



**FACULTAD DE INGENIERÍA, ARQUITECTURA Y  
URBANISMO**

**Escuela Académico Profesional de Ingeniería de Sistemas**

**TESIS**

**ESTUDIO PARA DETECTAR VULNERABILIDADES  
EN LA SEGURIDAD DEL SOFTWARE DE LA LÍNEA  
DE PRODUCCIÓN DE MICROFORMAS BASADO EN  
LA NORMA TÉCNICA PERUANA NTP ISO/IEC  
27001:2014; CASO DE ESTUDIO CONTRALORÍA  
GENERAL DE LA REPÚBLICA DEL PERÚ**

**PARA OPTAR EL TÍTULO PROFESIONAL DE  
INGENIERO DE SISTEMAS**

**Autor:**

**Bach. Romero Mas, Armando Demetrio**

**Asesor**

**Mg. Bravo Ruiz, Jaime Arturo**

**Línea de investigación**

**Ingeniería de software (calidad de software)**

**Pimentel – Perú**

**2018**

## Aprobación de la tesis

---

Ing. Tuesta Monteza, Víctor Alexci

**Presidente del jurado de tesis**

---

Ing. Diaz Espino Miguel Ángel

**Secretario del jurado de tesis**

---

Ing. José Manuel Bruno Sarmiento

**Vocal del jurado de tesis**

## DEDICATORIA

Quiero dedicar especialmente esta tesis a mi mejor amigo, mi Padre Belisario Armando Romero Vances, que, aunque ya no esté físicamente conmigo, vivirá siempre en mi corazón; gracias por educarme con tanto amor y humildad, enseñándome que todo lo bueno se obtiene a base de sacrificio, esfuerzo y mucho trabajo. Y sé que desde el cielo, cuidas y guías mis pasos. Gracias Papá.

A mi incondicional compañera y esposa Stephanie Ruíz Mera, por creer siempre en mí, apoyarme en todo momento, y por dar estímulo a esta difícil etapa de mi vida de esposo, padre y estudiante; y, sobre todo, por el empuje del día a día que alentó la realización de nuestra meta fijada.

A mis hijos Thiago Armando y Raziel Francesco, por ser mis principales motivaciones en mi vida y las razones para seguir superándome personal y profesionalmente.

A mi Madrecita linda Esther Mas García, por su esfuerzo en educarme, por los valores forjados y por brindarme siempre ese apoyo incondicional de luchar por mis sueños, y porque más que una madre has sabido ser una amiga incondicional.

**Armando**

## AGRADECIMIENTO

Quiero agradecer especialmente al Ing. Jaime Bravo y al Ing. Miguel Vidaurre, por su paciencia y asesoría, sin sus asesoramientos no hubiera podido culminar exitosamente esta tesis.

Y a todas las personas que llegaron a mi vida universitaria, docentes y compañeros, porque guardo las enseñanzas que alguna vez me dieron.

**Armando**

## INDICE

DEDICATORIA .....	iii
AGRADECIMIENTO .....	iv
RESUMEN .....	11
ABSTRACT .....	12
CAPÍTULO I. INTRODUCCIÓN .....	13
1.1.Problema de investigación. ....	14
1.2.Antecedentes de la investigación. ....	16
1.3.Aspectos teóricos.....	18
1.4.Formulación del Problema .....	29
1.6.Delimitación de la investigación. ....	29
1.7.Justificación e importancia de la investigación. ....	29
1.8.Limitaciones de la investigación. ....	31
1.9.Objetivos.....	31
CAPÍTULO II. MATERIALES Y MÉTODOS .....	33
2.1. Tipo y diseño de la investigación .....	34
2.2. Población y muestra. ....	34
2.3. Variables .....	35
2.4.Operacionalización.....	36
2.5. Métodos, técnicas e instrumento de recolección de datos.....	36
2.6.Procedimiento para la recolección de datos .....	37
2.7.Análisis Estadístico e Interpretación de los datos .....	38
2.8.Criterios éticos .....	38
CAPÍTULO III. RESULTADOS.....	39
3.1. Resultado en tablas, gráficos y documentación.....	40
CAPÍTULO IV. DISCUSIÓN .....	80
4.1.Discusión de resultados.....	81

CAPÍTULO V. PROPUESTA DE INVESTIGACIÓN .....	83
5.1. Introducción .....	84
5.2. Entradas .....	84
5.3. Proceso .....	88
5.3.1. Planear .....	89
5.4. Hacer .....	98
5.5. Verificar .....	107
5.6. Actuar .....	112
5.7. Salida .....	121
CAPÍTULO VI. CONCLUSIONES Y RECOMENDACIONES .....	122
6.1. Conclusiones .....	123
6.2. Recomendaciones .....	124
REFERENCIAS .....	125
ANEXOS .....	128
Anexo 01. Carta para permiso de investigación .....	129
Anexo 02. Oficio N° 00056-2017-CG/D320 de respuesta a solicitud .....	130
Anexo 03. La NTP ISO/IEC 27001:2014 – Objetivos de Control y Controles de Referencia .....	131
Anexo 04. Encuesta aplicada a personal de la Línea de Producción de Microformas ....	149
Anexo 05. Relación de N° de pregunta de Encuesta con cláusulas del Anexo A de la NTP ISO/IEC 27001:2014 .....	154
Anexo 06. Manual de Seguridad de la Información para la Línea de Producción de Microformas .....	157
Anexo 07. Resultados de Urkund .....	175

