidentes, que, en caso de repetirse, deberá ser detectado y notificado; así también organizado con una clasificación precisa de roles y responsabilidades, donde permita identificar perfiles y amenazas de alto riesgo. Por otro lado, está el análisis de los incidentes, que examina cómo sucedió el evento y el daño que causó es donde se implementan las acciones correctivas.

A nivel Local, (Arevalo Rodríguez, y otros, 2019), en su investigación, "*Sistema Web y Móvil para Mejorar la Gestión de Incidencias de los Activos Informáticos en una Universidad de Trujillo - 2019"*, sustenta que, el objetivo principal es optimizar la gestión de eventos informáticos en la universidad mediante el desarrollo de un sistema web y móvil, como objetivo específico poder reducir el tiempo de seguimiento y registro de la atención al cliente por parte del activo informático, además de reducir el período de reportes de los activos informáticos.

A nivel Nacional, (Ayala Leon, y otros, 2019), en su investigación, *"Diseño e implementación de la ISO 27035 (gestión de incidentes de seguridad de la información) para el área de plataforma de servicios de una entidad del estado peruano"*, sustenta que, para establecer un adecuado modelo de gestión eficaz de eventos, incidentes y vulnerabilidades de seguridad de la información en la plataforma de servicios de una dependencia del gobierno peruano, esta debe tener una adecuada gestión y poder asegurar el cumplimiento de la implementación.

(Leonardo Panta, y otros, 2020), en su investigación, *"Diseño de Modelo de Gestión de Incidentes de TI para mejorar los procedimientos de seguridad de la información en la universidad de Lambayeque"*, sustenta que, la Universidad, hace uso de conjunto de tecnologías de la información para desarrollar sus procesos, como la mayoría de instituciones, dependiendo principalmente en de la disponibilidad de su infraestructura tecnológica. Esto

hace que ante cualquier incidente de seguridad pueda ser afectado directamente en sus servicios, afectando la continuidad del negocio.

A nivel internacional, (BOCANEGRA DÍAZ, y otros, 2015) en su investigación, *"Aplicativo para la gestión de incidentes de seguridad de la Información en aplicaciones, basado en la NTC-ISO/IEC 27002-27035 Para el caso de uso de la universidad distrital"*, sustenta que, el software de la universidad que es utilizado para la gestión de incidentes de seguridad de la información, utiliza la Norma ISO 27035 permite que la oficina asesora de sistemas pueda monitorear y dar solución a los incidentes de seguridad que se presentan en la universidad. Cumpliendo su objetivo, se estableció la base de datos que facilitará el control y el acceso a los datos de la universidad de forma segura.

Las siguientes teorías sirven de base teórica para una mejor comprensión del trabajo de investigación:

ISO: (ISO, 2022), ***define*** que, ISO es una organización internacional independiente no gubernamental que cuenta con una membresía de 167 organismos nacionales de normalización. A través de sus miembros, reúne a expertos para compartir conocimientos y puedan desarrollar Normas Internacionales.

Evento: (ISO, 2016)**,** ***define*** que, es una ocurrencia observable que podría afectar la seguridad de su información.

Incidente de seguridad de información: (ISO, 2016)**,** ***define*** que, es uno o más evento de seguridad de la información, que logren dañar los activos de la organización o crear un riesgo para su correcto funcionamiento, que da como resultado una violación de datos o de privacidad.

Manejo de incidentes: (ISO, 2016)**,** ***define*** que, son las medidas relacionadas con la detección, informe, evaluación, respuesta, procesamiento y aprendizaje que permitirá adquirir experiencia necesaria para manejar incidentes de seguridad de la información.

Servicio: (Axelos Global Best Practice, 2019), ***define*** que, una forma de crear valor, para un usuario es algo que le ayuda a hacer algo sin requerir que el usuario administre riesgos y costos específicos.

Empresa Comercial: (López, 2022), ***define*** que, es una sociedad comprometida a comprar y luego vender bienes sin cambiarlos o transformarlos.

III. METODOLOGÍA

3.1 Tipo y diseño de investigación

- **Tipo de investigación:**

Según la naturaleza de estudio es de tipo aplicada, puesto que tiene, como finalidad resolver un problema a través de la investigación, una solución innovadora de conocimientos que se adquieren y resolverlo en un corto tiempo.

Investigación aplicada, (CONCYTEC, 2018), en su reglamento *"Reglamento de calificación, clasificación y registro de los investigadores del sistema nacional de ciencia, tecnología e innovación tecnológica - reglamento RENACYT"*, precisa que, su objetivo es identificar, mediante el conocimiento científico, recursos (métodos, protocolos y tecnologías), puedan utilizarse para abordar necesidades reconocidas y específicas.

- **Diseño de investigación:**

Este estudio condujo a un diseño pre experimental de un grupo, pre y pos prueba.

Diseño pre experimental, (Hernandez Sampieri, 2014 pág. 141), en el libro," Metodología *de la investigación sexta edición"*, define que, es un diseño de un solo grupo con un nivel mínimo de control. Suele ser útil como primera aproximación a un problema de investigación.

3.2 Variables y operacionalización

- **Variables:**
  - **V. Independiente:** Aplicación de la Norma internacional ISO 27035:2016
    - **Definición Conceptual:**

      ISO, (ISO, 2022), define que, es un estándar que proporciona las pautas, procesos correctos y mejores prácticas de gestión eficaz de incidentes de seguridad de la información adaptable para distintos tipos de organizaciones, tamaños y sectores. Además de que las organizaciones puedan seguir el

conjunto de buenas prácticas y procedimientos de gestión de incidentes internacionales probadas y recomendadas, brinda una gran cantidad de beneficios a la organización en costos, resolución más rápida de incidentes, mejora continua, fortalece la prevención de incidentes además de reducir los impactos que puedan ocasionar a las organizaciones.

- **Definición operacional:**

  (ISO, 2016), en su norma, ***"ISO/IEC 27035-1:2016(en)",*** Sostiene que, la norma es aplicable a organizaciones de todos los tamaños y en todos los sectores, las empresas podrían adecuar o ajustar los lineamientos de la ISO 27035 al tipo de empresa de acuerdo a los niveles de seguridad de datos que puedan manejar, esto no limita a solo empresas que brinden servicios solo de tecnología.

  Para el desarrollo del estudio, La implementación que se realizará de la Norma internacional ISO 27035:2016, se puede medir por la efectividad de implementar controles y procesos correctos de seguridad de la información.

- **V. Dependiente:** Gestión de incidentes

  - **Definición Conceptual:**

    (ISO, 2016), define que, mantiene un enfoque consistente y efectivo para la resolución de incidentes de seguridad de la información

  - **Definición operacional:**

    Para el desarrollo del estudio, la Gestión de incidentes se puede medir a través de tiempo de respuesta de incidentes atendidos, porcentaje respuesta de incidentes atendidos, porcentaje de reincidencia de incidentes y nivel de satisfacción del personal.

3.3 Población, muestra y muestreo

Población:

Para el desarrollo de la investigación, para el primer indicador, la población, se encuentra determinada por los incidentes reportados en un pedido de 6 días laborables que es equivalente a una semana de trabajo en promedio registra 10 incidentes diarios.

$$N_1 = \frac{10\ Operaciones}{1\ Día}\ X\ \frac{6\ Día}{1\ Semana} = 60\ \text{Incidentes/Semana}$$

$$N_1 = 60\ \text{Incidente/Semana}$$

Para el desarrollo de la investigación, para el segundo indicador, la población, se encuentra determinada por los reportes generados en un periodo de 6 días laborables que es equivalente a una semana de trabajo.

$$N_2 = 6\ Reporte/\text{Semana}$$

Para el desarrollo de la investigación, para el tercer indicador, la población, se encuentra determinada por los reportes generados en un periodo de 6 días laborables que es equivalente a una semana de trabajo.

$$N_3 = \frac{1\ Reporte}{1\ Día}\ X\ \frac{6\ Día}{Semana} = 6\ Reporte/\text{Semana}$$

$$N_3 = 6\ Reporte/\text{Semana}$$

Para el desarrollo de la investigación, para el cuarto indicador, la población, se encuentra determinada por los trabajadores que conforman el área de TI que son de 3 personas.

N_4= 3 Personas

Muestra:

Para el primer indicador, tiempo promedio de respuesta de Incidentes atendidos, la muestra, calculada la población según la información proporcionada por la empresa LISERME, es mayor o igual que 30, entonces se aplica la fórmula para hallar la muestra obteniendo un valor de 57 incidentes.

Para el segundo indicador, porcentaje de respuesta de incidentes atendidos, la muestra, calculada la población mediante la información brindada por la empresa LISERME, que es de 6 reportes menor igual a 30, la muestra es de 6 reportes.

Para el tercer indicador, porcentaje de reincidencia de incidentes, la muestra, calculada la población de acuerdo a la información proporcionada por la empresa LISERME, que es de 6 reportes menor igual a 30, la muestra es de 6 reportes.

Para el cuarto indicador, nivel de satisfacción del personal del área de TI, la muestra, calculada la población de acuerdo a la información proporcionada por la empresa LISERME, que es de 3 personas menor igual a 30, la muestra es de 3 personas.

Muestreo:

Este estudio condujo a que el muestreo sea no probabilístico porque la muestra poblacional se seleccionó mediante manipulación de la muestra que se utilizara.

3.4 Técnicas e instrumentos de recolección de datos

Para el desarrollo del estudio, la recopilación de datos fue hecha para elegir evidencia de calidad que permita que el análisis desarrolle respuestas convincentes y confiables. La observación técnica, donde la información se obtiene a través de la observación, se ha utilizado como método de recolección de datos, la observación técnica que la información se obtiene a través de la observación que es una base esencial para la formación de hipótesis además se utilizó la ficha de observación como instrumento, La encuesta es un proceso de recopilación de datos que incluye varios métodos de recopilación de datos, como el instrumento utilizado, que son el cuestionario y el análisis de documentos, que es el proceso de recopilar información para su posterior análisis y se utilizó como instrumento el análisis documental.

Validez: (Sampieri, y otros, 2014 pág. 200), en el libro, *"Metodología de la investigación"*, *define* qué, "validez grado en que un instrumento en verdad mide la variable que se busca medir".

Para poder realizar la validación de instrumentos en la elaboración de la investigación utilizaremos, Juicio de experto (Ver Anexo 3).

Confiabilidad: (Sampieri, y otros, 2014 pág. 200)**,** en el libro, *"Metodología de la investigación"*, define que, es el nivel en que un instrumento proporciona resultados coherentes y consistentes.

Para poder determinar la confiabilidad de las encuestas a emplear utilizaremos Alfa de Cron Bach (Ver Anexo 8).

3.5 Procedimientos

Para el desarrollo de la investigación, para el primer objetivo se recopiló datos de la empresa mediante el análisis documental, obtenidos mediante un permiso del representante de la empresa LISERME la cual nos permitía mediante una ficha de registro, (Ver Anexo 4) obtener dichos datos.

Para el desarrollo de la investigación, para el segundo objetivo se recopiló datos de la empresa el análisis documental, obtenidos mediante un permiso del representante de la empresa LISERME la cual nos permitía mediante una ficha de registro, (Ver Anexo 4) obtener dichos datos.

Para el desarrollo de la investigación, para el tercer objetivo se recopiló datos de la empresa aplicando el análisis documental, obtenidos mediante un permiso del representante de la empresa LISERME y el jefe del área que pudo proporcionar los datos necesarios, la cual nos permitía mediante una ficha de registro, (Ver Anexo 4) obtener dichos datos.

Para el desarrollo de la investigación, para el cuarto objetivo se recopiló datos de la empresa, obtenidos mediante un permiso del representante de la empresa LISERME realizar una entrevista al jefe del área de TI, para lo cual se utilizó un cuestionario personalizado, (Ver Anexo 4) obtener dichos datos.

3.6 Método de análisis de datos

Para la obtención de los datos se inició el uso de la aplicación del instrumento utilizando los cuestionarios, Con los datos recolectados se procede al análisis estadístico por estadística descriptiva y estadística inferencial para determinar los resultados para el desarrollo de estudio.

(JOHNSON, y otros, 2016), en el libro, "Estadística Elemental", define que, es un estudio de patrones que nos permite hacer predicciones o estimaciones sobre la población de la que se extrae la muestra.

(JOHNSON, y otros, 2016), en el libro, “Estadística Elemental”, define que, es un estudio y descripción de los datos obtenidos como resultado de un experimento.

3.7 Aspectos éticos

La información recolectada en este estudio es utilizada con fines de investigación, se respeta la propiedad de la información, conceptos y tablas, referenciados por los autores correspondientes y organizados según normas ISO 690.

Este trabajo de investigación toma en cuenta el código de ética en investigación de la universidad César Vallejo.

IV. RESULTADOS

Luego de analizar los resultados satisfactorios luego de implementar la aplicación de la Norma Internacional para la gestión eficaz de incidentes de seguridad en la empresa LISERME S.R.L., de la ciudad de Arequipa, primero se realizó un diagnóstico de la situación en la que se encontraba, para la investigación se toman en consideración los indicadores propuestos en el capítulo anterior y dentro del planteamiento del problema ver Anexo 4.

Objetivo específico: Reducir el tiempo promedio de respuesta de Incidentes atendidos.

a. Prueba Descriptiva

Se trabajó en el análisis de los datos recopilados, ver Anexo 4B, de acuerdo con la metodología de investigación utilizando herramientas apropiadas. Análisis inferencial, descriptivo mediante el software IBM SPSS v.28 sobre el indicador se obtiene la siguiente información:

Tabla 1. Tiempos de recolección de datos por tipo de prueba para el primer indicador

Tipo de prueba	Fecha de Inicio	Fecha de Término
Pre Prueba	18/04/2022	23/04/2022
Pos Prueba	20/06/2022	25/06/2022

Fuente: Elaboración propia

Tabla 2. Medidas descriptivas

Estadísticos descriptivos

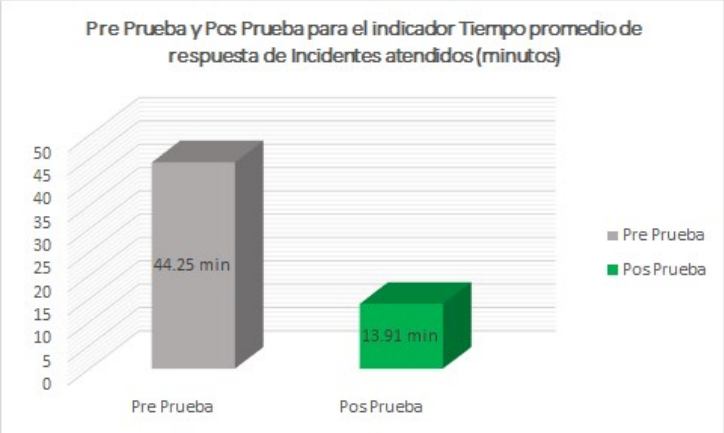
	N	Mínimo	Máximo	Media	Desviación estándar
Pre Prueba	57	15	136	44.25	28.408
Pos Prueba	57	5	23	13.91	4.368
N válido (por lista)	57				

Fuente: IBM SPSS Statistics v.28

Según los resultados de la tabla anterior, mediante el software estadístico IBM SPSS Statistics v.28, tomó un promedio de 44.25 minutos para la pre prueba y un promedio de 13.91 minutos para la pos prueba, lo cual es significativo, el progreso y la mejora significan el tiempo promedio de respuesta a incidentes como se muestra en la siguiente figura. Además, hubo un mínimo de 15 y un máximo de 136 minutos por incidente

en la pre prueba, y luego un mínimo de 5 y un máximo de 23 minutos por incidente en la pos prueba. Esta es una mejora significativa en las prácticas de gestión eficaz de seguridad de la empresa en términos de tiempo promedio de respuesta de incidentes atendidos.

Figura 1. Pre y pos prueba para el primer indicador



Fuente: Elaboración propia

b. Análisis Inferencial

La prueba de normalidad para el indicador, fue realizada mediante la prueba de normalidad de Kolmogórov-Smirnov, porque el tamaño de la muestra es mayor igual a 35, mediante el software estadístico IBM SPSS Statistics v.28.

Tabla 3. Prueba de normalidad de Kolmogorov-Smirnov para el primer indicador

Prueba de normalidad

	Kolmogorov-Smirnov[a]		
	Estadístico	gl	Sig.
Pre Prueba	.226	57	<.001
Pos Prueba	.160	57	<.001

a. Corrección de significación de Lilliefors

Fuente: IBM SPSS Statistics v.28

Según los resultados, de la tabla anterior, se puede ver que los resultados obtenidos de la prueba muestran que el valor de significación en la prueba previa y posterior es inferior a 0.001, es decir, menos de 0,05; si muestra una distribución no normal, por

consiguiente, se indica la prueba de distribución no paramétrica, prueba estadística de Wilcoxon.

Prueba de hipótesis

- **Hipótesis estadística**

  Hipótesis nula (H_n) = La aplicación de la norma internacional ISO 27035:2016 no reduce el tiempo promedio de respuesta de incidentes atendidos.

  Hipótesis alternativa ($H_{a)}$ = La aplicación de la norma internacional ISO 27035:2016 reduce el tiempo promedio de respuesta de incidentes atendidos.

  Indicador: Tiempo promedio de respuesta de incidentes atendidos.

- **Definición de las variables**

  $TPRIA_p$ = Tiempo promedio de respuesta de incidentes atendidos previo a la aplicación de la Norma ISO 27035:2016.

  $TPRIA_c$ = Tiempo promedio de respuesta de incidentes atendidos con la aplicación de la Norma ISO 27035:2016.

Se trabajó con un nivel de significancia para la prueba de las hipótesis de 0.05, además un nivel de confianza correspondiente es 95%.

Tabla 4. Prueba Estadística

Estadísticos de prueba[a]

	Pos Prueba - Pre Prueba
Z	-6.560[b]
Sig. asin. (bilateral)	<.001

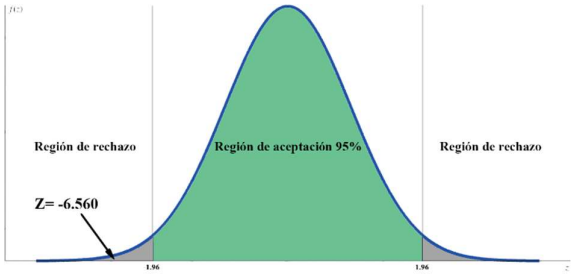
a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos positivos.

Fuente: IBM SPSS Statistics v.28

Se aplicó la prueba de Wilcoxon, ya que los datos son no paramétricos, con rangos de signos, obteniendo p valor es 0.001 además del valor de Z que es -6.560.

Figura 2. Región de aceptación y rechazo para el primer indicador



Fuente: Elaboración propia

El resultado es que el valor p es menor a 0.05 y el valor z está dentro del intervalo de rechazo, por consiguiente, se rechaza la hipótesis nula (Hn) y se acepta la hipótesis alternativa (Ha), con un nivel de confianza de 95%. Como resultado, la implementación de la Norma internacional ISO 27035:2016 reduce el tiempo promedio de respuesta a incidentes.