## INDICE DE TABLAS

<b>Tabla 1.</b> Operacionalización de variables.....	36
<b>Tabla 2.</b> Criterios éticos .....	38
<b>Tabla 3.</b> Consolidado de respuestas de los trabajadores.....	40
<b>Tabla 4.</b> Consolidado de respuestas de los trabajadores.....	43
<b>Tabla 5.</b> Vulnerabilidades advertidas .....	46
<b>Tabla 6.</b> Vulnerabilidad N° 01, Políticas de dispositivos móviles .....	48
<b>Tabla 7.</b> Vulnerabilidad N° 02 – A. 7.2.2 Conciencia, educación y capacitación sobre la seguridad de la información. ....	51
<b>Tabla 8.</b> Vulnerabilidad N° 03 – A.8.1.4 Retorno de activos y Vulnerabilidad N° 04 – A.8.3.3 Transferencia de medios físicos.....	53
<b>Tabla 9.</b> Vulnerabilidad N° 05 – N° 08.....	56
<b>Tabla 10.</b> Vulnerabilidad N° 09 Y N° 13 .....	61
<b>Tabla 11.</b> Vulnerabilidad N° 14 - N° 15.....	64
<b>Tabla 12.</b> Vulnerabilidad N° 16 - N° 17.....	67
<b>Tabla 13.</b> Vulnerabilidad N° 18 – A.16.1.3 Reporte de debilidades de seguridad de la información .....	69
<b>Tabla 14.</b> Vulnerabilidad N° 19 – A.17.1.1 Planificación de continuidad de seguridad de la información .....	71
<b>Tabla 15.</b> Vulnerabilidad N° 20 – A.18.1.3 Protección de registros .....	72
<b>Tabla 16.</b> Plantilla – Recursos Tecnológicos.....	84
<b>Tabla 17.</b> Plantilla – Sistemas de Información .....	85
<b>Tabla 18.</b> Consolidado de respuestas afirmativas y negativas por cláusula .....	86
<b>Tabla 19.</b> Vulnerabilidades vs NTP ISO/IEC 27001:2014.....	91
<b>Tabla 20.</b> Inventario de Activos de información vs Vulnerabilidades .....	92
<b>Tabla 21.</b> Requisito de Confidencialidad (C) .....	93
<b>Tabla 22.</b> Requisito de Integridad (I) .....	93
<b>Tabla 23.</b> Requisito de Disponibilidad (D).....	94
<b>Tabla 24.</b> Inventario de Activos de información vs Vulnerabilidades e Impactos.....	94
<b>Tabla 25.</b> Matriz AMFE .....	96
<b>Tabla 26.</b> NTP vs Indicadores .....	106
<b>Tabla 27.</b> Check List Controladores.....	108
<b>Tabla 28.</b> Plan de Verificación del Manual de Seguridad de Información.....	109
<b>Tabla 29.</b> Plan de Acciones preventivas.....	112



<b>Tabla 30.</b> Plan de Acciones Correctiva .....	118
<b>Tabla 31.</b> Objetivos de control y controles .....	131
<b>Tabla 32.</b> Relación N° de Pregunta – Cláusula NTP ISO/IEC 27001:2014 .....	154



## INDICE DE FIGURAS

<b>Figura 1.</b> Gráfico de incremento porcentual de las detecciones del Win32/Houdrat en Latinoamérica durante los últimos tres meses. ....	16
<b>Figura 2.</b> Familia de estándares de la ISO 27000. ....	27
<b>Figura 3.</b> Modelo de PHVA aplicado a los procesos del SGSI. ISO/IEC 27001:2005. ....	28
<b>Figura 4.</b> Enfoque a procesos del ISO 27001:2005 ....	28
<b>Figura 5.</b> Gráfico porcentual de la Vulnerabilidad N° 01 ....	48
<b>Figura 6.</b> Captura de pantalla de una PC asignada a LPM de microformas ....	49
<b>Figura 7.</b> Captura de pantalla, reconocimiento del dispositivo móvil.....	49
<b>Figura 8.</b> Captura de pantalla, transferencia de información.....	50
<b>Figura 9.</b> Captura de pantalla, culminación de transferencia de información. ....	50
<b>Figura 10.</b> Gráfico porcentual de la Vulnerabilidad N° 02 ....	51
<b>Figura 11.</b> Captura de pantalla, página web de la ENC – Sección: Líneas de capacitación.....	52
<b>Figura 12.</b> Captura de pantalla, página web de la ENC – Sección: Subdirección Académica .....	52
<b>Figura 13.</b> Captura de pantalla, página web de la ENC – Sección: Subdirección Posgrado .....	53
<b>Figura 14.</b> Gráfico porcentual de las Vulnerabilidades N° 03 y 04 .....	54
<b>Figura 15.</b> Estación de trabajo LPM – Sede Provincial .....	54
<b>Figura 16.</b> Ordenadores en desuso de la LPM en almacén de útiles .....	55
<b>Figura 17.</b> Gráfico porcentual de las Vulnerabilidades N° 05 al 08 .....	56
<b>Figura 18.</b> Captura de pantalla – Software de LPM: Laserfiche Rio 10.2 .....	57
<b>Figura 19.</b> Captura de pantalla – Descarga de documento digital. ....	57
<b>Figura 20.</b> Captura de pantalla – Documento “09201800732” descargado .....	58
<b>Figura 21.</b> Captura de pantalla – Ingreso al Software Quick Fields .....	59
<b>Figura 22.</b> Captura de pantalla – Inicio de sesión al Software Quick Fields.....	59
<b>Figura 23.</b> Captura de pantalla – Interfaz de Software Quick Fields .....	60
<b>Figura 24.</b> Gráfico porcentual de las Vulnerabilidades N° 09 al 13 .....	61
<b>Figura 25.</b> Ingreso a oficina de trámite documentario – Estación de LPM .....	62
<b>Figura 26.</b> Oficina de trámite documentario – Estación de LPM .....	62
<b>Figura 27.</b> Pc de LPM - Oficina de trámite documentario .....	63
<b>Figura 28.</b> Equipos desatendidos - Oficina de trámite documentario .....	64
<b>Figura 29.</b> Captura de pantalla – Procedimiento de instalación de Software Photoshop CS3.....	66
<b>Figura 30.</b> Captura de pantalla – Interfaz de Software Photoshop CS3 .....	66
<b>Figura 31.</b> Gráfico porcentual de la Vulnerabilidad N° 16 y 17.....	67
<b>Figura 32.</b> Captura de pantalla – Transferencia de información a otros usuarios.....	68
<b>Figura 33.</b> Captura de pantalla – Otorgando permisos de lectura y escritura.....	68

<b>Figura 34.</b> Captura de pantalla – Culminación de transferencia de información.....	69
<b>Figura 35.</b> Gráfico porcentual de la Vulnerabilidad N° 1836.....	70
<b>Figura 37.</b> Memorando Circular N° 00039-2016-CG/TD – Control de Incidencias .....	70
<b>Figura 38.</b> Gráfico porcentual de la Vulnerabilidad N° 19 .....	71
<b>Figura 39.</b> Gráfico porcentual de la Vulnerabilidad N° 20 .....	72
<b>Figura 40.</b> Captura de pantalla, Software QuickField – Digitalización de prueba .....	73
<b>Figura 41.</b> Captura de pantalla, Software Laserfiche – Digitalización de prueba.....	74
<b>Figura 42.</b> Captura de pantalla, Software Laserfiche – Digitalización de prueba.....	74
<b>Figura 43.</b> Captura de pantalla, Software Laserfiche – Eliminación de imágenes .....	75
<b>Figura 44.</b> Captura de pantalla, Software Laserfiche – Eliminación de imágenes .....	76
<b>Figura 45.</b> Captura de pantalla, Software Laserfiche – Eliminación de documento .....	77
<b>Figura 46.</b> Captura de pantalla, Software Laserfiche – Eliminación de documento .....	77
<b>Figura 47.</b> Captura de pantalla, Software Laserfiche – Papelera de reciclaje .....	78
<b>Figura 48.</b> Ciclo PDCA para el Manual de Seguridad .....	89
<b>Figura 49.</b> Proceso Planear .....	89
<b>Figura 50.</b> Proceso HACER .....	98
<b>Figura 51.</b> Proceso VERIFICAR .....	107
<b>Figura 52.</b> Proceso ACTUAR.....	112
<b>Figura 53.</b> Carta de permiso de investigación .....	129
<b>Figura 54.</b> Oficio N° 00056-2017-CG/D320 – Respuesta de solicitud.....	130
<b>Figura 55.</b> Pág. 01 de 05 – Encuesta aplicada a personal de la LPM.....	149
<b>Figura 56.</b> Pág. 02 de 05 – Encuesta aplicada a personal de la LPM.....	150
<b>Figura 57.</b> Pág. 03 de 05 – Encuesta aplicada a personal de la LPM.....	151
<b>Figura 58.</b> Pág. 04 de 05 – Encuesta aplicada a personal de la LPM.....	152
<b>Figura 59.</b> Pág. 05 de 05 – Encuesta aplicada a personal de la LPM.....	153

**ESTUDIO PARA DETECTAR VULNERABILIDADES EN LA SEGURIDAD DEL SOFTWARE DE LA LÍNEA DE PRODUCCIÓN DE MICROFORMAS BASADO EN LA NORMA TÉCNICA PERUANA NTP ISO/IEC 27001:2014; CASO DE ESTUDIO CONTRALORÍA GENERAL DE LA REPÚBLICA DEL PERÚ.**

**STUDY TO DETECT VULNERABILITIES IN THE SECURITY OF THE SOFTWARE OF THE MICROFORMER PRODUCTION LINE BASED ON THE PERUVIAN NTP TECHNICAL STANDARD NTP ISO / IEC 27001: 2014; CASE STUDY COMPTROLLER GENERAL OF THE REPUBLIC OF PERU.**

Romero Mas, Armando Demetrio.<sup>1</sup>

## **RESUMEN**

El presente trabajo de investigación se centra en el estudio para la detección de vulnerabilidades de seguridad del software de la línea de producción de microformas de la Contraloría General de la República, basado en la exigencia de los controles de la norma técnica peruana NTP-ISO/IEC 27001:2014.

Se realizaron reuniones con la gerente y supervisores, posteriormente, para la obtención de información y recolección de datos se consideró el uso de técnicas de recopilación de información tales como: encuestas, entrevistas y otros, lográndose determinar las deficiencias para mejorar los niveles de seguridad y confiabilidad. Los resultados obtenidos de la aplicación de los controles establecidos en la Norma técnica permitieron mitigar las vulnerabilidades de seguridad encontradas, y elaborar como producto final un Manual de Seguridad de la Información.

**Palabras Claves:** Controles, Estudio, NTP-ISO/IEC 27001:2014, Microformas, Vulnerabilidades, Seguridad, Software.

---

<sup>1</sup> Bachiller en Ingeniería de Sistemas, Escuela Académica Profesional de Ingeniería de Sistemas, Universidad Señor de Sipán, Chiclayo, Perú. Email. rmasarmandodeme@crece.uss.edu.pe

## ABSTRACT

The present research focuses on the study for the detection of security vulnerabilities of the software of the microform production line of the General Comptroller of the Republic, based on the requirement of the controls of the Peruvian technical standard NTP-ISO / IEC 27001: 2014.