Objetivo específico: Incrementar el porcentaje de respuesta de incidentes atendidos.

a. Prueba Descriptiva

Se trabajó en el análisis de los datos recopilados, ver Anexo 4B, de acuerdo con la metodología de investigación utilizando herramientas apropiadas. Análisis inferencial, descriptivo mediante el software SPSS v.28 sobre el indicador que recoge la siguiente información:

Tabla 5. Tiempos de recolección de datos por tipo de prueba para el segundo indicador

Tipo de prueba	Fecha de Inicio	Fecha de Término
Pre Prueba	18/04/2022	23/04/2022
Pos Prueba	20/06/2022	25/06/2022

Fuente: Elaboración propia

Tabla 6. Medidas descriptivas

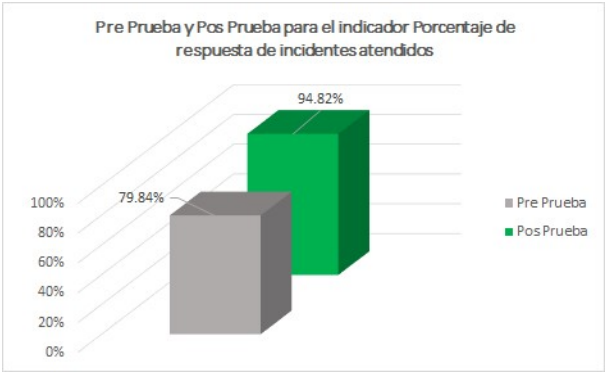
Estadísticos descriptivos

	N	Mínimo	Máximo	Media	Desviación estándar
Pre Prueba	6	57.14%	88.24%	79.8402%	11.44711%
Pos Prueba	6	85.71%	100.00%	94.8218%	6.08306%
N válido (por lista)	6				

Fuente: IBM SPSS Statistics v.28

De los resultados de la tabla anterior, mediante el software estadístico IBM SPSS Statistics v.28 se obtuvo un 79.84% para la pre prueba, mientras que para la pos prueba se obtuvo un 94.82%, lo que muestra una mejora significativa, a través del Incremento logrado en el porcentaje de respuesta de incidentes atendidos como se muestra en la imagen a continuación. Adicionalmente, hubo un mínimo de 57.14% y un máximo de 88.24% de respuesta de incidentes atendidos en la pre prueba, seguido de un mínimo de 85.71% y 100% de respuesta de incidentes atendidos en la pos prueba. Esta es una mejora significativa en las prácticas de gestión de seguridad de la información de la empresa en el Indicador de porcentaje respuesta de incidentes atendidos.

Figura 3. Pre y pre prueba para el segundo indicador



Fuente: Elaboración propia

b. Análisis Inferencial

La prueba de normalidad para el indicador, fue realizada mediante la prueba de normalidad de Shapiro-Wilk, porque el tamaño de la muestra es menor a 35, mediante el software estadístico IBM SPSS Statistics v.28.

Tabla 7. Prueba de normalidad de Shapiro-Wilk para el segundo indicador

Prueba de normalidad

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Pre Prueba	.719	6	.010
Pos Prueba	.833	6	.114

a. Corrección de significación de Lilliefors

Fuente: IBM SPSS Statistics v.28

Según los resultados, de la tabla anterior, se puede ver que los resultados obtenidos de la prueba muestran que el valor de significación en la prueba previa es 0.010, que es menor a 0.05, y después de la prueba es 0.114, que es mayor a 0.05; si muestra una distribución no normal, por consiguiente, se indica la prueba de distribución no paramétrica, prueba estadística de Wilcoxon.

- **Prueba de hipótesis**
  - **Hipótesis estadística**

    Hipótesis nula (H_n) = La aplicación de la norma internacional ISO 27035:2016 no incrementará el porcentaje de respuesta de incidentes atendidos.

    Hipótesis alternativa (H_a) = La aplicación de la norma internacional ISO 27035:2016 incrementara el porcentaje de respuesta de incidentes atendidos.

    Indicador: Porcentaje de respuesta de incidentes atendidos.

  - **Definición de las variables**

    $PRIA_p$ = Porcentaje de respuesta de incidentes atendidos previo a la aplicación de la Norma ISO 27035:2016.

    $PRIA_c$ = Porcentaje de respuesta de incidentes atendidos con la aplicación de la Norma ISO 27035:2016.

    Se trabajó con un nivel de significancia para la prueba de las hipótesis de 0.05, además un nivel de confianza correspondiente es 95%.

Tabla 8. Prueba Estadística

Estadísticos de prueba[a]

	Pos Prueba - Pre Prueba
Z	-1.992[b]
Sig. asin. (bilateral)	.046

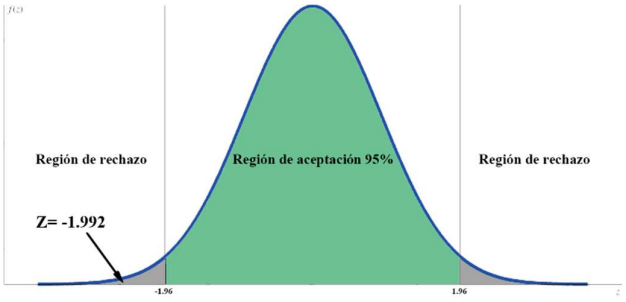
a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Fuente: IBM SPSS Statistics v.28

Se aplicó la prueba de Wilcoxon, ya que los datos son no paramétricos, con rangos de signos, obteniendo p valor es 0.046, además del valor de Z que es -1.992.

Figura 4. Región de aceptación y rechazo para el segundo indicador



Fuente: Elaboración propia

El resultado es que p es menor a 0.05 y el valor de z está dentro del intervalo de rechazo, por consiguiente, se rechaza la hipótesis nula (Hn) y se acepta la hipótesis alternativa (Ha), con un nivel de 95% de confianza. Como resultado la implantación de la norma internacional ISO 27035:2016 aumenta el porcentaje de respuestas de incidencias atendidas.

Objetivo específico: Reducir el porcentaje de reincidencia de incidentes

a. Prueba Descriptiva

Se trabajó en el análisis de los datos recopilados, ver Anexo 4B, de acuerdo con la metodología de investigación utilizando herramientas apropiadas. Análisis inferencial, descriptivo mediante el software SPSS v.28 sobre el indicador que recoge la siguiente información:

Tabla 9. Tiempos de recolección de datos por tipo de prueba para el tercer indicador

Tipo de prueba	Fecha de Inicio	Fecha de Término
Pre Prueba	18/04/2022	23/04/2022
Pos Prueba	20/06/2022	25/06/2022

Fuente: Elaboración propia

Tabla 10. Medidas descriptivas

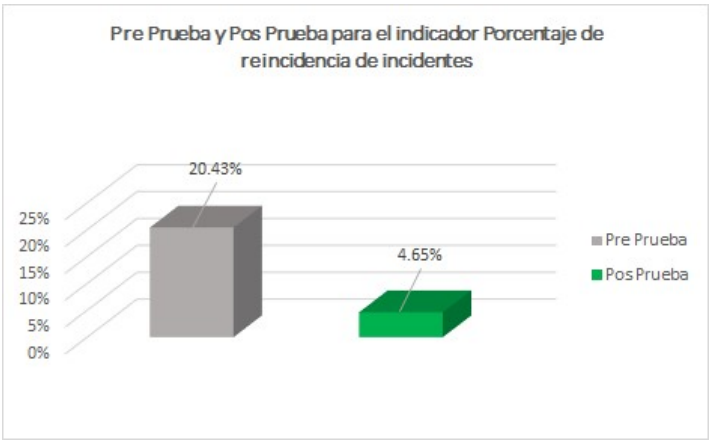
Estadísticos descriptivos

	N	Mínimo	Máximo	Media	Desviación estándar
Pre Prueba	6	14.29%	30.00%	20.4259%	6.97113%
Pos Prueba	6	0.00%	11.11%	4.6491%	5.20751%
N válido (por lista)	6				

Fuente: IBM SPSS Statistics v.28

Según los resultados de la tabla anterior, mediante el software estadístico IBM SPSS Statistics v.28 se obtuvo un 20.43% para la pre prueba, mientras que para la pos prueba se consiguió un 4.65%, lo que representa una mejora significativa, una disminución en el porcentaje de reincidencias de incidentes, como se muestra en la siguiente figura. Además, hubo un mínimo de 14.29% y un máximo de 30% de reincidencia de incidentes durante la pre prueba y luego un mínimo de 0% y 11.11% de reincidencia de incidentes durante la pos prueba. Esta es una mejora significativa en las capacidades de gestión de seguridad de la información de la empresa en términos de porcentaje de reincidencia de incidentes.

Figura 5. Pre y pre prueba para el tercer indicador



Fuente: Elaboración propia

b. Análisis Inferencial

La prueba de normalidad para el indicador, fue realizada mediante la prueba de normalidad de Shapiro-Wilk, porque el tamaño de la muestra es menor a 35, mediante el software estadístico IBM SPSS Statistics v.28.

Tabla 11. Prueba de normalidad de Shapiro-Wilk para el tercer indicador

Prueba de normalidad

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Pre Prueba	.794	6	.052
Pos Prueba	.794	6	.052

a. Corrección de significación de Lilliefors

Fuente: IBM SPSS Statistics v.28

De acuerdo a la tabla anterior, se puede observar que los resultados obtenidos de la prueba muestran que el valor de significancia en el pre y pos prueba es de 0.052, el cual es mayor a 0.05, por consiguiente, se indica la prueba de distribución paramétrica (T de Student).

- **Prueba** de hipótesis
  - **Hipótesis estadística**

    Hipótesis nula (H_n) = La aplicación de la Norma internacional ISO 27035:2016 no reducirá el porcentaje de reincidencia de incidentes.

Hipótesis alternativa (H_a) = La aplicación de la Norma internacional ISO 27035:2016 reducirá el porcentaje de reincidencia de incidentes.

Indicador: Porcentaje de reincidencia de incidentes.

- **Definición de las variables**

$PRIA_p$ = Porcentaje de reincidencia de incidentes previo a la aplicación de la Norma ISO 27035:2016.

$PRIA_c$ = Porcentaje de reincidencia de incidentes con la aplicación de la Norma ISO 27035:2016.

Se trabajó con un nivel de significancia para la prueba de las hipótesis de 0.05, además un nivel de confianza correspondiente es 95%.

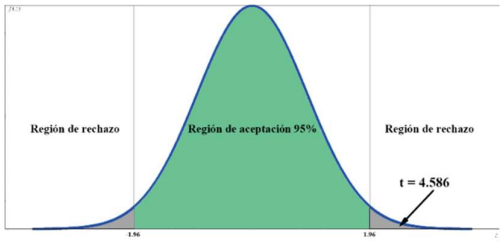
Tabla 12. Prueba Estadística

	Diferencias emparejadas							
				95% de intervalo de confianza de la				
	Media	Desviación estándar	Media de error estándar	Inferior	Superior	t	gl	Sig.(bilateral)
Par 1 Pre Prueba - Pos Prueba	15.77686%	8.42633%	3.44003%	6.93397%	24.61975%	4.586	5	.006

Fuente: IBM SPSS Statistics v.28

Se aplicó para muestras emparejadas la prueba T de Student, ya que los datos son paramétricos obteniendo p valor es 0.006 además que el valor de t es de 4.586.

Figura 6. Región de aceptación y rechazo para el tercer indicador



Fuente: Elaboración propia

El resultado es que p es menor a 0.05 y el valor de t está en el intervalo de rechazo, por lo tanto, se rechaza la hipótesis nula (Hn) y se acepta la hipótesis alternativa (Ha), con un nivel

de 95% de confianza. Como resultado de la implementación de la Norma internacional ISO 27035:2016 reduce el porcentaje de reincidencia de incidentes.

Objetivo específico: Incrementar el nivel de satisfacción del personal del área de TI

a. Prueba Descriptiva

Se trabajó en el análisis de los datos recopilados, ver Anexo 4B, de acuerdo con la metodología de investigación utilizando herramientas apropiadas. Análisis inferencial, descriptivo mediante el software SPSS v.28 sobre el indicador que recoge la siguiente información:

Tabla 13. Tiempos de recolección de datos por tipo de prueba para el cuarto indicador

Tabla1. Tiempos de recolección de datos por tipo de prueba

Tipo de prueba	Fecha de Inicio	Fecha de Término
Pre Prueba	18/04/2022	23/04/2022
Pos Prueba	20/06/2022	25/06/2022

Fuente: Elaboración propia

Tabla 14. Medidas descriptivas

Estadísticos descriptivos

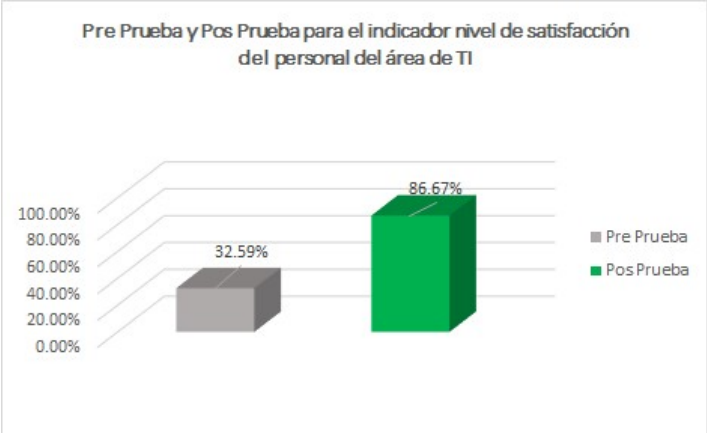
	N	Mínimo	Máximo	Media	Desviación estándar
Pre Prueba	9	1.00	3.00	1.6296	.65499
Pos Prueba	9	4.00	5.00	4.3333	.28868
N válido (por lista)	9				

Fuente: IBM SPSS Statistics v.28

Según los resultados de la tabla anterior, mediante el software estadístico IBM SPSS Statistics v.28 para la pre prueba, se consiguió una puntuación media de 1.63 equivalentes a 32.59% del puntaje promedio, mientras que para la pos prueba se obtuvo una media de 4.78 equivalentes a 95.56% del puntaje promedio, obteniendo un progreso notable incrementando el nivel de satisfacción del personal del área de TI, como se muestra en la figura a continuación. Además, dentro de la pre prueba hubo un mínimo de 1 y un máximo de 3 de puntaje promedio y luego dentro de la pos prueba hubo un mínimo de 4.67 y 5 de puntaje promedio. Esta es una mejora significativa en las prácticas de gestión

eficaz de la seguridad de la información de la empresa en el indicador de nivel de satisfacción del personal del área de TI.

Figura 7. Pre y pre prueba para el cuarto indicador



Fuente: Elaboración propia

b. Análisis Inferencial

La prueba de normalidad para el indicador, fue realizada mediante la prueba de normalidad de Shapiro-Wilk, debido a que el tamaño de la muestra es menor a 35, mediante el software estadístico IBM SPSS Statistics v.28.

Tabla 15. Prueba de normalidad de Shapiro-Wilk para el cuarto indicador

Prueba de normalidad

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Pre Prueba	.849	9	.074
Pos Prueba	.728	9	.003

a. Corrección de significación de Lilliefors

Fuente: IBM SPSS Statistics v.28

De acuerdo a la tabla anterior, se puede observar que los resultados obtenidos de la prueba, muestran que el valor de significación en la prueba previa es 0.074, que es más de 0.05, y después de la prueba es 0.003, que es menos de 0.05; si muestra una distribución no normal, por consiguiente, se indica la prueba de distribución no paramétrica, prueba estadística de Wilcoxon.

- **Prueba** de hipótesis

- **Hipótesis estadística**

  Hipótesis nula (H_n) = La aplicación de la norma internacional ISO 27035:2016 no incrementará el nivel de satisfacción del personal del área de TI.

  Hipótesis alternativa (H_a) = La aplicación de la norma internacional ISO 27035:2016 incrementará el nivel de satisfacción del personal del área de TI.

  Indicador: Nivel de satisfacción del personal del área de TI.

- **Definición de las variables**

  NSP_p = Nivel de satisfacción del personal del área de TI previo a la aplicación de la Norma ISO 27035:2016.

  $PRIA_c$ = Nivel de satisfacción del personal del área de TI con la aplicación de la Norma ISO 27035:2016.

Se trabajó con un nivel de significancia para la prueba de las hipótesis de 0.05, además un nivel de confianza correspondiente es 95%.

Tabla 16. Prueba Estadística

Estadísticos de prueba[a]

	Pos Prueba - Pre Prueba
Z	-2.719[b]
Sig. asin. (bilateral)	.007

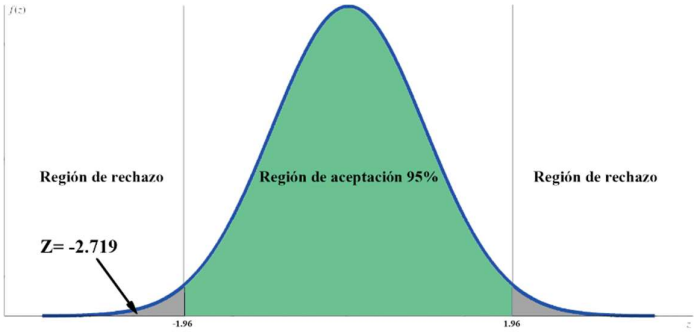
a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Fuente: IBM SPSS Statistics v.28

Se aplicó la prueba de Wilcoxon, ya que los datos son no paramétricos, obteniendo p valor es 0.007, además que el valor de Z es de -2.719.

Figura 8. Región de aceptación y rechazo para el cuarto indicador



Fuente: Elaboración propia

El resultado es que p es menor a 0.05 y el valor de z está dentro del intervalo de rechazo, por lo tanto, se rechaza la hipótesis nula (Hn) y se acepta la hipótesis alternativa (Ha) con un nivel de 95% de confianza. Por lo tanto, la implementación del estándar internacional ISO 27035: 2016 aumenta la satisfacción de los empleados de TI.

V. DISCUSIÓN

En cuanto al indicador tiempo promedio de respuesta de Incidentes atendidos, se obtuvo un tiempo promedio de respuesta de 44.25 minutos pre prueba y se redujo a 13.91 minutos pos prueba, consiguiendo una disminución significativa de 68.56%. Estos resultados obtenidos son semejantes a los descritos por (Chicano Tejada, 2016), Sostiene que, el objetivo de la gestión de incidentes es emplear adecuadamente los instrumentos esenciales para aplicar los procedimientos preventivos y correctivos de incidentes.

Del mismo modo, son equiparables por la (ISO, 2016), en su norma, Sostiene que, es especial para cualquier organización que desee tener un programa sólido de seguridad que contenga un enfoque planificado y estructurado para resolver incidentes de seguridad de la información más rápido y de manera proactiva, incluido el establecimiento de controles apropiados para prevenir, recuperarse y aprender de cada incidente.

En cuanto al indicador porcentaje de respuesta de incidentes atendidos, se obtuvo un incremento del porcentaje de respuesta de incidentes atendidos de 79.84% pre prueba a 94.82% pos prueba, consiguiendo un aumento significativo. Estos resultados obtenidos son semejantes a los descritos por (Leonardo Panta, y otros, 2020), Concluye que, el modelo de gestión de incidentes permite monitorear y detectar amenazas antes que ocurran fortaleciendo los procedimientos de seguridad en general.

Del mismo modo, son equiparables por la (ISO, 2016), Sostiene que, es especial para cualquier organización que desee un programa sólido de seguridad de la información que tenga un enfoque estructurado y planificado para informar las vulnerabilidades de seguridad de la información para que puedan evaluarse y ser tratadas adecuadamente.

En cuanto al indicador porcentaje de reincidencia de incidentes, se obtuvo una reducción del porcentaje de reincidencia de incidentes de 20.43% pre prueba a 5.21% pos prueba, consiguiendo una reducción significativa de 77.24% de promedio de reincidencia de incidentes. Estos resultados obtenidos son semejantes a los descritos por (BOCANEGRA DÍAZ, y otros, 2015), sustenta que, el software administrado por la universidad de gestión de

incidentes permitirá, dar solución y seguimiento a los incidentes de seguridad de información reportados que puedan causar un riesgo a la universidad.

Del mismo modo, son equiparables por la (ISO, 2016), Sostiene que, es especial para cualquier organización que desee un programa sólido de seguridad de la información que tenga un enfoque estructurado y planificado para aprender de los incidentes y vulnerabilidades de seguridad de la información, implementar controlescorrectos que permitan ser preventivos y mejorar la seguridad general fortaleciendo los puntos débiles del entorno para la gestión eficaz de incidentes de seguridad de la información.

En cuanto al indicador nivel de satisfacción del personal, se obtuvo un incremento del nivel de satisfacción del personal de 1.63 puntos que equivale 32.59% pre prueba a 4.33 puntos que equivale 86.67% de nivel de satisfacción del personal pos prueba, consiguiendo aumentar el nivel de satisfacción del personal de TI en un 54.07%. Estos resultados obtenidos son semejantes a los descritos por (Leonardo Panta, y otros, 2020), afirma que, el modelo propuesto fue evaluado y que obteniendo que el valor que más aporta es la satisfacción de personal, dando un gran nivel de aporte, consiguiendo una mayor rapidez, priorizando y teniendo buenos canales de comunicación.

Del mismo modo, son afirmados por (ISO, 2016), Sostiene que las organizaciones pueden ajustar la orientación proporcionada en la norma ISO/IRC 27035, por su tipo, tamaño y naturaleza del negocio, en relación con la situación de riesgo de seguridad de información.

VI. CONCLUSIONES

Oe_1: Se consigue reducir el tiempo promedio de la empresa LISERME S.R.L., Arequipa 2022, aplicando la Norma, obteniendo con resultados muy favorables de 44.25 minutos a 13.91 minutos lo cual demuestra una disminución de 68.56% en el promedio. Se prueba y demuestra que la solución que se presenta logra el objetivo propuesto de reducir el tiempo promedio.

Oe_2: Se consigue incrementar el porcentaje de respuesta de incidentes atendidos de la empresa LISERME S.R.L., Arequipa 2022, aplicando la Norma, de 79.84% a 94.82% de incidentes atendidos. Se prueba y demuestra que la solución propuesta logra el objetivo propuesto de incrementar el porcentaje.

Oe_3: Se consigue reducir el porcentaje de reincidencia de incidentes de la empresa LISERME S.R.L., Arequipa 2022, aplicando la Norma, de 20.43% a 4.65%. Se prueba y demuestra que la solución propuesta logra el objetivo propuesto de reducir el porcentaje.

Oe_4: Se consigue aumentar el nivel de satisfacción del personal de área de TI de la empresa LISERME S.R.L., Arequipa 2022, aplicando la Norma, de 1.63 puntos que equivale 32.59% a 4.33 puntos que equivale 86.67% de nivel de satisfacción del personal. Se prueba y demuestra que la solución propuesta logra el objetivo propuesto de incrementar el nivel de satisfacción del personal.

VII. RECOMENDACIONES

Se recomienda al gerente general pueda garantizar que la toma de decisiones se valide desde una perspectiva estratégica y operativa, así como delegar y facultar la ejecución de las acciones aprobadas, y demostrar una buena administración de recursos disponibles y considerando el bienestar a largo plazo de la empresa.

Se recomienda al jefe de TI, utilizar un sistema de seguimiento para las acciones recomendadas porque apoyará líderes organizacionales y otros para seguir el estado de implementación.

Se recomienda al jefe del área legal, programar capacitaciones constantes sobre asuntos de responsabilidad y cumplimiento además de brindar orientación sobre privacidad y libertades civiles para garantizar que las acciones de investigación y respuesta no infrinjan los derechos de los empleados.

Se recomienda al jefe de recursos humanos, hacer seguimiento a los porcentajes de incidencias atendidas y reincidencias de incidentes, ya que así se podrá determinar si la atención es correcta y tener una mejor productividad.

Se recomienda al jefe de relaciones públicas, programar capacitaciones sobre políticas y prácticas de divulgación de información.

Se recomienda al personal del área de TI, que trabaje en el cumplimiento de los procedimientos y políticas del área de TI, ya que debe de ser el ejemplo para las demás áreas de la organización.

Se recomienda a los empleados de las distintas áreas de la empresa, asistir a capacitaciones programadas para una buena gestión de incidentes.

REFERENCIAS

Arevalo Rodríguez, Percy Fernando y Montalvo Martínez, Leticia Cecilia. 2019. *Sistema Web y Móvil para Mejorar la Gestión de Incidencias de los Activos Informáticos en una Universidad de Trujillo - 2019.* Trujillo : s.n., 2019.

Axelos Global Best Practice. 2019. *ITIL Foundation, ITIL 4 Edition: Spanish Translation (ITIL 4 Foundation).* s.l. : TSO, The Stationery Office; 4a edición (27 Septiembre 2019), 2019.

Ayala Leon, Cristhian Fausto y Lopez Valencia, Enzo Francescoli. 2019. *Diseño e implementación de la ISO 27035 (gestión de incidentes de seguridad de la información) para el área de plataforma de servicios de una entidad del estado peruano.* Lima : s.n., 2019.

Blandez Ricalde, María de Guadalupe . 2016. *Proceso Administrativo.* s.l. : Editorial Digital UNID, 2016.

BOCANEGRA DÍAZ, FABIÁN ENRIQUE y ORDOÑEZ TOVAR, JEFFERSON SNEIDER. 2015. *Aplicativo para la gestión de incidentes de seguridad de la Información en aplicaciones, basado en la NTC-ISO/IEC 27002-27035. Para el caso de uso de la universidad distrital.* Bogota : s.n., 2015. NTC-ISO/IEC 27002-27035.

Chicano Tejada , Ester. 2016. *Gestión de incidentes de seguridad informática.* s.l. : IC editorial , 2016. 9788416351701.

CONCYTEC. 2018. REGLAMENTO DE CALIFICACIÓN, CLASIFICACIÓN Y REGISTRO DE LOS INVESTIGADORES DEL SISTEMA NACIONAL DE CIENCIA, TECNOLOGÍA E INNOVACIÓN TECNOLÓGICA - REGLAMENTO RENACYT. [En línea] 2018. https://vinculate.concytec.gob.pe/encyclopedia/investigacion-aplicada/#_ftn2.

European Network and Information Security Agency. 2010. Good Practice Guide for Incident Management. *Good Practice Guide for Incident Management.* 2010.

Hernandez Sampieri, Roberto. 2014. *Metodología de la Investigación.* México : McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V., 2014. 9781456223960.

INDECOPI. 2013. NORMA TÉCNICA PERUANA NTP-ISO/IEC 27035:2013. *NORMA TÉCNICA PERUANA NTP-ISO/IEC 27035:2013.* Lima : s.n., 2013. Vol. 1.

INEI. 2018. Perú: Tecnologías de Información y Comunicación en las Empresas. *Plataforma digital única del Estado Peruano.* [En línea] 2018. https://cdn.www.gob.pe/uploads/document/file/3444629/Per%C3%BA%3A%20Tecnolog%C3%ADas%20de%20Informaci%C3%B3n%20y%20Comunicaci%C3%B3n%20en%20las%20Empresas.pdf?v=1658509984.

ISO. 2022. Organización Internacional para a Normalización (ISO). *www.ISO.org.* [En línea] 2022. [Citado el: 01 de 04 de 2022.] www.ISO.org.

—. 2016. SO/IEC 27035-1:2016(en). 2016.

ISO/IEC 27000. 2018. Information technology — Security techniques — Information security management systems — Overview and vocabulary. *ISO/IEC 27000:2018.* 2018. ISO/IEC 27000:2018.

JOHNSON, ROBERT y KUBY, PATRICIA . 2016. *Estadística Elemental.* s.l. : Cengage Learning, 2016. Vol. 11. 9786075228358.

Leonardo Panta, Miguel Angel y Regalado Delgado, Edson. 2020. *Diseño de Modelo de Gestión de Incidentes de TI para mejorar los procedimientos de seguridad de la información en la universidad de Lambayeque.* Lambayeque : s.n., 2020.

López, José Francisco. 2022. Empresa comercial. *Economipedia.com.* [En línea] 2022. [Citado el: 1 de Abril de 2022.] https://economipedia.com/definiciones/empresa-comercial.html#:~:text=Una%20empresa%20comercial%20es%20una,no%20transforma%20los%20bienes%20comprados..

NIST. 2018. Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. *NIST Special Publication (SP) 800-37 Rev. 2.* 2018.

Paul Cichonski, Tom Millar,TimGrance,Karen Scarfone. 2021. Computer Security Incident Handling Guide. *NIST Special Publication 800-61, Revision 2, Computer Security Incident Handling Guide.* 2021. National Institute of Standards and Technology (NIST).

RAE. 2022. https://www.rae.es/. *Real Academia Española.* [En línea] 2022. [Citado el: 01 de 04 de 2022.]

Sampieri, Roberto Hernández, Collado, Carlos Fernández y Lucio, María del Pilar Baptista. 2014. *Metodología de la investigación 6a Edición.* México D.F. : McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V., 2014.

Sundaram, Vijay. 2022. diarioti. *diarioti.* [En línea] 20 de Diciembre de 2022. https://diarioti.com/siete-tendencias-tecnologicas-que-impulsaran-los-negocios-en-2022/118479.

WeLiveSecurity, ESET. 2021. ESET security report Latinoamérica. *welivesecurity.* [En línea] 2021. https://www.welivesecurity.com/wp-content/uploads/2021/06/ESET-security-report-LATAM2021.pdf.

ANEXOS

Anexos 1: Matriz de consistencia

Tabla 17: Matriz de consistencia

Problema	Objetivos	Hipótesis	Variables	Diseño Metodológico	Población, Muestra y Muestreo
¿De qué manera la aplicación de la norma internacional ISO 27035:2016 influye en la gestión de incidentes de seguridad de la información en la empresa LISERME S.R.L., Arequipa 2022?	Objetivo general: Mejorar la gestión de incidentes de seguridad de la empresa LISERME de la ciudad de Arequipa mediante la aplicación de la Norma internacional ISO 27035:2016 en el año 2022. Objetivos específicos: Reducir el Tiempo Promedio de respuesta de Incidentes atendidos, Incrementar el porcentaje de respuesta de incidentes atendidos, Reducir el porcentaje de reincidencia de incidentes, incrementar el nivel de satisfacción del personal del área de TI.	"La Aplicación de la Norma internacional ISO 27035:2016 mejorara significativamente la Gestión de incidentes de seguridad de la información en la empresa LISERME S.R.L., Arequipa 2022"	V. Independiente: Aplicación de la Norma internacional ISO 27035:2016 V. Dependiente: Gestión de incidentes de seguridad de la información	Tipo de investigación: Es una investigación es de tipo aplicada Nivel de investigación: Es una investigación pre experimental	Población Para el primer indicador: N_1 =60 Incidentes por semana Para el segundo indicador: N_2 = 6 Reportes semanales Para el tercer indicador: N_3 = 6 Reportes semanales Para el cuarto indicador N_4 = 3 Personas Muestra Para el primer indicador: n_1 =57 Incidentes Para el segundo indicador: n_2 = 6 Reportes Para el tercer indicador: n_3 = 6 Reportes Para el cuarto indicador n_4 = 3 Personas Muestreo El muestreo es de tipo no probabilístico porque se manipuló la elección de la muestra poblacional

Fuente: Elaboración propia

Anexos 2: Matriz de operacionalización

Tabla 18 Matriz de operacionalización de la variable independiente

Variable	Definición Conceptual	Definición Operacional	Dimensión	Indicador	Escala de Medición
V. Independiente: Aplicación de la Norma internacional ISO 27035:2016	ISO (2022) En su norma "ISO/IEC 27035-1:2016 Tecnología de la información. Técnicas de seguridad. Gestión de incidentes de seguridad de la información. Parte 1: Principios de la gestión de incidentes." Presenta que es la base de esta Norma Internacional de varias partes. Presenta conceptos básicos y fases de la gestión de incidentes de seguridad de la información y combina estos conceptos con principios en un enfoque estructurado para detectar, informar, evaluar y responder a incidentes, y aplicar las lecciones aprendidas.	La Aplicación de la Norma internacional ISO 27035:2016 se puede medir a través de efectividad de la implementación de los controles de seguridad de la información, Numero de incidentes detectados, Número de controles aplicables, Satisfacción del cliente.	Aplicabilidad de la norma	Efectividad	Intervalo
				Número de incidentes detectados	Intervalo
				Número de controles aplicables	Intervalo
			Seguridad de la Información	Confidencialidad	Valoración de riesgo
				Integridad	
				Disponibilidad	

Fuente: Elaboración propia

Tabla 19 Matriz de operacionalización de la variable dependiente

Variable	Definición Conceptual	Definición Operacional	Dimensión	Indicador	Instrumento	Unidad de Medida	Escala de Medición	Operatividad
V. Dependiente: Gestión de incidentes de seguridad de la información	ISO (2016) "Ejercicio de un enfoque coherente y eficaz para el manejo de incidentes de seguridad de la información"	La Gestión de incidentes de seguridad de la información se puede medir a través de tiempo de respuesta de incidentes atendidos, porcentaje respuesta de incidentes atendidos, porcentaje de reincidencia de incidentes y Nivel de Satisfacción del personal del área de TI.	Tiempo	Tiempo **Promedio** de respuesta de Incidentes atendidos	Ficha de registro	Minutos	Razón	TPRIA=$\frac{\sum_1^n Ti}{n}$ TPRI=Tiempo de respuesta de incidentes atendidos
				Porcentaje de respuesta de incidentes atendidos	Ficha de registro	Diario	Razón	PRIA=$\frac{TRIA\ X100}{TIR}$ PRIA=Porcentaje respuestas de incidentes atendidos TRIA=Total de respuesta de incidentes atendidas TIR=Total de incidentes reportados
				Porcentaje de reincidencia de incidentes	Ficha de registro	Diario	Razón	PRI=$\frac{TRIA\ X100}{TIR}$ PRI=Porcentaje reincidencia de incidentes TRIA=Total de reincidencia de incidentes atendidas TIR=Total de incidentes recibidas
			Personal de Área de TI	Nivel de satisfacción del personal	Cuestionario	Escala de Likert	Ordinal	NSP=$\sum_{i=1}^{3}\sum_{i=1}^{9} Ri\ i$ NSP= Grado de satisfacción de personal R=Respuesta

Fuente: Elaboración propia

Anexos 3. Método de juicio experto

Método de Juicio Experto

Evaluación de la metodología para la Aplicación de la Norma internacional ISO 27035:2016

Apellidos y nombres del experto: Agreda Gamboa, Everson David

Título profesional y/o Grado académico: Ingeniero de Sistemas / Doctor

Fecha: 15/04/2022

Título del proyecto de investigación: "Aplicación de la Norma internacional ISO 27035:2016 para la gestión de incidentes en la empresa LISERME, Arequipa 2022"

Autor(es): Limache Ynquilla, Anuar Mauro

Mediante, el método de juicio experto, Usted tiene la facultad de calificar las metodologías involucradas, mediante una serie de criterios con puntuaciones especificadas al final de la tabla. Así mismo le exhortamos en la correcta determinación de la metodología para el desarrollar la solución propuesta en el presente proyecto de investigación y, también si hubiese algunas sugerencias:

Ítem	Criterio	Descripción	Metodologías		
			ISO 27035	NIST SP 800-61	Good Practice Guide for Incident Management
1	Complejidad	Es el nivel de abstracción del estudio de la metodología	3	2	1
2	Tiempo de desarrollo	Es el tiempo que toma el desarrollo completo	3	2	1
3	Información	Es la cantidad de información disponible	3	2	1
4	Requerimientos	Es la cantidad de requerimientos	3	2	1
5	Claridad	Es decir, su sintáctica y semántica son adecuadas	3	2	1
6	Coherencia	Es la relación lógica con la dimensión o indicador que está midiendo	3	2	1
Total			**18**	12	6

La escala a evaluar es de: 1 - Malo,2 - Regular, 3 – Bueno

Sugerencias:

Firma del experto

Evaluación de la metodología para la Aplicación de la Norma internacional ISO 27035:2016

Apellidos y nombres del experto: Gómez Ávila, José Alberto

Título profesional y/o Grado académico: Ingeniero de Sistemas / Doctor

Fecha: 15/04/2022

Título del proyecto de investigación: "Aplicación de la Norma internacional ISO 27035:2016 para la gestión de incidentes en la empresa LISERME, Arequipa 2022"

Autor(es): Limache Ynquilla, Anuar Mauro

Mediante, el método de juicio experto, Usted tiene la facultad de calificar las metodologías involucradas, mediante una serie de criterios con puntuaciones especificadas al final de la tabla. Así mismo le exhortamos en la correcta determinación de la metodología para el desarrollar la solución propuesta en el presente proyecto de investigación y, también si hubiese algunas sugerencias:

Ítem	Criterio	Descripción	Metodologías		
			ISO 27035	NIST SP 800-61	Good Practice Guide for Incident Management
1	Complejidad	Es el nivel de abstracción del estudio de la metodología	3	3	1
2	Tiempo de desarrollo	Es el tiempo que toma el desarrollo completo	3	2	1
3	Información	Es la cantidad de información disponible	3	2	1
4	Requerimientos	Es la cantidad de requerimientos	3	3	2
5	Claridad	Es decir, su sintáctica y semántica son adecuadas	3	2	1
6	Coherencia	Es la relación lógica con la dimensión o indicador que está midiendo	3	2	1
Total			**18**	13	7

La escala a evaluar es de: 1 - Malo,2 - Regular, 3 – Bueno

Sugerencias:

Firma del experto

Evaluación de la metodología para la Aplicación de la Norma internacional ISO 27035:2016

Apellidos y nombres del experto: Córdova Otero, Juan Luis

Título profesional y/o Grado académico: Ing. Computación y Sistemas / Maestro

Fecha: 15/04/2022

Título del proyecto de investigación: "Aplicación de la Norma internacional ISO 27035:2016 para la gestión de incidentes en la empresa LISERME, Arequipa 2022"

Autor(es): Limache Ynquilla, Anuar Mauro

Mediante, el método de juicio experto, Usted tiene la facultad de calificar las metodologías involucradas, mediante una serie de criterios con puntuaciones especificadas al final de la tabla. Así mismo le exhortamos en la correcta determinación de la metodología para el desarrollar la solución propuesta en el presente proyecto de investigación y, también si hubiese algunas sugerencias:

Ítem	Criterio	Descripción	Metodologías		
			ISO 27035	NIST SP 800-61	Good Practice Guide for Incident Management
1	Complejidad	Es el nivel de abstracción del estudio de la metodología	2	2	1
2	Tiempo de desarrollo	Es el tiempo que toma el desarrollo completo	3	2	2
3	Información	Es la cantidad de información disponible	3	3	1
4	Requerimientos	Es la cantidad de requerimientos	3	2	2
5	Claridad	Es decir, su sintáctica y semántica son adecuadas	3	2	1
6	Coherencia	Es la relación lógica con la dimensión o indicador que está midiendo	2	2	1
Total			**16**	13	8

La escala a evaluar es de: 1 - Malo,2 - Regular, 3 – Bueno

Sugerencias:

Firma del experto

Resumen y resultados de criterios para selección de la metodología

Selección de la metodología para la Aplicación de la Norma internacional ISO 27035:2016

Expertos	Metodología		
	ISO 27035	NIST SP 800-61	Good Practice Guide for Incident Management
Dr. David Agreda Gamboa	18	12	6
Dr. José Gómez Ávila	18	13	7
Ms. Juan Córdova Otero	16	13	8
Total	**52**	38	21

De acuerdo con la tabla anterior se muestra las metodologías para la Aplicación de la Norma internacional ISO 27035:2016, seleccionados por tres expertos y sus respectivos puntajes obtenidos son los siguientes, **La Metodología ISO 27035 con la mayor puntuación entre las evaluadas con un total de 52 puntos**, NIST SP 800-61 con un total de 38 puntos e Good Practice Guide for Incident Management con un total de 21 puntos.

Anexos 4. Instrumentos de recolección de datos

Indicadores de las variables de estudio

Tabla 20. Indicadores de las variables de estudio

Objetivo específico	Indicador	Técnica / Instrumento	Unidad de medida	Operatividad	Muestra poblacional
Reducir el Tiempo Promedio de respuesta de Incidentes atendidos	Tiempo Promedio de respuesta de Incidentes atendidos (TPRIA)	Observación / Ficha de registro	Minutos	TPRIA=$\frac{\sum_1^n Ti}{n}$	n_1=57 Incidentes Reportados
Incrementar el porcentaje de respuesta de incidentes atendidos	Porcentaje de respuesta de incidentes atendidos (PRIA)	Observación / Ficha de registro	Diario	PRIA=$\frac{TRIA\ X100}{TIR}$ TRIA=Total de respuesta de incidentes atendidos TIR=Total de incidentes reportados	n_2= 6 Reportes
Reducir el porcentaje de reincidencia de incidentes	Porcentaje de reincidencia de incidentes (PRI)	Observación / Ficha de registro	Diario	PRI=$\frac{TRIA\ X10}{TIR}$ TRIA=Total de reincidencia de incidentes atendidas TIR=Total de incidentes reportados	n_2=6 Reportes
Incrementar el nivel de satisfacción del personal del área de TI	Nivel de satisfacción del personal (NSP)	Encuesta / Cuestionario	Escala de Likert	NSP=$\sum_{i=1}^{3}\sum_{j=1}^{9} Ri$	n_4=3 Personas

Fuente: Elaboración propia

Anexo 4A - Guía de entrevista aplicado al jefe de TI de la empresa LISERME

Entrevista para determinar la problemática actual

El objetivo de la presente entrevista es conocer su opinión sobre la gestión de incidentes como parte de un trabajo de investigación agradeciendo por anticipado su colaboración y objetividad al responder.