Meetings were held with the manager and supervisors. Data collection and collection techniques, such as: surveys, interviews and others were used to obtain information and data collection, and the deficiencies were identified in order to improve safety levels and reliability. The results obtained from the application of the controls established in the Technical Standard allowed to mitigate the security vulnerabilities found, and to elaborate as a product an Information Security Manual.

**Keywords:** Controls, Study, NTP-ISO / IEC 27001: 2014, Microforms, Vulnerabilities, Security, Software.

# CAPÍTULO I. INTRODUCCIÓN

### 1.1. Problema de investigación.

La mayoría de las entidades públicas y privadas, dependen de una que otra tecnología de información como herramienta para lograr los objetivos institucionales o para el desarrollo de sus procesos; asimismo, tienen que enfrentarse con amenazas y vulnerabilidades asociadas a los riesgos de la seguridad de la información.

La seguridad de la información es más que un problema de seguridad de datos en computadoras y servidores, se debe tener cuenta que es la información de toda una línea de producción de información confidencial del estado peruano, esta seguridad debe estar implementada y mejorada continuamente basándose en los requisitos y controles técnicos de la NTP ISO/IEC 27001:2014, orientada a proteger la propiedad intelectual y la información importante de la organización.

La seguridad de información se ha visto vulnerada en varias oportunidades, permitiendo que agentes no autorizados tengan acceso a información que se maneja en las organizaciones, así como su manipulación y posterior pérdida.

Aguilar (2011), menciona que: El sistema automatizado de digitalización de documentos (SADO) ayudará a simplificar el almacenamiento de varios documentos que se encuentran en forma física y a una mejor custodia de la información digital, pero no menciona los riesgos de seguridad a los que se encuentran propensos mencionados sistemas, por lo que se requiere realizar un estudio para la detección de vulnerabilidades que se pueden presentar en la seguridad de la información, teniendo como base normas establecidas que regulan los requisitos técnicos para la seguridad de la información.

Urbina (2012), comenta que el manejo de documentos electrónicos es una tendencia al alza en Chile, sin embargo en la actualidad la mayoría de la documentación con valor legal es manejada en papel, no existiendo un procedimiento que permita certificar copias electrónicas de documentos y mucho menos una implementación adecuada de los sistemas de seguridad; situación diferente en nuestro país, puesto que, la creación de la NTP ISO/IEC 27001:2014 se crea con la finalidad de establecer, implementar, mantener y



mejorar constantemente un sistema de seguridad de la información dentro del contexto de la organización.

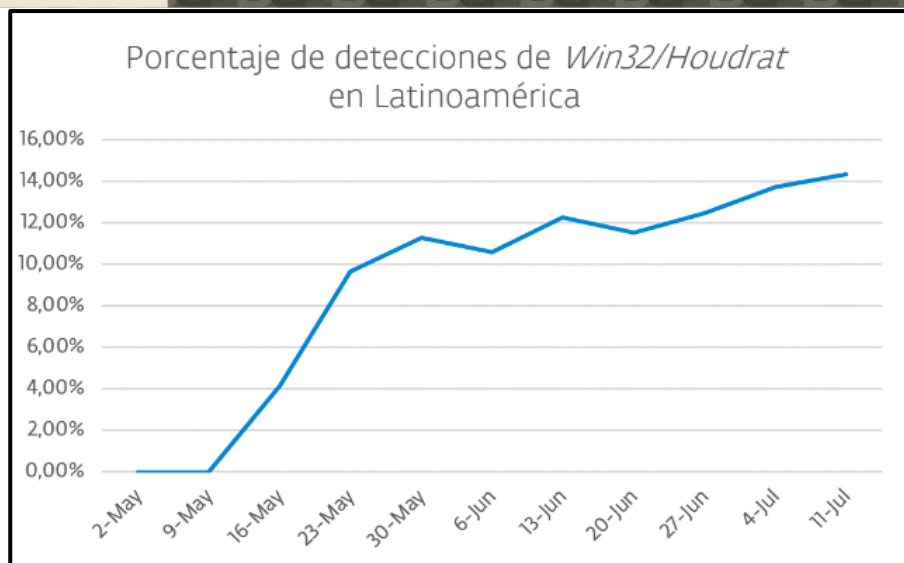
En el blog “Todos somos vulnerables a los ciberataques” del periodista Bruno Ortiz Bisso publicado en el diario El Comercio con fecha 15 de mayo de 2016, menciona la desagradable experiencia de Julián, respecto al secuestro de su información a través del malware ‘ransomware’. Así como Julián, miles de personas, empresas, instituciones y organizaciones públicas y estatales del Perú y del mundo reciben ataques de ciberdelincuentes. Según el boletín de seguridad de enero-marzo del 2016 de la empresa Kaspersky Labs, en los primeros tres meses del año se detectó que el 12,3% de sus usuarios en el Perú fueron atacados (285.004 incidentes). Por su parte, el reporte de seguridad del 2016 de la compañía ESET señala que el 40% de empresas de 14 países de Centro y Sudamérica sufrió algún incidente relacionado con un ‘malware’ en el último año. En el caso del Perú, el 51,7% de las empresas padeció este tipo de ataque.

En el Post “Crecen las amenazas en Autolt, propagación de Houdrat en Latinoamérica” de la web Welivesecurity.com, publicado el 21 de julio de 2016, nos menciona que; En el transcurso de los últimos meses, desde el Laboratorio de Investigación de ESET Latinoamérica se ha notado un gran incremento en los ataques dirigidos en Latinoamérica; uno de los últimos casos fue Cybergate, uno de los códigos maliciosos más detectados en los últimos meses en Latinoamérica, el cual se propaga con gran efectividad principalmente a través de dispositivos extraíbles. La amenaza, detectada por las soluciones de seguridad de ESET como Win32/Houdrat.A, es un archivo ejecutable desarrollado en AutoIt, en un lenguaje de scripting cada vez más utilizado por los cibercriminales.