Entrevistado: Miguel Calderon Flores

Cargo o Puesto: Jefe de TI Fecha: 28/03/2022

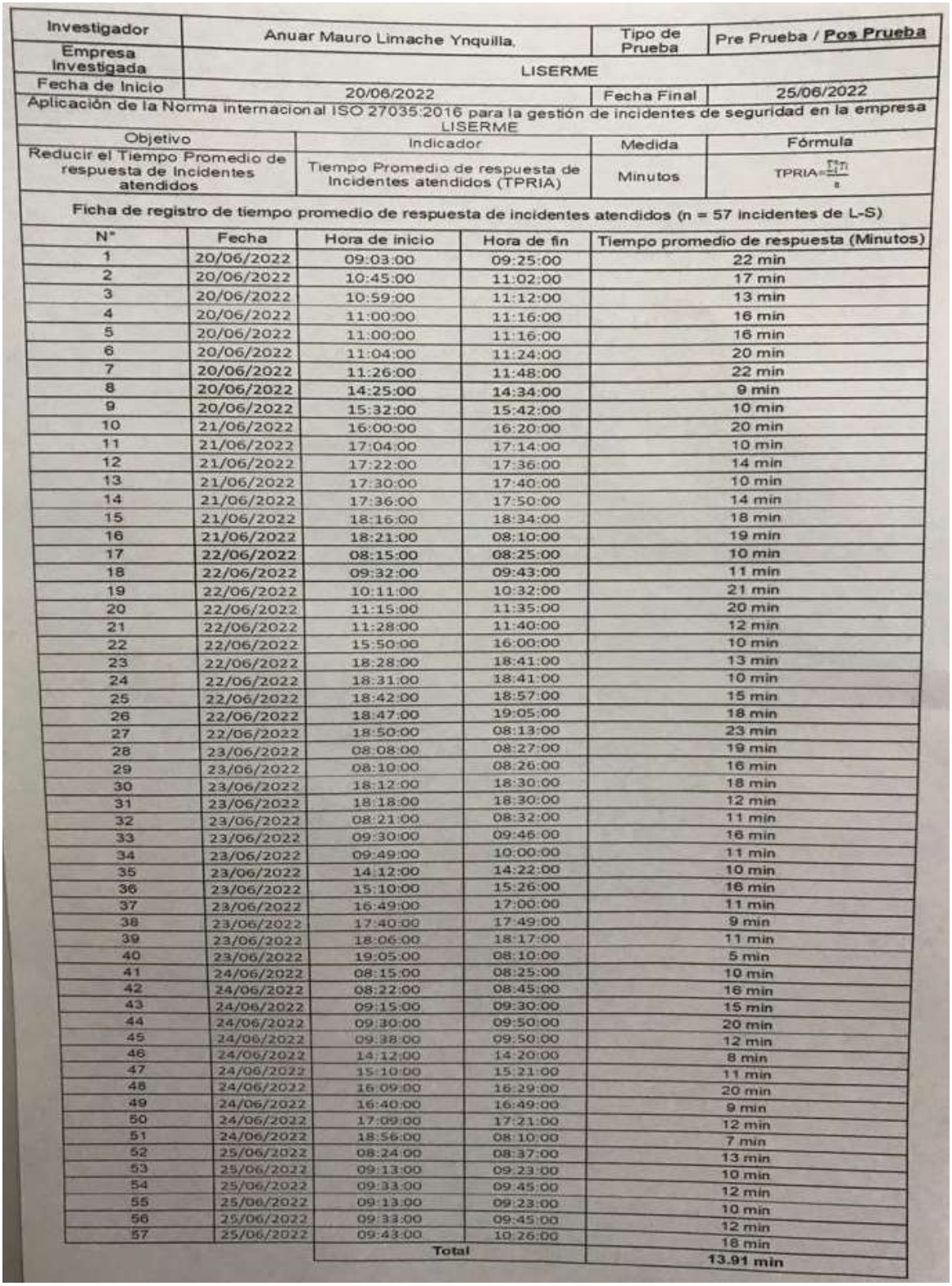
Variable	Definición Conceptual	Dimensión	Indicador	Escala de medición
V. Dependiente: Gestión de incidentes	ISO (2016) "Ejercicio de un enfoque coherente y eficaz para el manejo de incidentes de seguridad de la información"	Tiempo	Tiempo **Promedio** de respuesta de Incidentes atendidos	Razón
			Porcentaje de respuesta de incidentes atendidos	
			Porcentaje de reincidencia de incidentes	
		Personal de Área de TI	Nivel de satisfacción del personal	Ordinal

1. ¿Cuáles son las funciones principales del departamento de TI?
   Gestion y Mantenimiento de sistemas informaticos de la empresa, seguridad de la informacion y administracion de red
2. ¿Qué tipo de incidentes reportan los usuarios?
   Descofiguracion de programas, virus, perdida de datos, perdida servicio de Internet
3. ¿Existen una clasificación de incidentes?
   No existe
4. ¿Qué tipo de datos se almacenan cuando se reportan incidentes?
   No se almacenan
5. ¿Cuál es el promedio de incidentes reportados?
   10 incidentes por día
6. ¿Cuáles son los incidentes que suceden con frecuencia?
   Descofiguracion de programas, Virus, perdida servicio de Internet
7. ¿Manejan información que ayude identificar si el incidente ha sido tratado en el pasado?
   No
8. ¿Cómo considera usted en términos generales el proceso de gestión de incidentes?
   La gestion de incidentes es una herramienta necesaria para minimizar los impactos negativos en la empresa, pero el dialogo actualmente empleado
9. ¿Existen un registro del nivel de satisfacción en cuanto a la resolución de incidencias?
   No existen registros
10. ¿Actualmente cuentan con programas informáticos para el proceso de gestión de incidentes?
    Ninguno
11. ¿Actualmente se cuenta con políticas, procedimientos, mejores practicas para el proceso de gestión de incidentes?
    Ninguno
12. ¿Cree que es necesario implementar un sistema informático o implementar una norma (políticas, procedimientos, etc.) para el proceso de gestión de incidencias?
    No por el momento por costos un software de gestión es costoso. Si se podria implementar politicas procedimientos que ayuden a mejorar los procesos de help desk con tecnicos pre

Anexo 4B. Ficha de registro de tiempo promedio de respuesta de incidentes atendidos (Pre Prueba)

Investigador	Anuar Mauro Limache Ynquilla		Tipo de Prueba	**Pre Prueba** / Pos Prueba
Empresa Investigada	LISERME			
Fecha de Inicio	18/04/2022		Fecha Final	23/04/2022
Aplicación de la Norma internacional ISO 27035:2016 para la gestión de incidentes de seguridad en la empresa LISERME				
Objetivo	Indicador		Medida	Fórmula
Reducir el Tiempo Promedio de respuesta de Incidentes atendidos	Tiempo Promedio de respuesta de Incidentes atendidos (TPRIA)		Minutos	$TPRIA=\frac{\sum T}{n}$
Ficha de registro de tiempo promedio de respuesta de incidentes atendidos (n = 57 incidentes de L-S)				
N°	Fecha	Hora de inicio	Hora de fin	Tiempo promedio de respuesta (Minutos)
1	18/04/2022	08:11:00	08:40:00	29 min
2	18/04/2022	08:10:00	08:40:00	30 min
3	18/04/2022	09:11:00	09:42:00	31 min
4	18/04/2022	09:20:00	09:42:00	22 min
5	18/04/2022	10:20:00	10:38:00	18 min
6	18/04/2022	11:10:00	11:40:00	30 min
7	18/04/2022	18:26:00	09:20:00	114 min
8	18/04/2022	18:30:00	09:20:00	110 min
9	18/04/2022	18:34:00	18:57:00	23 min
10	18/04/2022	18:45:00	19:12:00	27 min
11	19/04/2022	08:00:00	08:48:00	48 min
12	19/04/2022	08:30:00	08:48:00	18 min
13	19/04/2022	09:03:00	09:27:00	24 min
14	19/04/2022	09:29:00	10:19:00	50 min
15	19/04/2022	10:10:00	11:41:00	91 min
16	19/04/2022	11:37:00	12:05:00	28 min
17	19/04/2022	15:16:00	15:53:00	37 min
18	19/04/2022	15:22:00	15:49:00	27 min
19	19/04/2022	15:28:00	16:15:00	47 min
20	19/04/2022	15:29:00	16:12:00	43 min
21	19/04/2022	15:30:00	15:53:00	23 min
22	19/04/2022	16:04:00	16:50:00	46 min
23	19/04/2022	16:18:00	16:47:00	29 min
24	19/04/2022	17:02:00	17:35:00	33 min
25	19/04/2022	17:08:00	17:35:00	27 min
26	19/04/2022	17:19:00	08:35:00	136 min
27	19/04/2022	18:20:00	08:30:00	70 min
28	20/04/2022	08:13:00	08:46:00	33 min
29	20/04/2022	10:09:00	11:06:00	57 min
30	20/04/2022	10:29:00	11:06:00	37 min
31	20/04/2022	14:19:00	14:52:00	33 min
32	20/04/2022	14:25:00	15:45:00	80 min
33	20/04/2022	15:03:00	15:25:00	22 min
34	20/04/2022	17:14:00	08:30:00	136 min
35	21/04/2022	08:29:00	08:55:00	26 min
36	21/04/2022	08:40:00	08:55:00	15 min
37	21/04/2022	09:10:00	09:45:00	35 min
38	21/04/2022	09:25:00	10:24:00	59 min
39	21/04/2022	10:46:00	11:09:00	23 min
40	21/04/2022	10:50:00	11:09:00	19 min
41	21/04/2022	11:00:00	11:37:00	37 min
42	21/04/2022	11:12:00	11:56:00	44 min
43	21/04/2022	16:55:00	17:29:00	34 min
44	21/04/2022	18:10:00	08:17:00	67 min
45	21/04/2022	18:14:00	18:50:00	36 min
46	21/04/2022	18:25:00	18:56:00	31 min
47	21/04/2022	18:36:00	08:55:00	79 min
48	22/04/2022	09:00:00	09:38:00	38 min
49	22/04/2022	09:20:00	09:38:00	18 min
50	22/04/2022	10:11:00	10:41:00	30 min
51	22/04/2022	11:15:00	11:54:00	39 min
52	22/04/2022	17:00:00	17:39:00	39 min
53	22/04/2022	18:20:00	08:37:00	77 min
54	23/04/2022	08:50:00	09:28:00	38 min
55	23/04/2022	09:19:00	10:36:00	77 min
56	23/04/2022	10:30:00	10:54:00	24 min
57	23/04/2022	11:15:00	11:43:00	28 min
		Total		44.25 min

Anexo 4B. Ficha de registro de tiempo promedio de respuesta de incidentes atendidos (Pos Prueba)



Investigador	Anuar Mauro Limache Ynquilla.	Tipo de Prueba	Pre Prueba / **Pos Prueba**
Empresa Investigada	LISERME		
Fecha de Inicio	20/06/2022	Fecha Final	25/06/2022

Aplicación de la Norma internacional ISO 27035:2016 para la gestión de incidentes de seguridad en la empresa LISERME

Objetivo	Indicador	Medida	Fórmula
Reducir el Tiempo Promedio de respuesta de Incidentes atendidos	Tiempo Promedio de respuesta de Incidentes atendidos (TPRIA)	Minutos	$TPRIA=\frac{\sum t_n}{n}$

Ficha de registro de tiempo promedio de respuesta de incidentes atendidos (n = 57 incidentes de L-S)

N°	Fecha	Hora de inicio	Hora de fin	Tiempo promedio de respuesta (Minutos)
1	20/06/2022	09:03:00	09:25:00	22 min
2	20/06/2022	10:45:00	11:02:00	17 min
3	20/06/2022	10:59:00	11:12:00	13 min
4	20/06/2022	11:00:00	11:16:00	16 min
5	20/06/2022	11:00:00	11:16:00	16 min
6	20/06/2022	11:04:00	11:24:00	20 min
7	20/06/2022	11:26:00	11:48:00	22 min
8	20/06/2022	14:25:00	14:34:00	9 min
9	20/06/2022	15:32:00	15:42:00	10 min
10	21/06/2022	16:00:00	16:20:00	20 min
11	21/06/2022	17:04:00	17:14:00	10 min
12	21/06/2022	17:22:00	17:36:00	14 min
13	21/06/2022	17:30:00	17:40:00	10 min
14	21/06/2022	17:36:00	17:50:00	14 min
15	21/06/2022	18:16:00	18:34:00	18 min
16	21/06/2022	18:21:00	08:10:00	19 min
17	22/06/2022	08:15:00	08:25:00	10 min
18	22/06/2022	09:32:00	09:43:00	11 min
19	22/06/2022	10:11:00	10:32:00	21 min
20	22/06/2022	11:15:00	11:35:00	20 min
21	22/06/2022	11:28:00	11:40:00	12 min
22	22/06/2022	15:50:00	16:00:00	10 min
23	22/06/2022	18:28:00	18:41:00	13 min
24	22/06/2022	18:31:00	18:41:00	10 min
25	22/06/2022	18:42:00	18:57:00	15 min
26	22/06/2022	18:47:00	19:05:00	18 min
27	22/06/2022	18:50:00	08:13:00	23 min
28	23/06/2022	08:08:00	08:27:00	19 min
29	23/06/2022	08:10:00	08:26:00	16 min
30	23/06/2022	18:12:00	18:30:00	18 min
31	23/06/2022	18:18:00	18:30:00	12 min
32	23/06/2022	08:21:00	08:32:00	11 min
33	23/06/2022	09:30:00	09:46:00	16 min
34	23/06/2022	09:49:00	10:00:00	11 min
35	23/06/2022	14:12:00	14:22:00	10 min
36	23/06/2022	15:10:00	15:26:00	16 min
37	23/06/2022	16:49:00	17:00:00	11 min
38	23/06/2022	17:40:00	17:49:00	9 min
39	23/06/2022	18:06:00	18:17:00	11 min
40	23/06/2022	19:05:00	08:10:00	5 min
41	24/06/2022	08:15:00	08:25:00	10 min
42	24/06/2022	08:22:00	08:45:00	16 min
43	24/06/2022	09:15:00	09:30:00	15 min
44	24/06/2022	09:30:00	09:50:00	20 min
45	24/06/2022	09:38:00	09:50:00	12 min
46	24/06/2022	14:12:00	14:20:00	8 min
47	24/06/2022	15:10:00	15:21:00	11 min
48	24/06/2022	16:09:00	16:29:00	20 min
49	24/06/2022	16:40:00	16:49:00	9 min
50	24/06/2022	17:09:00	17:21:00	12 min
51	24/06/2022	18:56:00	08:10:00	7 min
52	25/06/2022	08:24:00	08:37:00	13 min
53	25/06/2022	09:13:00	09:23:00	10 min
54	25/06/2022	09:33:00	09:45:00	12 min
55	25/06/2022	09:13:00	09:23:00	10 min
56	25/06/2022	09:33:00	09:45:00	12 min
57	25/06/2022	09:43:00	10:26:00	18 min
		Total		13.91 min

ANTES	DESPUÉS	DIF	REDUCCIÓN (%)
44.25 min	13.91 min	30.33 min	68.56%

Anexo 4C. Ficha de registro de porcentaje de respuesta de incidentes atendidos (Pre Prueba)

Investigador	Anuar Mauro Limache Ynquilla	Tipo de Prueba	**Pre Prueba** / Pos Prueba
Empresa Investigada	LISERME		
Fecha de Inicio	18/04/2022	Fecha Final	23/04/2022

Aplicación de la Norma internacional ISO 27035:2016 para la gestión de incidentes de seguridad en la empresa LISERME

Objetivo	Indicador	Medida	Fórmula
Incrementar el porcentaje de respuesta de incidentes atendidos	Porcentaje de respuesta de incidentes atendidos (PRIA)	Diario	$PRIA=\frac{TRIA \times 100}{TIR}$

Ficha de registro porcentaje de respuesta de incidentes atendidos (n = 6 reportes)

N°	Fecha	Porcentaje de respuesta de incidentes atendidos (Diario)
1	18/04/2022	80.00%
2	19/04/2022	88.24%
3	20/04/2022	85.71%
4	21/04/2022	84.62%
5	22/04/2022	83.33%
6	23/04/2022	57.14%
	Porcentaje	**79.84%**

Anexo 4C. Ficha de registro de porcentaje de respuesta de incidentes atendidos (Pos Prueba)

Investigador	Anuar Mauro Limache Ynquilla	Tipo de Prueba	Pre Prueba / **Pos Prueba**
Empresa Investigada	LISERME		
Fecha de Inicio	20/06/2022	Fecha Final	26/06/2022

Aplicación de la Norma internacional ISO 27035:2016 para la gestión de incidentes de seguridad en la empresa LISERME

Objetivo	Indicador	Medida	Fórmula
Incrementar el porcentaje de respuesta de incidentes atendidos	Porcentaje de respuesta de incidentes atendidos (PRIA)	Diario	$PRIA=\frac{TRIA \times 100}{TIR}$

Ficha de registro porcentaje de respuesta de incidentes atendidos (n = 6 reportes)

N°	Fecha	Porcentaje de respuesta de incidentes atendidos (Diario)
1	20/06/2022	100.00%
2	21/06/2022	85.71%
3	22/06/2022	90.91%
4	23/06/2022	92.31%
5	24/06/2022	100.00%
6	25/06/2022	100.00%
	Porcentaje	**94.82%**

ANTES	DESPUÉS	DIF
79.84%	94.82%	14.98%

Anexo 4D. Ficha de registro de porcentaje de reincidencia de incidentes (Pre Prueba)

Investigador	Anuar Mauro Limache Ynquilla	Tipo de Prueba	**Pre Prueba** / Pos Prueba
Empresa Investigada	LISERME		
Fecha de Inicio	18/04/2022	Fecha Final	23/04/2022

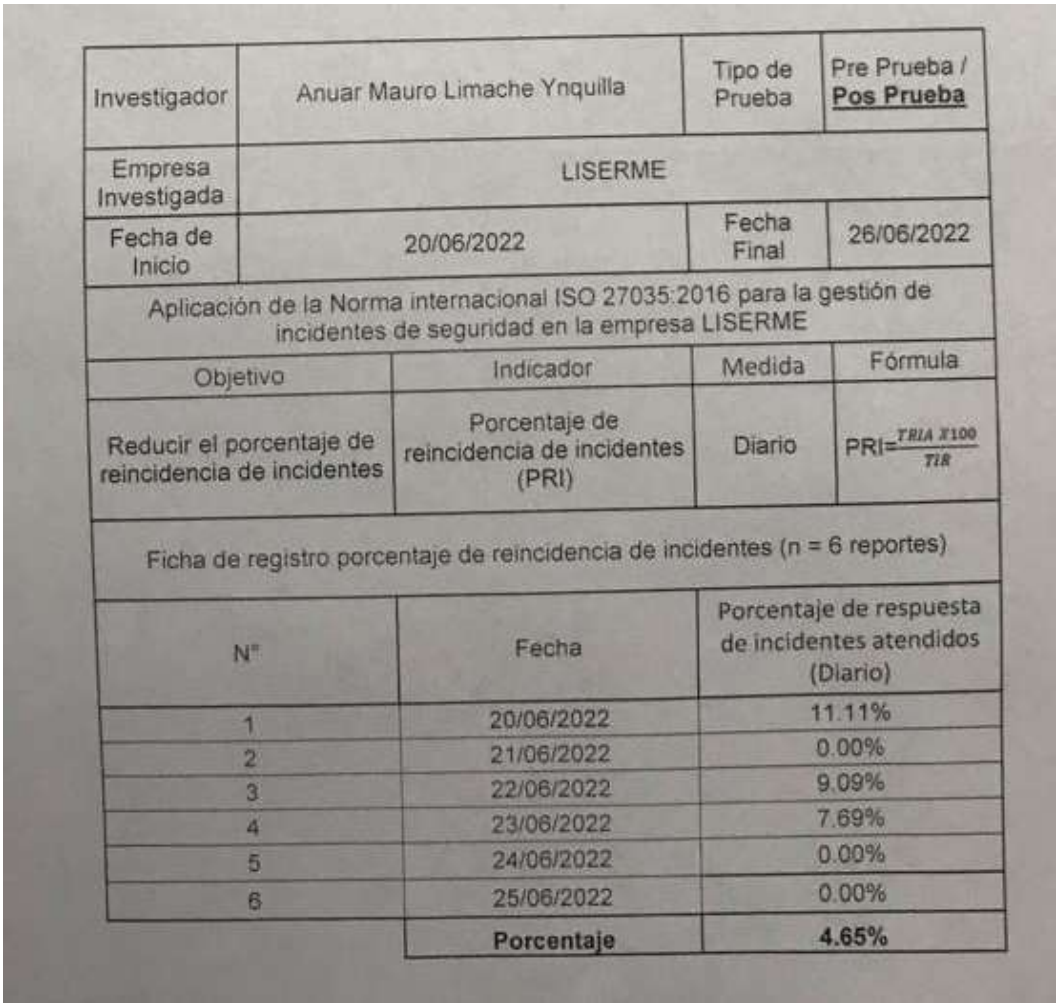
Aplicación de la Norma internacional ISO 27035.2016 para la gestión de incidentes de seguridad en la empresa LISERME