El código malicioso fue detectado por primera vez en abril de 2016 y desde entonces ha afectado a varios países de Latinoamérica, siendo Perú, Bolivia y Ecuador los primeros de la lista, con más del 90% de las detecciones en lo que va del año. El top 10 de las detecciones lo completan otros países de la región como Colombia, México, Argentina, Chile y Brasil.

El siguiente gráfico muestra cómo la cantidad de detecciones se ha ido incrementando a lo largo de los últimos tres meses:





**Figura 1.** Gráfico de incremento porcentual de las detecciones del Win32/Houdrat en Latinoamérica durante los últimos tres meses.

**Fuente:** Welivesecurity

La Entidad requiere asegurar sus activos de información con el propósito de proteger su exactitud y totalidad con el fin de que los mismos solo sean accesibles por aquellas personas que estén debidamente autorizadas. La entidad no cuenta con una metodología para la identificación y clasificación de sus activos de información y para la valoración y tratamiento de riesgos de seguridad de la información, lo que implica, que no cuenta con una visión global del estado de su seguridad.

Es por tales motivos, que el presente trabajo de investigación tiene por finalidad identificar las vulnerabilidades en la seguridad de la línea de producción de microformas de la Contraloría Regional de la República, basándose en la aplicación de controles de la NTP ISO/IEC 27001:2014, para de esa manera asegurar el logro de los niveles de seguridad y confiabilidad de la información.

## 1.2. Antecedentes de la investigación.

Guerrero, Garcés, & Muñoz (2015) en su tesis de pregrado *“Identificación de vulnerabilidades de seguridad en el control de acceso al Sistema de Gestión Documental, mediante pruebas de testeo de red en la empresa INGELEC S.A.S.”*, busca la realización de pruebas de testeo a la red de datos para el diagnóstico de vulnerabilidades en el control de acceso al Sistema de Gestión Documental de la empresa INGELEC S.A.S, de acuerdo

al dictamen revelado se ejecuta la evaluación y su impacto, con lo anterior se formaliza un planteamiento de estrategias de mitigación de riesgos encontrados para la prevención y fortalecimiento de la seguridad en el control de acceso del Sistema de Gestión Documental. Se empleó la aplicación de software libre OpenVAS (Sistema Abierto para Evaluación de Vulnerabilidades), el cual permite evidenciar la seguridad y las vulnerabilidades existentes en los sistemas de información.

Ríos (2014) en su investigación de pregrado *“Técnicas y herramientas de análisis de vulnerabilidades de una red”*, ofrece una visión general del estado del conjunto de herramientas disponibles para el análisis y explotación de vulnerabilidades en sistemas informáticos y más concretamente en redes de ordenadores. Por un lado, ha procedido a describir analíticamente el conjunto de herramientas de software libre que se ofrecen en la actualidad para analizar y detectar vulnerabilidades en sistemas informáticos. Se ha descrito el funcionamiento, las opciones, y la motivación de uso para dichas herramientas, comparándolas con otras en algunos casos, describiendo sus diferencias en otros, y justificando su elección en todos ellos. Por otro lado se ha procedido a utilizar dichas herramientas analizadas con el objetivo de desarrollar ejemplos concretos de uso con sus diferentes parámetros seleccionados observando su comportamiento y tratando de discernir qué datos son útiles para obtener información acerca de las vulnerabilidades existentes en el sistema, Además, se ha desarrollado un caso práctico en el que se pone en práctica el conocimiento teórico presentado de forma que el lector sea capaz de asentar lo aprendido comprobando mediante un caso real la utilidad de las herramientas descritas. Los resultados obtenidos han demostrado que el análisis y detección de vulnerabilidades por parte de un administrador de sistemas competente permite ofrecer a la organización en cuestión un conjunto de técnicas para mejorar su seguridad informática y así evitar problemas con potenciales atacantes.

Tola (2015) En su proyecto de Tesis de grado *“Implementación de un sistema de gestión de seguridad de la información para una empresa de consultoría y auditoría, aplicando la norma ISO/IEC 27001”*; pretende dar una adecuada solución de seguridad a la empresa A&CGroup S.A, a través de la implementación de un Sistema de Seguridad de la Información (SGSI), tomando como base estándar la norma ISO 27001:2005. Tomó como punto de partida la revisión de los conceptos básicos que le van a permitir tener una visión clara del conjunto de acciones necesarias para que la entidad involucrada pueda contar con

un sistema para la seguridad y gestión de riesgos de la información. Por otra parte, presentó los antecedentes de su proyecto, tales como la descripción del problema, la solución de propuesta, y los objetivos correspondientes. Luego detalla el levantamiento de información necesaria para la implementación del SGSI, y describe los tipos de metodología a utilizar, teniendo como principales referentes la metodología PDCA, metodología para la gestión de riesgos, y metodología MAGERIT; lo cual en conjunto, le permitió que una vez identificados los riesgos a los que se encontraban expuestos los activos de información, la organización debe implementar controles o salvaguardas, teniendo presente analizar el costo beneficio de la implementación de estos.

Cavalcanti (2012) en su tesis de pregrado *“Sistema para el análisis y Gestión de riesgos”*, propone mejorar el manejo de riesgos para la empresa GMD S.A, a través de una secuencia de actividades humanas que incluye, evaluación de riesgos, estrategias de desarrollo, mitigación del riesgo, todo esto, utilizando un seguimiento y control de riesgos. Las estrategias incluyen transferir el riesgo a otra parte, evadir el riesgo, reducir los efectos negativos del riesgo y aceptar algunas o todas las consecuencias de un riesgo particular.

Además, diseñó un nuevo material que refleja el crecimiento de los conocimientos y prácticas en el manejo de gestión de riesgos en seguridad de la información, se documentó las prácticas, herramientas, técnicas y otros elementos pertinentes generalmente reconocidos como buenas prácticas.

El beneficio por parte de la empresa GMD fue obtener una evaluación de riesgos mediante un sistema Web, manteniendo las técnicas y prácticas que se realizan en este momento de forma manual. Generando así los medios para evaluar las amenazas existentes de una forma adecuada y eficiente

### **1.3. Aspectos teóricos**

En la presente investigación se hace uso de los siguientes conceptos tales como: Seguridad Informática, Seguridad en los Sistemas Informáticos, Propiedades de la Seguridad Informática, Objetivos de la Seguridad, Términos de Riesgos, Factores de Riesgos, Análisis del Riesgo y su Evaluación, Medidas de Seguridad, Estandarización y Seguridad de las Tecnología de Información, Sistema de Gestión de Seguridad de la Información, y Herramientas para el Análisis de Riesgo entre otros.

## Seguridad Informática

Según Alexander (2007), Define a la seguridad como aquellas reglas técnicas y actividades destinadas a prevenir, proteger y resguardar lo que es considerado como susceptible de robo, pérdida o daño, ya sea de manera personal, grupal o empresarial, por esta razón la información es el elemento principal a proteger, resguardar y recuperar en las Instituciones Militares.

Es necesario considerar otras definiciones importantes al momento de hablar de seguridad informática, estas son:

**Activo:** Recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos. Cualquier cosa que tenga valor para la organización.

**Amenaza:** Es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

**Impacto:** Consecuencia de la materialización de una amenaza.

**Riesgo:** Posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la organización.

**Vulnerabilidad:** Posibilidad de ocurrencia de la materialización de una amenaza sobre un activo.

**Ataque:** Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

**Desastre o Contingencia:** Interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras necesarias para la normal operación de un negocio.

Un riesgo y una vulnerabilidad se podrían englobar en un mismo concepto, una

definición más informal denota la diferencia entre riesgo y vulnerabilidad, de modo que la vulnerabilidad está ligada a una amenaza y el riesgo a un impacto.

En el área de informática, existen varios riesgos tales como: ataque de virus, códigos maliciosos, gusanos, caballos de Troya y hackers; no obstante, con la adopción de Internet como instrumento de comunicación y colaboración, los riesgos han evolucionado y, ahora, las empresas deben enfrentar ataques de negación de servicio y amenazas combinadas; es decir, la integración de herramientas automáticas de "hackeo", accesos no autorizados a los sistemas y capacidad de identificar y explotar las vulnerabilidades de los sistemas operativos o aplicaciones para dañar los recursos informáticos.

Para los ataques de negación de servicio, el equipo de cómputo ya no es un blanco, es el medio a través del cual es posible afectar todo el entorno de red; es decir, anular los servicios de la red, saturar el ancho de banda o alterar el WebSite de la institución. Los riesgos están en la red y en menor grado en la computadora.

En las Instituciones Militares se protegerá la información que se trasmite a través del Sistema de Comunicaciones para la utilización de los Sistemas Informáticos por parte de los usuarios de los Repartos Militares.

### **Seguridad en los sistemas informáticos**

Según Hernández (2003), La alta informatización de la sociedad actual ha conllevado el aumento de los denominados delitos informáticos, por lo cual señala que un sistema informático es seguro si se puede confiar en él y si se comporta de acuerdo a lo esperado.

La seguridad en los sistemas informáticos es un conjunto de soluciones técnicas, métodos y planes con el objetivo de que la información que trata los sistemas informáticos sea protegida, así como establecer un plan de seguridad en el cual se definan las necesidades y objetivos en cuestiones de seguridad.

Es primordial indicar que la seguridad genera un costo y que la seguridad absoluta



es imposible, por tal motivo se debe definir cuáles son los objetivos y a qué nivel de seguridad se quiere llegar, por lo tanto, la seguridad en los sistemas informáticos de las instituciones militares se tiene que planificar haciendo un análisis del costo-beneficio.

### **Propiedades de la seguridad informática**

Según Alexander (2007), Se tomará en cuenta las definiciones sobre los atributos o propiedades principales que debe brindar un sistema de seguridad:

#### **Confidencialidad:**

Controlar quién puede leer la información (acceso) e impedir que información confidencial sea entregada a receptores no autorizados. Propiedad de que la información no está disponible o divulgada a individuos, entidades o procesos no autorizados.

#### **Disponibilidad:**

Asegurar que los sistemas trabajen prontamente con un buen desempeño y garantizar protección y recuperación del sistema en caso de ataque o desastre. Propiedad de estar accesible y utilizable bajo demanda de una entidad autorizada.

#### **Integridad:**

Asegurar que la información recibida sea exactamente igual a la información enviada, es decir que no ha sido dañada por errores de transmisión o alterada intencionalmente en su contenido o en su secuencia. Propiedad de salvaguardar la exactitud y la totalidad de los activos.

#### **Autenticidad:**

Garantizar que la información no es una réplica de información vieja la cual se quiere hacer pasar por información fresca, y que efectivamente proviene de una fuente genuina.

#### **Identificación y control de acceso:**

Verificar la identidad de las personas. Autorizar y controlar quién y cómo se accede a los datos y los recursos de un sistema.

La confidencialidad y el control de acceso trabajan conjuntamente para proteger la información contra personas no autorizadas, mientras que permiten que los usuarios autorizados tengan acceso utilizando técnicas de identificación, usualmente por medio del nombre de usuario (username) más su contraseña (password).