Objetivo	Indicador	Medida	Fórmula
Reducir el porcentaje de reincidencia de incidentes	Porcentaje de reincidencia de incidentes (PRI)	Diario	$PRI=\frac{TRIA\ X100}{TIR}$

Ficha de registro porcentaje de reincidencia de incidentes (n = 6 reportes)

N°	Fecha	Porcentaje de respuesta de incidentes atendidos (Diario)
1	18/04/2022	30.00%
2	19/04/2022	17.65%
3	20/04/2022	14.29%
4	21/04/2022	15.38%
5	22/04/2022	16.67%
6	23/04/2022	28.57%
	Porcentaje	**20.43%**

Anexo 4D. Ficha de registro de porcentaje de reincidencia de incidentes (Pos Prueba)



Investigador	Anuar Mauro Limache Ynquilla	Tipo de Prueba	Pre Prueba / **Pos Prueba**
Empresa Investigada	LISERME		
Fecha de Inicio	20/06/2022	Fecha Final	26/06/2022

Aplicación de la Norma internacional ISO 27035:2016 para la gestión de incidentes de seguridad en la empresa LISERME

Objetivo	Indicador	Medida	Fórmula
Reducir el porcentaje de reincidencia de incidentes	Porcentaje de reincidencia de incidentes (PRI)	Diario	$PRI=\frac{TRIA\ X100}{TIR}$

Ficha de registro porcentaje de reincidencia de incidentes (n = 6 reportes)

N°	Fecha	Porcentaje de respuesta de incidentes atendidos (Diario)
1	20/06/2022	11.11%
2	21/06/2022	0.00%
3	22/06/2022	9.09%
4	23/06/2022	7.69%
5	24/06/2022	0.00%
6	25/06/2022	0.00%
	Porcentaje	**4.65%**

ANTES	DESPUÉS	DIF
20.43%	4.65%	15.78%

Anexo 4E. Cuestionario aplicado al del Área de TI de la empresa LISERME (Pre Prueba)

Cuestionario aplicado al personal del área de TI de la empresa LISERME (Pre Prueba)

A continuación, se presenta una lista de preguntas contenidas en nueve (9) ítems que corresponden a la percepción de la gestión de incidentes por parte del personal del área de TI.

Cuestionario aplicado para conocer el nivel de satisfacción del personal de TI (n = 3 personas)

1	2	3	4	5
Deficiente	Malo	Regular	Bueno	Excelente

Ítem	Preguntas	Deficiente 1	Malo 2	Regular 3	Bueno 4	Excelente 5	Total	Promedio Pre Prueba
1	Bajo su experiencia, ¿Está satisfecho con la manera de resolver los problemas de sistemas actuales?	0	0	3	0	0	9	3.00
2	¿Qué tan satisfecho está usted con la calidad general del servicio?	0	2	1	0	0	7	2.33
3	¿Cómo califica el nivel de gestión de incidentes?	2	1	0	0	0	4	1.33
4	¿Cómo calificaría la confiabilidad de los incidentes reportados?	2	1	0	0	0	4	1.33
5	¿Cómo calificaría el tiempo que invierte en los informes diarios sobre los incidentes presentados?	2	0	1	0	0	5	1.67
6	¿Considera usted que existe los suficientes procedimientos para resolver los incidentes reportados?	3	0	0	0	0	3	1.00
7	¿Qué tan satisfecho está usted con la tasa de reincidencia?	3	0	0	0	0	3	1.00
8	¿Cómo calificaría las herramientas que utiliza para resolver su trabajo?	2	0	1	0	0	5	1.67
9	¿Cómo calificaría el tiempo dedicado para hacer frente a los incidentes?	2	1	0	0	0	4	1.33

Anexo 4E. Cuestionario aplicado al del Área de TI de la empresa LISERME (Pos Prueba)

Cuestionario aplicado al personal del área de TI de la empresa LISERME (Pos Prueba)

A continuación, se presenta una lista de preguntas contenidas en nueve (9) ítems que corresponden a la percepción de la gestión de incidentes por parte del personal del área de TI.

Cuestionario aplicado para conocer el nivel de satisfacción del personal de TI (n = 3 personas)

1	2	3	4	5
Deficiente	Malo	Regular	Bueno	Excelente

Ítem	Preguntas	Deficiente 1	Malo 2	Regular 3	Bueno 4	Excelente 5	Total	Promedio Pos Prueba
1	Bajo su experiencia, ¿Está satisfecho con la manera de resolver los problemas de sistemas actuales?	0	0	0	0	3	15	5.00
2	¿Qué tan satisfecho está usted con la calidad general del servicio?	0	0	0	2	1	13	4.33
3	¿Cómo califica el nivel de gestión de incidentes?	0	0	0	2	1	13	4.33
4	¿Cómo calificaría la confiabilidad de los incidentes reportados?	0	0	0	2	1	13	4.33
5	¿Cómo calificaría el tiempo que invierte en los informes diarios sobre los incidentes presentados?	0	0	0	2	1	13	4.33
6	¿Considera usted que existe los suficientes procedimientos para resolver los incidentes reportados?	0	0	0	3	0	12	4.00
7	¿Qué tan satisfecho está usted con la tasa de reincidencia?	0	0	0	3	0	12	4.00
8	¿Cómo calificaría las herramientas que utiliza para resolver su trabajo?	0	0	0	2	1	13	4.33
9	¿Cómo calificaría el tiempo dedicado para hacer frente a los incidentes?	0	0	0	2	1	13	4.33

Nivel de satisfacción del personal del área de TI Pre Prueba			**Nivel de satisfacción del personal del área de TI Pre Prueba**			**Nivel de impacto de la satisfacción del personal**	
Promedio (1 - 5)	**Promedio (%)**	**Nivel**	**Promedio (1 - 5)**	**Promedio (%)**	**Nivel**	**DIF**	**Promedio (%)**
1.63	32.59%	Malo	4.33	86.67%	Excelente	2.70	54.07%

Anexos 5. Validación de instrumentos de recolección de datos

Validación de instrumentos de recolección de datos

Señor(a)(ita): Dr. Agreda Gamboa, Everson David

Asunto: Validación de instrumentos a través de juicio de experto

Es muy grato dirigirme a Usted para expresarle saludos cordiales y, asimismo, hacer de su conocimiento que, siendo estudiante de la carrera profesional de Ingeniería de sistemas de la Universidad César Vallejo, semestre 2022-0 y, siendo requisito la validación de los instrumentos con los cuales recogeré la información necesaria para desarrollar mi investigación, gracias a la cual optaré el título profesional.

El título de mi proyecto de investigación es “Aplicación de la Norma internacional ISO 27035:2016 para la Gestión de incidentes de seguridad en una Empresa de seguridad y resguardo, Arequipa 2022”, siendo imprescindible contar con la aprobación de docentes especializados para poder aplicar los instrumentos en mención, he considerado conveniente recurrir a usted, ante su connotada experiencia.

El expediente de validación, adjunto al presente, contiene:

- Matriz de consistencia.
- Matriz de operacionalización de variables.
- Instrumento de evaluación.
- Hoja de validación del instrumento.

Reiterando mis sentimientos de respeto y consideración me despido de Usted, no sin antes agradecerle por la atención que dispense a la presente.

Atentamente,

Anuar Limache Ynquilla

DNI: 43983633

Hoja de validación del instrumento

I. Datos generales:

Nombre del instrumento a evaluar: Cuestionario

II. Instrucciones:
En el siguiente cuadro, para cada ítem del contenido del instrumento que revisa, marque usted con un check (√) o un aspa (X) la opción SÍ o NO que elija según el criterio de *Claridad, Pertinencia o Relevancia.*

Dimensión / Indicadores	Ítem	Claridad		Pertinencia		Relevancia		Observaciones
		SI	NO	SI	NO	SI	NO	
Personal / Nivel de satisfacción del personal de TI	Bajo su experiencia, ¿Está satisfecho con la manera de resolver los problemas de sistemas actuales?	√		√		√		
	¿Qué tan satisfecho está usted con la calidad general del servicio?	√		√		√		
	¿Cómo califica el nivel de gestión de incidentes?	√		√		√		
	¿Cómo calificaría la confiabilidad de los incidentes reportados?	√		√		√		
	¿Cómo calificaría el tiempo que invierte en los informes diarios sobre los incidentes presentados?	√		√		√		
	¿Considera usted que existe los suficientes procedimientos para resolver los incidentes reportados?	√		√		√		
	¿Qué tan satisfecho está usted con la tasa de reincidencia?	√		√		√		
	¿Cómo calificaría las herramientas que utiliza para resolver su trabajo?	√		√		√		
	¿Cómo calificaría el tiempo dedicado para hacer frente a los incidentes?	√		√		√		

Nota: Los ítems fueron tomados de la matriz de operacionalización

[1]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

[2]**Pertinencia:** Si el ítem pertenece a la dimensión.

[3]**Relevancia:** El ítem es apropiado para representar a la dimensión específica del constructo.

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

Observaciones	
Opinión de aplicabilidad Aplicable [√] Aplicable después de corregir [ ] No aplicable [ ]	
Apellidos y nombres del juez evaluador	Dr. Agreda Gamboa, Everson David
Título profesional y/o Grado académico	Ingeniero de Sistemas / Doctor
 **DNI: 18161457**	**Arequipa, 16 de abril 2022**

Validación de instrumentos de recolección de datos

Señor(a)(ita): Gómez Ávila, José Alberto
Asunto: Validación de instrumentos a través de juicio de experto

Es muy grato dirigirme a Usted para expresarle saludos cordiales y, asimismo, hacer de su conocimiento que, siendo estudiante de la carrera profesional de Ingeniería de sistemas de la Universidad César Vallejo, semestre 2022-0 y, siendo requisito la validación de los instrumentos con3los cuales recogeré la información necesaria para desarrollar mi investigación, gracias a la cual optaré el título profesional.

El título de mi proyecto de investigación es “Aplicación de la Norma internacional ISO 27035:2016 para la Gestión de incidentes de seguridad en una Empresa de seguridad y resguardo, Arequipa 2022”, siendo imprescindible contar con la aprobación de docentes especializados para poder aplicar los instrumentos en mención, he considerado conveniente recurrir a usted, ante su connotada experiencia.

El expediente de validación, adjunto al presente, contiene:

- Matriz de consistencia.
- Matriz de operacionalización de variables.
- Instrumento de evaluación.
- Hoja de validación del instrumento.

Reiterando mis sentimientos de respeto y consideración me despido de Usted, no sin antes agradecerle por la atención que dispense a la presente.

Atentamente,

Anuar Limache Ynquilla

DNI: 43983633

Hoja de validación del instrumento

I. Datos generales:

Nombre del instrumento a evaluar: Cuestionario

II. Instrucciones:
En el siguiente cuadro, para cada ítem del contenido del instrumento que revisa, marque usted con un check (√) o un aspa (X) la opción SÍ o NO que elija según el criterio de *Claridad, Pertinencia o Relevancia.*

Dimensión / Indicadores	Ítem	Claridad		Pertinencia		Relevancia		Observaciones
		SI	NO	SI	NO	SI	NO	
Personal / Nivel de satisfacción del personal de TI	Bajo su experiencia, ¿Está satisfecho con la manera de resolver los problemas de sistemas actuales?	√		√		√		
	¿Qué tan satisfecho está usted con la calidad general del servicio?	√		√		√		
	¿Cómo califica el nivel de gestión de incidentes?	√		√		√		
	¿Cómo calificaría la confiabilidad de los incidentes reportados?	√		√		√		
	¿Cómo calificaría el tiempo que invierte en los informes diarios sobre los incidentes presentados?	√		√		√		
	¿Considera usted que existe los suficientes procedimientos para resolver los incidentes reportados?	√		√		√		
	¿Qué tan satisfecho está usted con la tasa de reincidencia?	√		√		√		
	¿Cómo calificaría las herramientas que utiliza para resolver su trabajo?	√		√		√		
	¿Cómo calificaría el tiempo dedicado para hacer frente a los incidentes?	√		√		√		

Nota: Los ítems fueron tomados de la matriz de operacionalización

[1] **Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

[2] **Pertinencia:** Si el ítem pertenece a la dimensión.

[3] **Relevancia:** El ítem es apropiado para representar a la dimensión específica del constructo.

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

Observaciones	
Opinión de aplicabilidad Aplicable [√] Aplicable después de corregir [ ] No aplicable [ ]	
Apellidos y nombres del juez evaluador	Gómez Ávila, José Alberto
Título profesional y/o Grado académico	Ingeniero de Sistemas / Doctor
 **DNI:** 40990648	**Arequipa, 16 de abril 2022**

Validación de instrumentos de recolección de datos

Señor(a)(ita): Córdova Otero, Juan Luis
Asunto: Validación de instrumentos a través de juicio de experto

Es muy grato dirigirme a Usted para expresarle saludos cordiales y, asimismo, hacer de su conocimiento que, siendo estudiante de la carrera profesional de Ingeniería de sistemas de la Universidad César Vallejo, semestre 2022-0 y, siendo requisito la validación de los instrumentos con los cuales recogeré la información necesaria para desarrollar mi investigación, gracias a la cual optaré el título profesional.

El título de mi proyecto de investigación es "Aplicación de la Norma internacional ISO 27035:2016 para la Gestión de incidentes de seguridad en una Empresa de seguridad y resguardo, Arequipa 2022", siendo imprescindible contar con la aprobación de docentes especializados para poder aplicar los instrumentos en mención, he considerado conveniente recurrir a usted, ante su connotada experiencia.

El expediente de validación, adjunto al presente, contiene:

- Matriz de consistencia.
- Matriz de operacionalización de variables.
- Instrumento de evaluación.
- Hoja de validación del instrumento.

Reiterando mis sentimientos de respeto y consideración me despido de Usted, no sin antes agradecerle por la atención que dispense a la presente.

Atentamente,

Anuar Limache Ynquilla

DNI: 43983633

Hoja de validación del instrumento

I. Datos generales:

Nombre del instrumento a evaluar: Cuestionario

II. Instrucciones:
En el siguiente cuadro, para cada ítem del contenido del instrumento que revisa, marque usted con un check (√) o un aspa (X) la opción SÍ o NO que elija según el criterio de *Claridad, Pertinencia o Relevancia.*

Dimensión / Indicadores	Ítem	Claridad		Pertinencia		Relevancia		Observaciones
		SI	NO	SI	NO	SI	NO	
Personal / Nivel de satisfacción del personal de TI	Bajo su experiencia, ¿Está satisfecho con la manera de resolver los problemas de sistemas actuales?	√		√		√		
	¿Qué tan satisfecho está usted con la calidad general del servicio?	√		√		√		
	¿Cómo califica el nivel de gestión de incidentes?	√		√		√		
	¿Cómo calificaría la confiabilidad de los incidentes reportados?	√		√		√		
	¿Cómo calificaría el tiempo que invierte en los informes diarios sobre los incidentes presentados?	√		√		√		
	¿Considera usted que existe los suficientes procedimientos para resolver los incidentes reportados?	√		√		√		
	¿Qué tan satisfecho está usted con la tasa de reincidencia?	√		√		√		
	¿Cómo calificaría las herramientas que utiliza para resolver su trabajo?	√		√		√		
	¿Cómo calificaría el tiempo dedicado para hacer frente a los incidentes?	√		√		√		

Nota: Los ítems fueron tomados de la matriz de operacionalización

[1]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

[2]**Pertinencia:** Si el ítem pertenece a la dimensión.

[3]**Relevancia:** El ítem es apropiado para representar a la dimensión específica del constructo.

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

Observaciones	
Opinión de aplicabilidad Aplicable [√] Aplicable después de corregir [ ] No aplicable [ ]	
Apellidos y nombres del juez evaluador	Córdova Otero, Juan Luis
Especialidad del evaluador	Ing. Computación y Sistemas / Maestro
 **DNI: 18122765** **Arequipa, 16 de abril 2022**	

Anexos 6. Desarrollo de la solución

El Desarrollo de la aplicación de la norma ISO 27035:2016 permitirá que haya una gestión de incidentes de seguridad de información logrando obtener una gestión adecuada para el cumplimiento de cada uno de los objetivos planteados en la investigación.

1. Objetivo

Los objetivos más específicos de un enfoque estructurado y bien planificado para la gestión de incidentes deben incluir el seguimiento:

a) Los eventos de seguridad de la información se detectan y tratan de manera eficiente, en particular, decidiendo cuándo deben clasificarse como incidentes de seguridad de la información;
b) Los incidentes de seguridad de la información identificados se evalúan y responden de la manera más adecuada y eficiente;
c) Los efectos adversos de los incidentes de seguridad de la información en la organización y sus operaciones se minimizan mediante controles apropiados como parte de la respuesta a incidentes;
d) Se establece un vínculo con elementos relevantes de la gestión de crisis y la gestión de la continuidad del negocio a través de un proceso de escalamiento;
e) Las vulnerabilidades de la seguridad de la información se evalúan y tratan adecuadamente para prevenir o reducir incidentes. Esta evaluación puede realizarla el IRT u otros equipos dentro de la organización, según la distribución de tareas;
f) Las lecciones se aprenden rápidamente de los incidentes de seguridad de la información, las vulnerabilidades y su gestión. Este mecanismo de retroalimentación tiene como objetivo aumentar las posibilidades de evitar que ocurran futuros incidentes de seguridad de la información, mejorar la implementación y el uso de los controles de seguridad de la información y mejorar el plan general de gestión de identidades de seguridad de la información.

2. Identificación de la situación actual de la gestión de incidentes

La respuesta a incidentes actualmente en la empresa, presenta documentación de poca importancia o nula donde no existen procedimientos ni políticas que puedan ayudar a una correcta respuesta ante incidentes de seguridad de la información y se resuelven de forma empírica en su mayoría de ocasiones al ser estos incidentes notados principalmente cuando el personal cree que pueda afectar a la empresa económicamente, la reacción a tales incidentes debe basarse, en la medida de lo posible o práctico, en planes de respuesta a incidentes documentados, que son revisados, probados y practicados regularmente por quienes tienen que estar capacitados. La ocurrencia de un incidente real de tal emergencia no es el momento de dejarlo pasar o seguir una documentación que, si esta no la revisan, está desactualizada y se refiere a procesos o sistemas que han cambiado mucho o que ya no se usan.

La detección y el análisis de incidentes serían fáciles si se tendría la norma ISO 27035:2016, pero en estos momentos para la empresa no cuenta. Los indicadores proporcionados por el usuario, como una queja de que un servicio no está disponible, a menudo son incorrectos. Los sistemas de detección de intrusos pueden producir indicadores incorrectos.

Incluso si un indicador es preciso, no significa necesariamente que haya ocurrido un incidente. Algunos indicadores, como un bloqueo de un usuario o la modificación de archivos críticos, pueden ocurrir por varias razones además de un incidente de seguridad, incluido un error humano. Sin embargo, dada la ocurrencia de indicadores, es razonable sospechar que podría estar ocurriendo un incidente. Ante un incidente deberá ser manejarse de la misma manera, independientemente de si está relacionada con la seguridad.

3. Metodología de gestión de incidentes ISO 27035:2016

Para la implementación de la norma ISO 270035, se dividirá en cinco fases, como se referencia en la norma. Estas fases ayudarán a cumplir los objetivos declarados de la norma.