La integridad se garantiza por medio de bits de chequeo (checksums) que se añaden a la información y la autenticidad por medio de extractos (hash) y otros mecanismos.

### **Términos de riesgo**

Según Freitas (2009), La problemática en la seguridad de la información ha sido enfrentada con criterios tomados de otras disciplinas. Estos enfoques han dado lugar al uso de términos diferentes con significados no muy claros, tales como los siguientes casos:

#### **a) Valorización del riesgo:**

Analizar las amenazas a un sistema de información, las vulnerabilidades del mismo y el impacto potencial si se concretan dichas amenazas.

#### **b) Evaluación del riesgo:**

Evaluación del riesgo respecto algún criterio de seguridad, por ejemplo, una norma.

#### **c) Análisis de riesgo:**

Identificación y valuación de los niveles de riesgo de activos, amenazas y vulnerabilidades.

#### **d) Gestión de riesgo:**

Determinación de la estrategia efectiva en costo, del tratamiento y procedimientos a aplicar a partir de los resultados de la valuación, por ejemplo: 1) Aceptarlos, 2) Minimizarlos, identificando, seleccionando e implementando contramedidas (salvaguardas) para su reducción a niveles aceptables, y 3) Transferirlos.



**Factores de riesgo:**

Según Alexander (2007), El riesgo es la combinación de una amenaza que aprovecha alguna vulnerabilidad de un activo para impactarlo y causarle daño, señala los siguientes factores de riesgos:

**Activos:**

Cualquier bien que necesite protección, frente a posibles situaciones de pérdida de condiciones como son la Confidencialidad, Integridad o Disponibilidad. La confidencialidad es la propiedad de que la información no está disponible o divulgada a individuos, entidades o procesos no autorizados, la integridad es la propiedad de salvaguardar la exactitud y la totalidad de los activos y la disponibilidad es la propiedad de estar accesible y utilizable bajo demanda de una entidad autorizada.

Un activo de información es algo a lo que una institución le asigna un valor y, por lo tanto, la organización debe proteger. Asimismo, los clasifica en las siguientes categorías:

Activos de información (Datos, manuales de usuarios)

Documentos de papel (contratos)

Activos de software (aplicación, software de sistemas)

Activos físicos (computadoras, medios magnéticos)

Personal (Clientes, personal)

Imagen de la institución y reputación

Servicios (comunicaciones)

Como se observa, los activos de información son muy amplios es por eso que señala, que se debe realizar un correcto análisis y una evaluación del riesgo y establecer adecuadamente el modelo ISO 27001:2005.

En las Instituciones Militares, el proceso de identificación y de tasación de activos debe realizarlo un grupo multidisciplinario compuesto por personas involucradas en los procesos y subprocesos que abarca el alcance del modelo.

Los activos se consideran y categorizar por su criticidad en cuanto a lo que significan para las operaciones. El análisis tiende a establecer una cantidad de niveles que generalmente no baja de cinco y que en algunos casos puede llegar a diez.

### **Vulnerabilidades:**

Son los puntos débiles relacionados con los activos organizacionales, operacionales, físicos y de sistemas TI en las Instituciones.

Los niveles de vulnerabilidad se pueden estimar en función de: severidad, dado por los recursos necesarios para aprovechar la vulnerabilidad y el efecto en el activo, y el grado de exposición, extensión del efecto básico, facilitando la explotación de otras vulnerabilidades del mismo activo y/o se extiende a otros activos.

Las amenazas son acciones que pueden causar daño en un activo de las Instituciones Militares. Se las puede clasificar por fuerza mayor, deficiencias organizacionales, fallas humanas, fallas técnicas y actos deliberados.

Los niveles de vulnerabilidad pueden estimarse de acuerdo a la capacidad y motivación del agente provocador, la concreción de una amenaza provoca un impacto en un activo, dicho impacto y la probabilidad de ocurrencia a lo largo del tiempo pueden usarse como medida del efecto de una amenaza.

### **Análisis del riesgo y su evaluación**

El análisis del riesgo es la utilización sistemática de la información para identificar las fuentes y estimar el riesgo (NTE INEN, ISO/IEC 27002:2009, 2009). El objetivo del análisis del riesgo es identificar y calcular los riesgos basados en la identificación de los activos, y en el cálculo de las amenazas y vulnerabilidades.

Los riesgos se calculan de la combinación de los valores de los activos, que expresan el impacto de pérdidas por confidencialidad, integridad y disponibilidad y del cálculo de la posibilidad de que amenazas y vulnerabilidades relacionadas se junten y causen un incidente.

En las Instituciones Militares una vez efectuado el cálculo del riesgo por cada activo, en relación de su amenaza, se debe determinar cuáles son aquellas amenazas cuyos riesgos son los más significativos, este proceso se denomina evaluación del riesgo.

Luego de analizar el riesgo, se debe iniciar un proceso de toma de decisiones con respecto a cómo se tratará el riesgo, la decisión está influenciada por dos factores:

El posible impacto si el riesgo se pone de manifiesto

Qué tan frecuente puede suceder, estos factores dan una idea de la pérdida esperada si el riesgo ocurriera, si nada se hiciera para mitigar este riesgo.

Se debe seguir las siguientes estrategias para el tratamiento del riesgo:

#### **Reducción del riesgo:**

Para todos aquellos riesgos donde la opción de reducirlos se ha tomado, se deben implementar controles apropiados para poder reducirlos al nivel que se haya definido como aceptable.