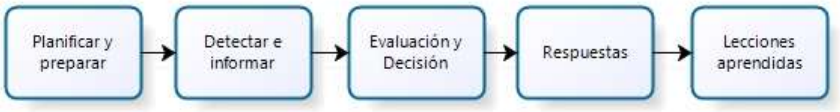


Figura: Fuente propia

1. **Planificar y preparar**

Los incidentes de seguridad de la información deben gestionarse de manera eficaz, lo que requiere una planificación y una preparación cuidadosas. La empresa realiza varias tareas de planificación previa para implementar un plan eficaz de gestión de incidentes de seguridad de la información, que incluyen:

a) Política de respuesta ante incidentes y se cuenta con el compromiso del personal de empresa, Ver Anexo 11.
b) Actualización de las políticas de seguridad de la información.
c) Política de la seguridad de la información, Ver Anexo 12.
d) Establecimiento del IRT, Ver Anexo 13.
e) Establecimiento y preservación de relaciones y conexiones apropiadas con empresas internas y externas que estén directamente involucradas en la gestión de incidentes.
f) Establecer, implementar y operar mecanismos técnicos, organizativos y operativos para apoyar el plan de gestión de incidentes de seguridad de la información y el trabajo del IRT. Desarrollar e implementar los sistemas de información necesarios para respaldar el IRT, incluida una base de datos de seguridad de la información.
g) Diseñar y desarrollar un programa de concientización y capacitación.
h) Probar el uso del plan de gestión de incidentes de seguridad de la información, sus procesos y procedimientos.

2. **Detectar e informar**

En esta fase implica la identificación de eventos de seguridad de la información y la existencia de vulnerabilidades de seguridad de la información mediante técnicas manuales o automatizadas, así como la recopilación y notificación de la información correspondiente, Es posible que

los eventos y las vulnerabilidades aún no se consideren incidentes de seguridad de la información en este momento. La capacidad de enviar eventos de seguridad de acuerdo con las pautas de informes de la organización permite un análisis adicional, si es necesario.

La empresa lleva a cabo las acciones cruciales que se enumeran a continuación para la fase de Detección e informar:

a) Se supervisa y registra las actividades del sistema de la empresa.
b) Se detecta y reporta la ocurrencia de un evento de seguridad de la información, ya sea de forma manual por parte del personal o de forma automática.
c) Se recopila información sobre un evento o vulnerabilidad de seguridad de la información.
d) Se recopila información de conciencia situacional de fuentes de datos internas y externas.
e) Se Asegura de que todas las actividades, resultados y decisiones relacionadas se registren correctamente para su posterior análisis.
f) Se asegura que la evidencia se recopile y almacene de manera segura.
g) Se garantiza que se mantenga actualizada la base de datos de seguridad de la información.
h) Se escala, según sea necesario a lo largo de la fase, para una mayor revisión o decisiones.

3. Evaluación y Decisión

La revisión de los datos relacionados con la ocurrencia de eventos de seguridad de la información y la elección de etiquetar las ocurrencias como incidentes de seguridad de la información son parte de la tercera fase de la gestión de incidentes de seguridad de la información. Se deben tomar las siguientes acciones si se descubre e informa un evento de seguridad de la información:

a) Se distribuye la responsabilidad de las actividades de gestión de incidentes de seguridad de la información que involucren tanto al personal de seguridad como al personal que no es de seguridad.

b) Se proporciona procedimientos que debe seguir cada empleado, las acciones individuales dependerán del tipo y la gravedad del incidente.

- Impacto: Es el daño que causa en la empresa.
- Urgencia: La velocidad que la empresa necesita solucionar el posible problema ocasionado por el incidente.

		Impacto			
		Critico	Alto	Medio	Bajo
Urgencia	Critico				
	Alto				
	Medio				
	Bajo				

Tabla Fuente propia

c) Se utiliza las pautas de la documentación existente si el evento de seguridad de la información se clasifica como un incidente de seguridad de la información.
d) Se recopila información que puede incluir pruebas, mediciones y otra recopilación de datos sobre la detección de un evento de seguridad de la información.
e) Realizar una evaluación por parte del manejador de incidentes para determinar si el evento es un incidente de seguridad de la información posible o confirmado o una falsa alarma.
f) Asegurarse que se registren correctamente todas las actividades, resultados y decisiones relacionadas para su posterior análisis en particular el IRT.
g) Se asegura que se mantenga el régimen de control de cambios para mantener actualizada la base de datos de seguridad de la información.

4. Respuestas

La cuarta etapa incluye responder antes los incidentes de seguridad de la información acuerdo con las actividades decididas en la etapa anterior. Dependiendo de las opciones, las reacciones se pueden dar instantáneamente, en tiempo real o casi en tiempo real, algunas reacciones pueden incluir una investigación. Una vez que se ha confirmado un incidente

de seguridad de datos y se han decidido las respuestas, se deben seguir las siguientes actividades:

a) Distribuir la responsabilidad de las actividades de gestión de incidentes de seguridad de la información a través de una jerarquía adecuada de personal con toma de decisiones y acciones según sea necesario.
b) Proporcione procedimientos formales para que siga cada persona involucrada, incluida la revisión y modificación de los informes, la reevaluación de los daños y la notificación al personal pertinente. Las acciones individuales dependerán del tipo y la gravedad del incidente;
c) Use pautas para la documentación de un incidente de seguridad de la información y sus acciones posteriores.
d) Investigar incidentes según sea necesario y en relación con la calificación de la escala de clasificación de incidentes de seguridad de la información.
e) Revisión por parte del IRT para determinar si el incidente de seguridad de la información está bajo control y, de ser así, realizar la respuesta requerida.
f) Asignar recursos internos e identificar recursos externos para responder a un incidente.
g) Escalar según sea necesario a lo largo de la fase para evaluaciones o decisiones adicionales.
h) Asegurar que todas las partes involucradas, particularmente el IRT, registren correctamente todas las actividades para su posterior análisis.
i) Garantizar que las pruebas digitales se recopilen y almacenen de manera comprobablemente segura.
j) Asegúrese de que se mantenga el régimen de control de cambios para cubrir el seguimiento de incidentes de seguridad de la información y sus actualizaciones.
k) Comunicar la existencia del incidente de seguridad de la información y compartir cualquier detalle relevante de acuerdo con los planes de comunicación organizacionales. Notificar a los propietarios de los activos, proveedores de servicios de Internet y organizaciones de intercambio de información que podrían ayudar con la gestión y

resolución de problemas ocasionados por los incidentes presentados. Compartir información de los incidentes presentados, ya que las mismas amenazas y ataques a menudo afectan a varias empresas.

l) Después de la recuperación de un incidente, se debe iniciar una actividad posterior al incidente según la naturaleza y la gravedad del incidente. Esta actividad incluye;

   1) Investigación de la información relativa al incidente.
   2) Investigación de otras fuentes relevantes, como el personal involucrado.
   3) Informe resumido de los resultados de la investigación.

m) Una vez que se ha resuelto el incidente, debe cerrarse de acuerdo con los requisitos del IRT o de la empresa y se debe notificar a todas las partes interesadas.

5. Lecciones aprendidas

Cuando se han manejado los eventos de seguridad de la información, el proceso de gestión de incidentes de seguridad de la información entra en su quinta fase. El objetivo de esta fase es aprender del manejo de incidentes y vulnerabilidades. La empresa debe llevar a cabo las acciones cruciales que se enumeran a continuación para la fase de lecciones aprendidas:

a) Identificar las lecciones aprendidas de los incidentes y vulnerabilidades de seguridad de la información.
b) Revisar, identificar y realizar mejoras en la implementación de controles de seguridad de la información controles nuevos o actualizados, así como la política de gestión de incidentes de seguridad de la información.
c) Revisar, identificar y realizar mejoras en la evaluación de riesgos de seguridad de la información.
d) Revisar qué tan efectivos fueron los procesos, procedimientos, para responder, evaluar y recuperarse de incidentes de seguridad de la información. Sobre la base de las lecciones aprendidas, identificar y realizar mejoras en el incidente de seguridad de la información.

e) Comunicar y compartir los resultados de la revisión dentro de la empresa si se requiera;
f) Determinar si la información del incidente, los vectores de ataque asociados y las vulnerabilidades se pueden compartir con las empresas asociadas.
g) Realizar una evaluación integral del desempeño y la eficacia de IRT de forma periódica.

Anexos 7. Tabla de datos

Análisis de datos Pre Prueba - satisfacción del personal del área de TI

N°	01	02	03	04	05	06	07	08	09
Persona 01	3	2	1	1	1	1	1	1	1
Persona 02	3	2	1	1	1	1	1	1	1
Persona 03	3	3	2	2	3	1	1	3	2

Tabla Fuente propia

Análisis de datos Post Prueba - satisfacción del personal del área de TI

N°	01	02	03	04	05	06	07	08	09
Persona 01	**5**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**
Persona 02	**5**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**
Persona 03	**5**	**5**	**5**	**5**	**5**	**4**	**4**	**5**	**5**

Tabla Fuente propia

Anexos 8 Confiabilidad de los instrumentos de recolección de datos

Análisis de confiabilidad de los instrumentos de datos pre prueba

Tabla 21. Análisis de confiabilidad pre prueba

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
.914	9

Fuente: IBM *SPSS Statistics v.28*

Para poder establecer la confiabilidad de los instrumentos de recolección de datos se utilizó el software estadístico IBM SSPS Statistics v.28, en la tabla anterior se muestra el estadístico Alfa de CronBach que es de 0.914 que es mayor a 0.67 por consiguiente se puede interpretar que el instrumento de medición es excelente.

Análisis de confiabilidad de los instrumentos de datos pos prueba

Tabla 22. Análisis de confiabilidad pos prueba

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
.937	9

Fuente: IBM *SPSS Statistics v.28*

Para poder establecer la confiabilidad de los instrumentos de recolección de datos se utilizó el software estadístico SSPS Statistics v.28, en la tabla anterior se muestra el estadístico Alfa de CronBach que es de 0.937 que es mayor a 0.67 por consiguiente se puede interpretar que el instrumento de medición es excelente.

Anexos 9 Carta de autorización de aplicación de instrumentos

LISERME S.R.L.

Especialista En Fabricación De Productos Metálicos Para Uso Estructural

"Año del Bicentenario del Congreso de la República del Perú"

Arequipa, 27 de Marzo del 2022

CARTA N° 001-2022-LISERME

SRES

UNIVERSIDAD CESAR VALLEJO

ATENCIÓN: DR. JUAN FRANCISCO PACHECO TORRES

DIRECTOR DE ESCUELA INGENIERÍA DE SISTEMAS

DR. AGREDA GAMBOA, EVERSON DAVID

ASESOR DEL PROYECTO DE INVESTIGACIÓN

PRESENTE

ASUNTO: Autorización de proyecto de investigación

Ante todo, reciban un cordial saludo y por medio de la presente hacer de su conocimiento que el señor Anuar Mauro Limache Ynquilla estudiante de la escuela de ingeniería de sistemas, ha sido aceptado satisfactoriamente para realizar su investigación en nuestra empresa de LISERME, la investigación a desarrollarse se denomina "***Aplicación de la norma internacional ISO 27035:2016 para la gestión de incidentes de seguridad en la empresa LISERME S.R.L., Arequipa 2022***".

Sin más que hacer referencia

Atentamente,

LISERME S.R.L.

GERENTE GENERAL

Anexos 10 Política de respuesta a incidentes

POLÍTICA DE RESPUESTA A INCIDENTES

Versión 1.0

Tabla de Contenido

1. Introducción

Este documento describe un plan general de respuesta a incidentes de seguridad de la información. Define los roles y responsabilidades de los participantes.

1.1. Objetivo

El objetivo del plan de respuesta a incidentes de seguridad de la información es detectar y responder a incidentes de seguridad informática, determinar su alcance para responder adecuadamente, comunicar los resultados y los riesgos a todas las partes interesadas y reducir la probabilidad de que el incidente vuelva a ocurrir.

1.2. Alcance

Este Plan de Respuesta y Gestión de Incidentes establece el procedimiento a seguir en caso de incidentes. Procesos recomendados para incorporar en Este documento cubre las mejores prácticas de seguridad por el equipo de TI. Se aplica a los Sistemas de Información, datos y redes de la empresa y cualquier persona o dispositivo que se tenga acceso.

1.3. Referencias normativas

Los siguientes documentos, en todo o en parte, están referenciados normativamente en este documento y son indispensables para su aplicación. Para las referencias con fecha, sólo se aplica la edición citada. Para las referencias sin fecha, se aplica la última edición del documento de referencia (incluidas las modificaciones).

ISO/IEC 27000, Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Visión general y vocabulario.

ISO/IEC 27035-2, Tecnología de la información. Técnicas de seguridad. Gestión de incidentes de seguridad de la información. Parte 2: Directrices para planificar y prepararse para la respuesta a incidentes.

1.4. Definiciones

Evento de seguridad de la información: Ocurrencia que indica una posible violación de la seguridad de la información o falla de los controles

Equipo de respuesta a incidentes IRT: Equipo de miembros de la organización debidamente calificados y confiables que manejan incidentes durante su ciclo de vida, CERT (Equipo de respuesta a emergencias informáticas) y CSIRT (Equipo de respuesta a incidentes de seguridad informática) son términos comúnmente utilizados para IRT.
Incidente de seguridad de la información: Uno o múltiples eventos de seguridad de la información relacionados e identificados que pueden dañar los activos de una organización o comprometer sus operaciones

Gestión de incidentes de seguridad de la información: Ejercicio de un enfoque coherente y eficaz para el manejo de incidentes de seguridad de la información
manejo de incidentes: Acciones de detección, informe, evaluación, respuesta, tratamiento y aprendizaje de incidentes de seguridad de la información

Respuesta al incidente: Acciones tomadas para mitigar o resolver un incidente de seguridad de la información, incluidas aquellas tomadas para proteger y restaurar las condiciones operativas normales de un sistema de información y la información almacenada en él.

Filtración de datos: Un Incidente de Seguridad o Privacidad que conduzca a la destrucción, pérdida, alteración, divulgación no autorizada, acceso accidental o ilegal de Datos transmitidos, almacenados o procesados de otro modo.

Controlador de datos: Significa la persona u organización que determina el propósito y los medios del Tratamiento de Datos.

Escalar incidentes: La contratación de recursos adicionales para resolver o proporcionar el estado de un incidente.

Registro de incidentes: Creado en el momento en que se reconoce inicialmente un incidente de seguridad. Contiene toda la información relevante relacionada con el incidente de seguridad.

Seguridad de información: Preservación de la confidencialidad, integridad y disponibilidad de la Información y los equipos o servicios que contienen o proporcionan dicha Información.

incidente de seguridad Un evento único o una serie de Eventos de Seguridad no deseados o inesperados que comprometen las operaciones comerciales con un impacto en la Seguridad de la Información.

2. Fases

2.1. Planificar y preparar

La gestión eficaz de incidentes de seguridad de la información requiere una planificación y preparación adecuadas.

Para que se ponga en marcha un plan de gestión de incidentes de seguridad de la información eficiente y eficaz, una organización debe completar:

- Sus empleados estén debidamente capacitados con respecto a sus funciones y responsabilidades de respuesta a incidentes en caso de violación de datos.

- Desarrolle escenarios de simulacros de respuesta a incidentes y realice regularmente violaciones de datos simuladas para evaluar su plan de respuesta a incidentes.
- Asegúrese de que todos los aspectos de su plan de respuesta a incidentes como capacitación, ejecución, recursos de hardware y software, entre otros estén aprobados.

2.2. Detectar e informar

La segunda fase de la gestión de incidentes de seguridad de la información implica la detección, la recopilación de información asociada y la notificación de eventos de seguridad de la información y la existencia de vulnerabilidades de seguridad de la información por medios manuales o automáticos. En esta fase, es posible que los eventos y las vulnerabilidades aún no se clasifiquen como incidentes de seguridad de la información. La notificación de eventos de seguridad de acuerdo con las políticas de notificación de la organización permite un análisis posterior si es necesario.

El CSIRT, o una entidad interna o externa, identifica un evento de seguridad o privacidad que puede ser el resultado de una posible explotación de una vulnerabilidad de Seguridad.

Inmediatamente después de la observación o notificación de cualquier sospecha de evento de seguridad, el personal informara de inmediato dicho conocimiento y/o sospecha al departamento de seguridad de la Información por cualquier tipo de medio como teléfono, correo electrónico o apersonarse al área de seguridad de la Información.

Un evento de seguridad se puede descubrir de muchas maneras, incluidas las siguientes como, la observación de comportamientos sospechosos o sucesos inusuales, fallas en la seguridad física o digital, información que llega a manos de personal no autorizado o de terceros, información expuesta inapropiadamente en un sitio web público, para evaluar si se debe informar un evento de seguridad; el personal deberá considerar si existen indicios de que la información fue utilizada por personal no autorizado o terceros, se ha descargado o copiado

indebidamente información de los sistemas o equipos informáticos de la empresa, se han perdido o robado equipos o dispositivos que contienen Información, los equipos o dispositivos que contienen Información han estado sujetos a actividades no autorizadas como podría ser piratería, malware, los datos personales se han divulgado, accedido o transferido de manera inapropiada.

Además, se considerarán las siguientes situaciones para el reporte de Eventos de Seguridad o Privacidad:

- Controles de seguridad ineficaces.
- Falta de confidencialidad o disponibilidad de la Información.
- Errores humanos.
- Infracciones de acceso.
- Incumplimiento de políticas o normas.
- Incumplimiento de seguridad física.
- Cambios de sistemas no controlados.
- Mal funcionamiento del software o hardware.

El personal debe de informar cualquier incidente de seguridad aun si no está seguro que es un evento de seguridad. El CSIRT generalmente requerirá información necesaria para el registro de incidente, normalmente se proporcionará la siguiente información:

- Nombre de contacto e información de la persona que reporta el incidente de seguridad.
- Fecha y hora en que ocurrió y notificó el incidente de seguridad.
- Tipo y circunstancias del incidente de seguridad.
- El tipo de datos, información o equipo involucrado.
- Datos o equipos afectados.
- Magnitud del incidente de seguridad
- Si hubiera cualquier número de ticket asociado, correos electrónicos o entradas de registro asociadas con el incidente de seguridad.

El jefe del CSIRT, se asegurará de que el CSIRT se active de inmediato una vez que se reciba dicho aviso. También se realizarán las siguientes acciones:

El CSIRT, bajo el liderazgo del líder principal del CSIRT, analizara el incidente posterior a la notificación y decidir si procede con la fase de análisis de los procedimientos de respuesta a incidentes. La determinación de iniciar el análisis debe hacerse rápidamente para que el personal pueda tomar una determinación inicial sobre la urgencia y gravedad de la situación.

Al tomar la decisión de iniciar la Fase de Análisis, si el CSIRT sospecha que el incidente de seguridad puede resultar en daño a la reputación de la empresa o tenga alguna responsabilidad legal, el Área legal deberá iniciar una evaluación de la seguridad real o potencial sobre los asuntos legales.

Toda la información recopilada relacionada con un evento o vulnerabilidad de seguridad de la información debe almacenarse en la base de datos de seguridad de la información administrada por el IRT. La información reportada durante cada actividad debe ser lo más completa posible en ese momento. Esto apoyará las evaluaciones, decisiones y acciones a tomar.

2.3. Evaluación y decisión

La respuesta inicial a la detección de un incidente de seguridad empieza con la evaluación. El CSIRT determina si un incidente de seguridad es un incidente de seguridad real. Para determinar si un incidente de seguridad es un incidente de seguridad, se tomarán en consideración los siguientes aspectos:

Utilizar los diagnósticos de eventos de los equipos para analizar el incidente de seguridad utilizando herramientas directamente en el sistema operativo o de una aplicación externa. Esto puede incluir, pero no limitarse a toma de capturas de pantalla, consulta de logs y rastreos de red, realizar análisis sobre la información que se encontró.

Identificar si el incidente de seguridad fue el resultado de un error del personal o de las acciones de un atacante potencial. En este último caso, se procurará identificar quién puede ser el potencial atacante, mediante procesos como; Validación de la dirección IP del atacante, investigar al atacante a través de motores de búsqueda, uso de bases de datos de incidentes, monitorear los canales de comunicación del atacante, si es posible y con la aprobación de un asesor legal de la empresa, escanear potencialmente el sistema del atacante.

Si el CSIRT ha determinado que un incidente de seguridad se notificará a la alta dirección y se llamará a los miembros del equipo CSIRT correspondientes y el CSIRT comenzará a documentar la investigación y recopilar pruebas. El tipo de Incidente de seguridad se basa en la naturaleza del incidente. Como la exposición de datos, acceso no autorizado/acceso basado en roles inapropiados, denegación de servicio, código malicioso, uso inadecuado, escaneos e Intento de acceso.

Si se determina que no se ha desencadenado un Incidente de seguridad, las actividades adicionales indicadas en las actividades posteriores al incidente pueden iniciarse bajo la dirección del CSIRT.

Se evaluará el impacto potencial del Incidente de Seguridad se asignará una clasificación de gravedad inicial de baja, media, alta o crítica al Incidente de seguridad. Para el análisis de situación, alcance e impacto, la CSIRT deberá:

- Definir y confirmar el nivel de gravedad y el impacto potencial del incidente de seguridad.
- Identificar qué recursos se han visto afectados y qué recursos se verán afectados en el futuro.
- Estimar el efecto actual y potencial del incidente de seguridad.

El CSIRT determinara el alcance del incidente de seguridad y verificar si el incidente de seguridad sigue activo.

Si el incidente de seguridad involucra al tipo de malware, el CSIRT analizará el malware para determinar sus capacidades y el impacto potencial. Con base en la evidencia revisada, el CSIRT determinará si el Incidente de seguridad o privacidad requiere una reclasificación en cuanto a su gravedad.

Como se indicó anteriormente, un incidente de seguridad o privacidad puede requerir la recopilación de pruebas. La recolección de tales pruebas se hará con la debida diligencia y se aplicarán los siguientes procedimientos:

La recopilación y el manejo de pruebas tendrá los siguientes datos; Información de identificación como la ubicación, el número de serie, el número de modelo, el nombre de host, la dirección MAC y la dirección IP, nombre, cargo y número de teléfono de todas las personas que recolectaron o manejaron la evidencia durante la investigación, Hora y fecha de cada ocurrencia de manejo de evidencia, los lugares donde se almacenaron las pruebas, y condiciones de almacenamiento y se creara dos copias de seguridad una se utilizara como prueba y la otra se usará como fuente de copias de seguridad adicionales.

Cuando corresponda, y dependiendo de la gravedad del Incidente de Seguridad, los artículos y áreas que se asegurarán y conservarán como áreas de trabajo incluyendo papeleras, hardware de computadora, software, medios de almacenamiento, documentación incluido manuales, impresos, cuadernos, blocs de notas.

En caso de daños, el sistema informático y su área circundante, así como otros dispositivos de almacenamiento de datos, se conservarán para la posible recopilación de pruebas como huellas dactilares.

Es importante establecer quién estaba usando el sistema informático en el momento del incidente de seguridad o privacidad y/o quién estaba en el área inmediata. El CSIRT deberá obtener copias de los registros como registros de acceso, grabaciones de cámaras de vigilancia.

Según el nivel de gravedad y la categorización del Incidente de seguridad o privacidad, el CSIRT notificará y contactará al equipo o personal adecuado, hasta que el CSIRT con la aprobación de la alta gerencia mantendrá el proceso confidencial.

2.4. Respuestas

La contención mitiga la causa raíz del incidente de seguridad para evitar más daños. Intenta limitar el impacto de un incidente de seguridad antes de un evento de erradicación y recuperación. El CSIRT puede implementar controles, según sea necesario, para limitar el daño de un incidente de seguridad. si se determina que un incidente de seguridad se debe a un error humano, es posible que no se necesite la erradicación.

Se eliminan del entorno las vulnerabilidades que causan el Incidente de Seguridad, y cualquier compromiso asociado. Una erradicación eficaz para un ataque dirigido elimina el acceso del atacante al entorno de una sola vez, durante un evento coordinado de contención y erradicación. Aunque las acciones específicas tomadas durante la erradicación pueden variar según el incidente de seguridad, el proceso estándar para la erradicación será el siguiente:

1. Determine los síntomas y la causa relacionados con los sistemas afectados.

2. Eliminar componentes del incidente de seguridad. Esto puede incluir la eliminación de malware, la desactivación de cuentas de usuario violadas, etc.

3. Reforzar los controles que rodean los sistemas afectados.

4. Si se identifican problemas o síntomas adicionales, tome las medidas preventivas adecuadas para eliminar o minimizar posibles compromisos futuros.

5. Actualice el Registro de incidentes con la información obtenida de la evaluación de vulnerabilidades, incluida la causa, los

síntomas y el método utilizado para solucionar el problema con los sistemas afectados.

6. Si es necesario, se debe escalar a niveles más altos de apoyo para mejorar las capacidades, los recursos o el tiempo de erradicación.

7. Informar a la alta gerencia del progreso, según corresponda.

Después de que se haya implementado los cambios para la erradicación, es importante verificar que la causa y persona o personas que causan el incidente de seguridad se haya erradicado completamente. El CSIRT también probará la eficacia de los controles de seguridad o los cambios que se hayan realizado en el medio ambiente durante la contención y la erradicación.

La Fase de Respuesta representa el esfuerzo del CSIRT para restaurar el funcionamiento de los sistemas afectados después de que se hayan corregido los problemas que dieron lugar al incidente de seguridad y las consecuencias del incidente de seguridad. Los eventos de recuperación pueden ser complejos según el tipo de incidente de seguridad y pueden requerir planes completos de gestión de proyectos para que sean efectivos.

Aunque las acciones específicas tomadas durante la recuperación pueden variar según el incidente de seguridad identificado, el proceso estándar para lograr esto será el siguiente:

1. Ejecución de las siguientes acciones, según corresponda; Instalación de parches, reconstrucción de sistemas, cambio de contraseñas, restauración de sistemas a partir de copias de seguridad limpias, sustitución de archivos afectados por versiones estables.

2. Determinación de si los sistemas afectados se han modificado de alguna manera. Si se han cambiado los sistemas, el sistema se restaura la última copia de seguridad estable. Una vez restauradas, las funciones del sistema se validan para verificar que el sistema y

procesos funcione según lo previsto. Esto puede requerir la participación de la unidad de negocio propietaria de los sistemas afectados. Si se interrumpió la operación de los sistemas (es decir, los sistemas se desconectaron), se restaurarán y validarán, y se monitoreará el comportamiento adecuado de los sistemas.

Si los sistemas no se han modificado de ninguna manera, pero se desconectaron o interrumpieron, reinicie el sistema y controle el comportamiento adecuado.

3. Se puede implementar monitoreo y alertas adicionales para identificar actividades similares.

4. Actualice el Registro de incidentes con cualquier detalle que se considere relevante.

5. Informar a la alta gerencia del progreso, según corresponda.

2.5. Lecciones aprendidas

Además de los requisitos de notificación de violación de datos y actividades anormales identificados en el análisis anterior, y luego de la verificación de una contención exitosa y cualquier erradicación necesaria, el CSIRT deberá tomar las siguientes actividades posteriores al incidente, según sea necesario:

- Identificar las lecciones aprendidas de los incidentes y vulnerabilidades, identificar las lecciones aprendidas de los incidentes y vulnerabilidades de seguridad de la información;
- Revisar, identificar y realizar mejoras en la implementación de controles de seguridad de la información (controles nuevos o actualizados), así como la política de gestión de incidentes de seguridad de la información. Las lecciones pueden provenir de uno o varios incidentes de seguridad de la información o vulnerabilidades de seguridad informadas. Las mejoras cuentan con la ayuda de métricas que se incorporan a la estrategia de la organización sobre dónde invertir en controles de seguridad de la información;

- Revisar, identificar y realizar mejoras en la evaluación de riesgos de seguridad de la información y las revisiones de gestión existentes de la organización;
- Revisar qué tan efectivos fueron los procesos, procedimientos, formatos de informes y estructura organizativa para responder, evaluar y recuperarse de incidentes de seguridad de la información y tratar las vulnerabilidades de seguridad de la información. Sobre la base de las lecciones aprendidas, identificar y mejorar el plan de gestión de incidentes de seguridad de la información y su documentación;
- Comunicar y compartir los resultados de la revisión dentro de una comunidad de confianza (si la organización así lo desea);
- Determinar si la información del incidente y las vulnerabilidades se pueden compartir con las organizaciones asociadas para ayudar a prevenir que ocurran los mismos incidentes en sus entornos.
- Realizar periódicamente una evaluación exhaustiva del desempeño y la eficacia de la IRT.

Se enfatiza que las actividades de gestión de incidentes de seguridad de la información son iterativas y, por lo tanto, una organización debe realizar mejoras periódicas en una serie de elementos de seguridad de la información a lo largo del tiempo. Estas mejoras deben proponerse sobre la base de revisiones de los datos sobre incidentes de seguridad de la información, respuestas y vulnerabilidades de seguridad de la información informadas.

3. Registro de revisiones

Versión	Fecha	Revisión
1.0	**Abril 2022**	**Versión Inicial**

Anexos 11 Política de seguridad de la información

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Versión 1.0

Tabla de Contenido

1. Introducción

Este documento describe un plan general de seguridad de la información, con cada actualización de la tecnología, surge un nuevo potencial para la violación de la seguridad de la información. Los peligros a una computadora de escritorio son muy diferentes que de un teléfono móvil o una tablet. Incluso las redes inalámbricas son más susceptibles de ataques que los sistemas cableados.

Mientras que la mayor parte de la seguridad de la información se centran en amenazas externas como de piratas informáticos y descargas maliciosas, las amenazas internas representan muchas más pérdidas que las amenazas externas. Una amenaza interna podría ser la eliminación o difusión de archivos informáticos relacionados con el caso de un cliente. Un empleado también podría compartir su contraseña con otro, otorgándole alguien tiene acceso más allá del alcance de su posición. Para prevenir los problemas intencionales o no intencionales creados por el uso de software y equipo por parte de los empleados, desarrollar una política de seguridad de datos exhaustiva es más importante que nunca.

1.1. Objetivo

Los objetivos de una política de seguridad de la información es la preservación de la confidencialidad, integridad y disponibilidad de los sistemas y la información utilizada por personal de la empresa.

1.2. Alcance

Esta Política de Seguridad de la Información se aplica a todo el personal, directivos, jefes, consultores, contratistas, socios, organizaciones y personal asociado de la empresa. Abarca toda la información manejada, almacenada, procesada o compartida por la empresa, se aplica a todos los sistemas de información computarizados y no computarizados propiedad de la empresa.

1.3. Roles y responsabilidades

Usuarios: Cumplir con las políticas de seguridad, Informar de cualquier intento de violación de la seguridad.

Contratistas externos: Todos los contratos con contratistas externos que permitan el acceso a los datos o sistemas de información de la organización deben estar en funcionamiento antes de que se permita el acceso. Estos contratos deben garantizar que el personal o los subcontratistas de la organización externa cumplan con todas las políticas de seguridad apropiadas.

Jefe de seguridad de la información: Responsable de todos los aspectos de la seguridad de la información de la Organización.

Equipo de seguridad de la información: Implementa y opera la seguridad informática, implementa los privilegios y derechos de acceso a los recursos, actualiza políticas de seguridad, responsable de la seguridad de la infraestructura informática, planificar contra amenazas, vulnerabilidades y riesgos de seguridad, implementar y mantener documentos de política de seguridad, garantizar programas de formación en seguridad, garantizar que la infraestructura de TI sea compatible con las políticas de seguridad, responder a incidentes de seguridad de la información, ayuda en planes de recuperación ante desastres.

Propietarios de la información: ayuda con los requisitos de seguridad para su área específica, determinar los privilegios y derechos de acceso a los recursos dentro de sus áreas.

1.4. Definiciones

Equipo de respuesta a incidentes IRT: Equipo de miembros de la organización debidamente calificados y confiables que manejan

incidentes durante su ciclo de vida, CERT (Equipo de respuesta a emergencias informáticas) y CSIRT (Equipo de respuesta a incidentes de seguridad informática) son términos comúnmente utilizados para IRT.

Confidencialidad: La propiedad de que la información no se pone a disposición ni se revela a personas, entidades o procesos no autorizados.

Disponibilidad: La propiedad de ser accesible y utilizable a pedido de una entidad autorizada.

Mitigación: Limitación de la consecuencia negativa de un evento particular.

Riesgo: El potencial de que una amenaza dada aproveche las vulnerabilidades de un activo o grupo de activos y, por lo tanto, cause daño a la organización.

Integridad: La propiedad de salvaguardar la exactitud e integridad de los activos.

Sistema de gestión de seguridad de la información: Aquella parte del sistema de gestión general, basado en un enfoque de riesgo empresarial, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

Evento de seguridad de la información: Ocurrencia que indica una posible violación de la seguridad de la información o falla de los controles.

Incidente de seguridad de la información: Uno o múltiples eventos de seguridad de la información relacionados e identificados que pueden dañar los activos de una organización o comprometer sus operaciones

Manejo de incidentes: Acciones de detección, informe, evaluación, respuesta, tratamiento y aprendizaje de incidentes de seguridad de la información

Respuesta al incidente: Acciones tomadas para mitigar o resolver un incidente de seguridad de la información, incluidas aquellas tomadas para proteger y restaurar las condiciones operativas normales de un sistema de información y la información almacenada en él.

Filtración de datos: Un Incidente de Seguridad o Privacidad que conduzca a la destrucción, pérdida, alteración, divulgación no autorizada, acceso accidental o ilegal de Datos transmitidos, almacenados o procesados de otro modo.

Controlador de datos: Significa la persona u organización que determina el propósito y los medios del Tratamiento de Datos.

Escalar incidentes: La contratación de recursos adicionales para resolver o proporcionar el estado de un incidente.

Registro de incidentes: Creado en el momento en que se reconoce inicialmente un incidente de seguridad. Contiene toda la información relevante relacionada con el incidente de seguridad.

Seguridad de información: Preservación de la confidencialidad, integridad y disponibilidad de la Información y los equipos o servicios que contienen o proporcionan dicha Información.

Incidente de seguridad: Un evento único o una serie de Eventos de Seguridad no deseados o inesperados que comprometen las operaciones comerciales con un impacto en la Seguridad de la Información.

2. Política

Esta política ayudara hacer el mejor uso de los recursos informáticos a su disposición, al tiempo que minimiza los riesgos de seguridad. Debe comprender lo siguiente:

- Usted es individualmente responsable de proteger el equipo, el software y la información en sus manos. La seguridad es responsabilidad de todos.

- Identificar qué datos no son públicos, lo que incluye datos confidenciales de la empresa, datos de clientes y datos personales, como se describe más adelante. Si no sabe o no está seguro, pregunte. Aunque no se pueda tocar, la información es un activo, a veces un activo invaluable.
- Utilizar los recursos a su disposición únicamente en beneficio de la empresa.
- Comprenda que usted es responsable de lo que hace en el sistema.
- Proteja el equipo de pérdidas y robos. Solo almacene datos de la empresa en dispositivos encriptados.
- No pase por alto las reglas establecidas de conexión a la red y al acceso a Internet.
- No pase por alto ni desinstale su software antivirus o de firewall.
- No cambie ni instale ningún software no autorizado o como complementos del navegador.
- No copie ni almacene datos de la empresa en dispositivos externos o ubicaciones externas no autorizadas incluidos los servicios basados en la nube que no son servicios aprobados por la empresa. Póngase en contacto con TI para obtener la mejor solución para la transferencia segura de archivos cuando sea necesario.
- Si se entera de un Incidente de seguridad potencial o real, debe informar el incidente lo antes posible.
- Todo el personal debe leer, comprender, reconocer y seguir las políticas y los estándares de apoyo de este capítulo. Estos establecen las reglas básicas bajo las cuales la empresa opera y protege sus datos y sistemas de información para reducir el riesgo y minimizar el efecto de posibles incidentes.

2.1. Protección de datos

Para proporcionar confidencialidad de datos en caso de pérdida de datos accidental o malintencionada, todos los Datos personales, se cifrarán al menos AES de 256 bits.

El cifrado de redes inalámbricas se habilitará utilizando los siguientes niveles de cifrado, separando las redes según el tipo de dispositivo que se utilice:

- Propiedad de la empresa: El acceso a redes será de todo corporativo más Internet con autenticación 802.1x + AES.
- Empleados: El acceso a la red será de solo Internet con autenticación: 802.1x + AES.
- Invitado: El acceso a la red será solo Internet con autenticación MAC.

Cualquier requisito de encriptación de red inalámbrica que no pueda ser abordado por los tipos de dispositivos identificados anteriormente debe ser revisado y aprobado por Seguridad de la Información. Los Datos personales de los empleados, no se almacenarán en equipos que no sean propiedad de empresa, ni estén administrados por este.

Se implementarán políticas y procesos documentados para garantizar que se implemente el cifrado y la gestión de claves adecuados, incluida la rotación periódica de claves. Se implementarán procesos y herramientas de prevención de pérdida de datos para identificar y/o prevenir la pérdida de datos.

2.2. Seguridad de los recursos humanos

La Selección de empleo, se realizarán verificaciones de antecedentes de todos los empleados, contratistas y proveedores cuando lo exija el acceso a información confidencial.

Todos los gerentes deben asistir a la capacitación anual de revisión y política de seguridad, la gerencia requerirá que los empleados y los usuarios externos apliquen seguridad de acuerdo con las políticas y procedimientos de seguridad de la información de la empresa, las responsabilidades de la gerencia incluirán garantizar que los empleados y usuarios externos estén debidamente informados sobre sus responsabilidades de seguridad de la información antes de que se

les conceda acceso a información o sistemas confidenciales, están obligados a cumplir con las políticas de seguridad de la empresa.

La capacitación en seguridad de la información requerirá que todos los empleados completen una capacitación anual sobre concientización y conceptos de seguridad de la información, informen cualquier incidente, inquietud o actividad sospechosa a su supervisor directo, recursos humanos o al CSIRT.

Se seguirá un proceso disciplinario formal, tal como se define en el manual de recursos humanos de la empresa, para disuadir y disciplinar a los empleados o agentes externos que violen las políticas y normas de seguridad de la información.

2.3. Gestión de activos de TI

Se utiliza una variedad de activos de información, que van desde computadoras portátiles y teléfonos móviles.

Se debe de mantener un inventario que debe incluir los siguientes detalles para todos los activos de información significativos que pertenecen o son utilizados por la empresa, nombre y características del activo, el propietario de la información, el responsable de la información y la ubicación como base de datos, requerimientos del activo en cuanto a disponibilidad, tiempo de actividad.

2.4. Política de seguridad, vulnerabilidades, debilidades e incidentes

La capacitación en concientización sobre seguridad se llevará a cabo al menos una vez por año calendario. La formación deberá cubrir las políticas de seguridad de la información, así como las mejores prácticas y política de respuesta a incidentes.

La capacitación de concientización sobre seguridad se brindará en la primera sesión de incorporación a la que asistan los nuevos empleados. Se debe brindar capacitación especializada a las partes

interesadas clave (es decir, informes y gestión de incidentes, ISO 27035:2016, política y proceso de seguridad.

Las vulnerabilidades de seguridad se informarán de inmediato a seguridad de la información ya que podrían desencadenar un evento de seguridad. Los eventos de Seguridad serán analizados por CSIRT para determinar si son considerados Incidentes de seguridad, los cuales deben ser atendidos de acuerdo con los procedimientos de respuesta a incidentes.

2.5. Política de acceso al sistema

Todas las computadoras deben estar protegidas por sistemas de control de acceso basados en contraseña aprobados, la autenticación para el acceso remoto a redes para los empleados, administradores y terceros se implementará donde esté disponible.

Las cuentas predeterminadas estarán deshabilitadas y/o se cambiarán con las contraseñas predeterminadas asociadas con dichas cuentas, es obligatorio el cambio de contraseñas durante el primer inicio de sesión y en intervalos de 120 días, no se mostrarán ni se transmitirán por los usuarios.

Las contraseñas se almacenarán en un formato cifrado, se mantendrá un historial de contraseñas para evitar la reutilización de contraseñas, un máximo de tres fallas de inicio de sesión sucesivas resultará en el bloqueo de la cuenta hasta que un administrador la desbloquee y se deben mantener las siguientes reglas para administrar los accesos a los usuarios:

- El registro de usuarios debe de ser aprobado y se dará acceso a los usuarios según sus funciones.
- Se Debe determinar jerarquías claras para cada sistema para la gestión de privilegios y cada jerarquía debe aprobarse formalmente. Por ejemplo, para Oracle, hay 13 niveles de autoridad formalmente reconocidos, y cualquier cambio en ese número o en su composición debe ser aprobado formalmente por el Controlador del Grupo.

- Los accesos de usuarios están sujetos a revisiones periódicas, las cuentas inactivas deben configurarse para desactivarse automáticamente después de 120 días.

2.6. Política de uso de activos

Los recursos de tecnología de la información de la empresa proporcionan a los usuarios facilitar el desempeño eficiente y eficaz de sus funciones. El uso de dichos recursos impone ciertas responsabilidades y obligaciones a los usuarios y está sujeto a las políticas de la empresa. Todas las políticas o procedimientos adicionales deben ser aprobados por el jefe de seguridad de la información.

2.7. Política de Redes y Comunicación

Las redes orientadas al exterior deben tener un firewall a un nivel apropiado, los cambios físicos y lógicos de red solo deben ser realizados por usuarios aprobados, deben existir controles apropiados en las interfaces de red, los servicios WAN solo deben adquirirse a través de proveedores aprobados, se debe implementar el registro y monitoreo de eventos de red.

Los usuarios de terceros no deberán conectar sus dispositivos informáticos a la red cableada o inalámbrica, a menos que estén autorizados, las computadoras pueden conectarse a computadoras o redes de terceros solo con aprobación, las contraseñas de las redes inalámbricas para invitados deben cambiarse con regularidad.

2.8. Política de Copias de seguridad

Se realizarán copias de seguridad periódicas de los datos, las aplicaciones y la configuración de los servidores, para permitir la recuperación de datos en caso de un desastre o un evento de continuidad, las copias de seguridad se almacenarán en una ubicación separada geográficamente física y lógicamente segura.

2.9. Política de seguridad de dispositivos móviles

Implementar los controles adecuados para mitigar los riesgos para la información móvil y los entornos de trabajo remotos, mediante

procesos y herramientas de prevención de pérdida de datos para identificar y prevenir la pérdida de datos. El uso de dispositivos de propiedad personal deberá cumplir con las políticas de uso y seguridad de la información.

Los dispositivos propiedad de los empleados nunca se utilizarán para acceder a los datos del cliente, a menos que se hayan implementado los controles de monitoreo apropiados y aprobados además no pueden conectarse a redes corporativas.

2.10. Política de protección contra virus y malware

Se instalará software antivirus actualizado para detectar, eliminar y proteger contra virus sospechosos en todos los servidores, estaciones de trabajo y computadoras portátiles, se actualizará regularmente para todos los equipos.

Se informará a los usuarios sobre los procedimientos y políticas antivirus vigentes, el personal deberá informar inmediatamente al departamento de seguridad de información en caso de una posible infección de virus, los sistemas deben aislarse de la red, escanearse y limpiarse adecuadamente.

Todos los medios extraíbles u otros sistemas a los que se haya propagado el virus se tratarán en consecuencia. Si se ha identificado un sistema como potencialmente infectado y no se puede probar definitivamente la eliminación o cuarentena del virus o malware, el sistema se borrará por completo y se volverá a crear una imagen, los usuarios afectados por incidentes de seguridad relacionados con virus serán notificados tan pronto como sea razonablemente posible de acuerdo a la política de respuesta a incidentes, las posibles infecciones de virus y malware se informarán de inmediato al área seguridad de la información y se escalarán al equipo de respuesta a incidentes de seguridad CSIRT.

2.11. Licencias

Los sistemas operativos, aplicaciones y software de base de datos que estarán bajo acuerdo de licencia, Es importante tener un control sobre el uso de software en las computadoras.

2.12. Política de seguridad física

El acceso a todas las oficinas, salas de máquinas informáticas y otras áreas de trabajo que contengan información confidencial debe estar físicamente restringido, todos los usuarios deben asegurarse de que ningún activo de información importante quede desatendido en los escritorios, especialmente fuera del horario laboral.

Los servidores deben estar ubicadas en un lugar donde el riesgo de desastres naturales esté controlado, los puntos de entrada a las instalaciones de TI deben controlarse con mecanismos de control de acceso electrónico, deben existir controles ambientales apropiados, como aire acondicionado y sistemas de supresión de incendios, debe de tener energía de respaldo con una duración suficiente, el acceso de visitantes debe ser controlado, no se permiten alimentos ni bebidas en los centros de datos.

3. Registro de revisiones

Versión	Fecha	Revisión
1.0	**Abril 2022**	**Versión Inicial**

Anexos 12 Establecimiento del CSIRT

Establecimiento del CSIRT

Objetivo

El objetivo de establecer el CSIRT es proporcionar a la organización la capacidad adecuada para evaluar, responder y aprender de los incidentes de seguridad de la información, y proporcionar la coordinación, gestión, retroalimentación y comunicación necesarias. Un CSIRT contribuye a la reducción del daño físico y monetario, así como a la reducción del daño a la reputación de la empresa que en ocasiones se asocia con incidentes de seguridad de la información.

Misión

Brindar información y asistencia a todo el personal de la empresa para reducir los riesgos de incidentes de seguridad informática además de responder a los incidentes cuando se presenten.

Visión

Lograr ser una empresa líder en seguridad y confiable contando con personal apto que utiliza los procedimientos y políticas de la empresa de forma eficiente.

Alcance

Los sistemas de información, toda la Información datos y redes de la empresa y cualquier persona o dispositivo que obtenga acceso a estos sistemas o datos.

Principales actividades del CSIRT

- Gestión de sistemas integrados de seguridad: Monitorización y gestión de eventos de seguridad de la información de agentes instalados en sistemas heterogéneos (por ejemplo, sistema de detección de intrusos, sistema de prevención de intrusos, cortafuegos, recurso de red, etc.).

- Implementar una política consistente: Minimizar los riesgos para el sistema de información mediante la aplicación de un conjunto consistente de tareas de respuesta de acuerdo con la política definida.
- Responder con prontitud: reaccionar rápidamente ante amenazas, infracciones y ataques para minimizar los daños y reducir el costo de recuperación.
- Los deberes de un CSIRT también pueden incluir actividades de monitoreo y gestión de la siguiente manera:
- Gestión y seguimiento integrado: seguimiento 24 × 7 × 365 h de objetivos, seguimiento proactivo y respuesta ante incidentes, gestión de logs.
- Gestión de informes: Informes periódicos de seguridad, gestión de parches de seguridad, informe de incidencias.
- Gestión administrativa: gestión de políticas para varios entornos de sistemas, incluido el control de tareas y las operaciones de CSIRT.
- Gestión técnica: Gestión de la seguridad de redes, sistemas, aplicaciones, contenidos y servicios.
- Operación y gestión del sistema: capacidad del sistema, rendimiento, configuración de seguridad y gestión de la configuración del entorno.

Rol

1. **Gerente de** CSIRT**:** Es responsable de administrar a los miembros del personal, definir el alcance del trabajo e informar el estado a las organizaciones de nivel superior.
2. **Planificación**: Es responsable de operar un CSIRT. Establece o planifica diversas políticas de seguridad, las reporta a las autoridades superiores, coopera con terceros y registra y aprueba informes de vulnerabilidad. Sus funciones son las siguientes:

   a) Establecer y planificar políticas de seguridad;

   b) Implementar procesos de seguridad;

   c) Ajustar las prioridades de riesgo;

d) Comunicarse con organizaciones de alto nivel y otras organizaciones de terceros;

e) Administración de apoyo;

f) Discutir/registrar/aprobar informes de vulnerabilidad de las organizaciones objetivo;

g) Realizar otras actividades dirigidas por el responsable del CSIRT.

3. **Vigilancia:** responsable del monitoreo en tiempo real y las actividades de operación reales, como el monitoreo/detección/identificación de eventos de seguridad, registro de incidentes y prevención. Se realiza las actividades de monitoreo de seguridad en tiempo real y lo siguiente:

   a) Monitoreo y operación 24 h × 365 h;

   b) Detección de pruebas de intrusión, registro de incidentes y primeras respuestas;

   c) Realizar los parches y actualizaciones de seguridad;

   d) Implementación de la política de seguridad y gestión de copias de seguridad;

   e) Mesa de ayuda;

   f) Gestión de instalaciones;

   g) Realizar otras actividades dirigidas por el responsable del CSIRT.

4. **Respuesta:** Gestiona el caso desde los agentes de vigilancia para incidentes relacionados con intrusión, la filtración de datos o la exposición, realiza análisis y acciones secundarias adicionales, incluidos los esfuerzos de investigación, realiza acciones de recuperación y establece la estrategia adecuada. Servicios tales como respuestas en tiempo real, asistencia técnica apoyo, y también se proporciona lo siguiente:

   a) Propagar y reportar incidentes;

   b) Análisis de correlación entre sistemas de seguimiento;

   c) Investigación de incidentes y apoyos de recuperación;

d) Análisis de vulnerabilidad de la organización objetivo y del CSIRT;

e) Realizar otras actividades dirigidas por el responsable del CSIRT.

5. **Análisis:** En cooperación con el equipo de respuesta, realiza un análisis en profundidad que incluye análisis de correlación para los incidentes. También se analizan los incidentes y los siguientes imprevistos:

   a) Planificar el análisis de vulnerabilidad para la organización objetivo y el CSIRT;

   b) Mejorar las herramientas de análisis de seguridad y la lista de verificación;

   c) Mejorar las reglas de seguimiento;

   d) Publicación de boletín;

   e) Realizar otras actividades dirigidas por el responsable del CSIRT.

Responsabilidad

1. **Gerente o líder de equipo:**

   - Proporciona dirección estratégica
   - Permite y facilita el trabajo de los miembros del equipo
   - Supervisa el equipo
   - Representa a CSIRT ante la gerencia y otros
   - Entrevistas y contrata a nuevos miembros del equipo

2. **Subgerentes, supervisores o grupo lideres:**
   - Apoya la dirección estratégica del área funcional asignada
   - Apoya al líder del equipo según sea necesario
   - Proporciona dirección y tutoría a los miembros del equipo
   - Asigna tareas y deberes
   - Participa en entrevistas con nuevos miembros del equipo

3. **Personal de mesa de ayuda:**

- Manejar los teléfonos CSIRT principales para incidentes o informes de seguridad
- Proporcionar asistencia inicial, dependiendo de las habilidades
- Llevar a cabo la entrada inicial de datos y la clasificación y priorización de la información entrante

4. **Manejadores de incidentes:**
   - Llevar a cabo el análisis, el seguimiento, el registro y la respuesta a incidentes
   - Coordinar la orientación reactiva y proactiva que se proporcionará (desarrollar material como documentación, listas de verificación, mejores prácticas y pautas)
   - Difundir información
   - Interactuar con el equipo de CSIRT, expertos externos y otros (como sitios, medios de comunicación, fuerzas del orden o personal legal) según corresponda, por asignación del líder del equipo u otro personal administrativo
   - Emprender actividades de vigilancia tecnológica, si se le asignan
   - Desarrollar materiales de capacitación apropiados (para el personal del CSIRT)
   - Asesorar al nuevo personal del CSIRT, según lo asignado
   - Supervisar los sistemas de detección de intrusos, si este servicio forma parte de las actividades del CSIRT
   - Realizar pruebas de penetración si este servicio es parte de las actividades de CSIRT
   - Participar en entrevistas con nuevos miembros del personal según las indicaciones

5. **Manejadores de vulnerabilidades:**
   - Analizar, probar, rastrear y registrar informes de vulnerabilidad
   - Investigar o desarrollar parches y correcciones como parte del esfuerzo de respuesta a la vulnerabilidad

- Interactuar, el equipo de CSIRT, los desarrolladores de aplicaciones de software, expertos externos según sea necesario
- Difundir información sobre vulnerabilidades y correcciones, parches o soluciones alternativas correspondientes
- Emprender actividades de vigilancia tecnológica, si se le asignan
- Asesorar al nuevo personal del CSIRT, según lo asignado
- Participar en entrevistas con el nuevo personal del CSIRT

Clasificación de incidentes

Un incidente se clasificará como uno de los cuatro niveles de gravedad. Estos niveles de gravedad se basan en el impacto en la empresa y puede expresarse en términos de impacto financiero, impacto en los servicios.

Nº	CLASIFICACIÓN DE INCIDENTES	EJEMPLOS DE INCIDENTES	DESCRIPCIÓN
1	Falla en la infraestructura daño físico	Terremotos, incendios, contaminación, falla de energía eléctrica, falta de servicio de agua, etc.	Desastres naturales no controlados por el hombre o falla de suministro de servicios esenciales.
2	Intentos de intrusión	Intentos de acceso	Múltiples intentos de inicio de sesión, adivinar, descifrar contraseñas, o ingreso por fuerza bruta.
		Explotación de vulnerabilidades conocidas	Un intento de interrumpir cualquier servicio mediante la explotación de vulnerabilidades como desbordamiento de búfer, puerta trasera, secuencias de comandos entre sitios, etc.
3	Contenido	Correo no deseado	Correo masivo no solicitado.
		Discriminación	Desacreditación o discriminación de alguna persona.
4	Código malicioso	Malware, Virus, Gusano, Troyano, Spyware, etc.	Software que se incluye o inserta intencionalmente en un sistema con un propósito dañino.
5	Seguridad del contenido de la información	Acceso no autorizado a la información.	Posibles los ataques que interceptan y acceden a la información durante la transmisión, suplantación de identidad o secuestro ocasionado por error humano o de configuración de software de los dispositivos de la empresa.
		Modificación no autorizada de la información	
6	Recopilación de información	Exploración	Ataques que envían solicitudes a un sistema para descubrir puntos débiles. Esto incluye también algún tipo de proceso de prueba para recopilar información sobre hosts, servicios y cuentas. Ejemplos: digitación, consulta de DNS, ICMP, SMTP (EXPN, RCPT, …), escaneo de puertos.

		oler	Observación y registro del tráfico de la red (escuchas telefónicas).
		Ingeniería social	Recopilación de información de un ser humano de una manera no técnica (por ejemplo, mentiras, trucos, sobornos o amenazas).
7	intrusiones	Compromiso de cuenta privilegiada	Ingreso exitoso de un sistema o aplicación. Esto puede haber sido causado remotamente por una vulnerabilidad conocida o nueva, pero también por un acceso local no autorizado.
		Compromiso de cuenta sin privilegios	
		Compromiso de la aplicación, Bot	
8	Disponibilidad	DOS	Tipo de ataque que un sistema es bombardeado con tantos paquetes que las operaciones se retrasan o el sistema falla.
		Sabotaje	Ataques DoS, de amplificación de DNS, etc. además que la disponibilidad puede verse afectada por acciones locales destrucción, interrupción del suministro eléctrico, etc.
		Interrupción (sin malicia)	fallas espontáneas o errores humanos.
9	Fraude	Suplantación de identidad	Hacerse pasar por otra entidad para persuadir al usuario de que revele una credencial privada
		Derechos de autor	Ofrecer o instalar copias de software comercial sin licencia u otros materiales protegidos por derechos de autor.
		Uso no autorizado de recursos	Usar recursos de la empresa para fines no autorizados como el uso del correo electrónico para usos personales.
		Engaño	Tipo de ataques en los que una entidad asume ilegítimamente la identidad de otra para beneficiarse de ella.
10	Vulnerable	Abierto por abuso	Servicios abiertos Impresoras legibles, cámaras de vigilancia, firmas de virus no actualizadas, etc.
11	Otro	Todos los incidentes que no encajan en una de las categorías dadas deben incluirse en esta clase.	Si aumenta el número de incidentes en esta categoría, es un indicador de que se debe revisar el esquema de clasificación.

Tabla Fuente propia

Descripción del nivel de gravedad

- Bajo: Incidente donde el impacto es mínimo. Como podrían ser correo electrónico SPAM, virus, etc.
- Medio: Incidente donde el impacto es significativo. Pueden ser un retraso o capacidad limitada para brindar servicios, retraso en la entrega de correo electrónico o transferencias de datos, etc.
- Alto: Incidente donde el impacto es severo. Pueden ser una interrupción del servicio y/o desempeño de funciones, virus que se ha propagado ampliamente, etc.
- Critico: Incidente donde el impacto es catastrófico. Los ejemplos pueden ser un cierre de todos los servicios de red de la empresa, la información confidencial comprometida y publicada en un lugar o sitio público, sistemas no están disponibles, etc.

Tabla Fuente propia

- Impacto: Es el daño que causa en la empresa.
- Urgencia: La velocidad que la empresa necesita solucionar el posible problema ocasionado por el incidente.

Relación con otras partes de la organización

La gestión de incidentes no es un proceso autónomo. Se deben establecer relaciones, canales de comunicación, acuerdos para compartir datos y políticas y procedimientos en toda la organización. Estas colaboraciones internas pueden incluir lo siguiente.

- **Gerentes de negocios.** Necesitan comprender qué es el CSIRT y cómo puede ayudar a respaldar sus procesos. Se deben hacer acuerdos con respecto a la autoridad del IRT sobre los sistemas y quién tomará

decisiones si los sistemas críticos deben desconectarse de la red o apagarse.

- **Representantes de TI.** Las interacciones y el flujo de trabajo entre el personal de TI y el CSIRT deben definirse, incluidas las acciones que realizará el personal de TI y los miembros del CSIRT, qué información puede proporcionar el personal de TI al CSIRT y qué información puede proporcionar el CSIRT a el equipo de TI, y qué funciones y autoridad tiene cada uno.
- **Representantes del departamento legal.** Estos representantes pueden brindar orientación sobre asuntos de responsabilidad y cumplimiento además de brindar orientación sobre privacidad y libertades civiles para garantizar que las acciones de investigación y respuesta no infrinjan los derechos de los empleados.
- **Representantes de recursos humanos.** Deberán participar en el desarrollo de políticas y procedimientos para despedir a los empleados internos que se encuentren participando en actividades informáticas no autorizadas o ilegales.
- **Representantes de relaciones públicas.** Deben estar preparados para manejar cualquier consulta de los medios y ayudar a desarrollar políticas y prácticas de divulgación de información.
- **Cualquier grupo de seguridad existente, incluida la seguridad física.** El CSIRT deberá intercambiar información con estos grupos sobre incidentes informáticos y puede compartir con ellos la responsabilidad de resolver problemas relacionados con el robo de datos o computadoras.
- **Especialistas en auditoría y gestión de riesgos.** Pueden ayudar a desarrollar métricas de amenazas e identificar riesgos para los sistemas de circunscripción.

Dado que muchas amenazas de ciberseguridad afectan a varias organizaciones simultáneamente, este tipo de intercambio de información se considera crucial para las operaciones de CSIRT responsables. Cuando sea práctico, se deben establecer intercambios automatizados de información sobre incidentes para aumentar la velocidad a la que se pueden detectar nuevos incidentes a través de la actividad CSIRT colectiva.

Las partes interesadas externas pueden incluir, personal de apoyo externo contratado, CSIRT de organizaciones externas, proveedores de servicios gestionados, incluidos proveedores de servicios de telecomunicaciones, ISP, vendedores y proveedores; organismos encargados de hacer cumplir la ley, personal jurídico, funcionarios de relaciones públicas y/o miembros de los medios de comunicación, socios comerciales, clientes.

Registro de revisiones

Versión	Fecha	Revisión
1.0	**Abril 2022**	**Versión Inicial**

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Declaratoria de Autenticidad del Asesor

Yo, AGREDA GAMBOA EVERSON DAVID, docente de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA ESTE, asesor de Tesis titulada: "Aplicación de la Norma internacional ISO 27035:2016 para la Gestión de incidentes de seguridad de la información en la Empresa LISERME S.R.L., Arequipa 2022", cuyo autor es LIMACHE YNQUILLA ANUAR MAURO, constato que la investigación tiene un índice de similitud de 19.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

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

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

LIMA, 12 de Octubre del 2022

Apellidos y Nombres del Asesor:	**Firma**
AGREDA GAMBOA EVERSON DAVID **DNI:** 18161457 **ORCID:** 0000-0003-1252-9692	Firmado electrónicamente por: AGREDA el 12-10-2022 06:35:36

Código documento Trilce: TRI - 0433869

INVESTIGA UCV