Estos controles pueden reducir el riesgo estimado en dos maneras: reduciendo la posibilidad de que la vulnerabilidad sea explotada por la amenaza y reduciendo el posible impacto si el riesgo ocurriese.

#### **Aceptar el riesgo:**

Muchas veces se presenta la situación en la cual la organización no encuentra controles para mitigar el riesgo, o en la cual la implantación de controles tiene un costo mayor que las consecuencias del riesgo.

#### **Transferencia del riesgo:**

La transferencia del riesgo es una opción cuando es difícil reducir o controlar el riesgo a un nivel aceptable, la alternativa de transferencia a una tercera parte es más económica ante estas circunstancias.

Existen mecanismos para transferir los riesgos a otra organización; por ejemplo,

utilizar una aseguradora o la utilización de terceros para manejar activos o procesos críticos, en la medida en que tengan capacidad de hacerlo.

### **Evitar el riesgo:**

Se entiende cualquier acción orientada a cambiar las actividades, o la manera de desempeñar una actividad comercial en particular, para así evitar la presencia del riesgo.

El riesgo puede evitarse por medio de: no desarrollar ciertas actividades comerciales (por ejemplo: la no utilización de internet), mover los activos de un área de riesgo y decidir no procesar información particularmente sensitiva.

### **Sistema de Gestión de Seguridad de la Información.**

El modelo ISO 27001:2005 define a un SGSI como “la parte del sistema de gestión global, basada en una orientación a riesgo de negocio, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información”.

El modelo ISO 27001:2005 define a un Sistema de Gestión de Seguridad de la Información como “la parte del sistema de gestión global, basada en una orientación a riesgo de negocio, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información”.

ISO 27001:2005 define la seguridad de la información como la “preservación de la confidencialidad, integridad, no repudio y confiabilidad”. A continuación, se hace referencia a la Norma ISO 27001:2005, la nueva familia 27000.

### **ISO/IEC 27001:2005**

El origen es británico y en el año 2005, la Organización Internacional para la Normalización (ISO) la oficializó como norma.

En marzo de 2006, posteriormente a la publicación de la ISO 27001:2005, BSI publicó la BS 7799-3:2006, la cual está centrada en la gestión del riesgo de los sistemas de información y servirá como base a la ISO 27005.

ISO 27005: En fase de desarrollo publicada en el año 2008. Consiste en una guía para la gestión del riesgo de la seguridad de información y sirve de apoyo a la ISO 27001 y a la implantación de un SGSI. Se basa en la BS 7799-3:2006.

<b>ISO 27000 SGSI</b> "Fundamentos y vocabularios"	<b>ISO/IEC 27001:2006</b> Requerimientos	<b>ISO/IEC 27002:2007</b> (ISO 17799: 2005)
<b>ISO/IEC 27003</b> "Lineamientos para la Implementación"	<b>ISO/IEC 27004</b> Lineamientos "Métrica y Mediciones"	<b>ISO/IEC 27005 SGSI</b> Lineamientos "Gestión del riesgo"

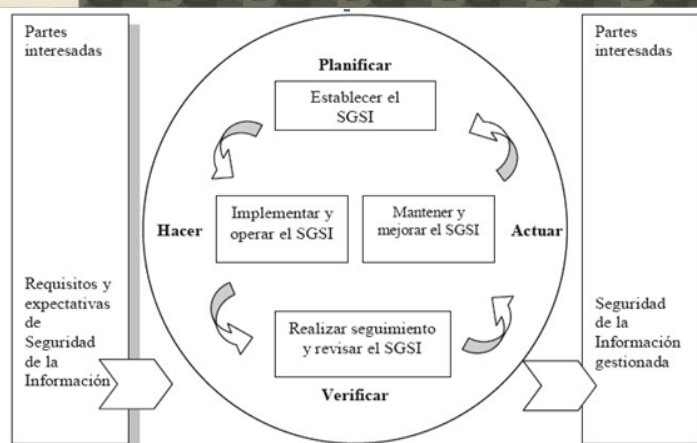
**Figura 2.** Familia de estándares de la ISO 27000.

Fuente: ISO 27000

ISO 27006: Publicada en febrero de 2007. Especifica los requisitos para la acreditación de entidades de auditoria y certificación de los SGSI. Esta norma adopta un enfoque basado en procesos para establecer, implementar, operar, realizar seguimiento, revisar, mantener y mejorar el SGSI de una organización.

Esta norma adopta el modelo "Planificar – Hacer – Verificar – Actuar" (PHVA), el cual es aplicado para estructurar todos los procesos del SGSI, la Figura 03, ilustra cómo un SGSI toma como entrada los requisitos y expectativas de seguridad de la información.

Alexander (2007), señala que el modelo ISO 27001:2005 está diseñado bajo una óptica de enfoque a procesos. El SGSI está conceptualizado para funcionar en cualquier tipo de organización, operando bajo el enfoque de procesos.



**Figura 3.** Modelo de PHVA aplicado a los procesos del SGSI. ISO/IEC 27001:2005.

**Fuente:** Alberto, A. (2007).

En la Figura 04, se ilustra la presentación de los distintos componentes del modelo ISO 27001:2005, bajo la perspectiva de procesos, el modelo está concebido para que opere con base en insumos provenientes de clientes, proveedores, usuarios, accionistas, socios y otras partes interesadas.

El modelo ISO 27001:2005, en su óptica de procesos, también permite que cada organización influencie el desempeño del modelo a través de consideraciones estratégicas, tales como objetivos y políticas.



**Figura 4.** Enfoque a procesos del ISO 27001:2005

**Fuente:** Alberto, A. (2007).



#### **1.4. Formulación del Problema**

¿Cómo identificar vulnerabilidades en la seguridad del software de la línea de producción de microformas de la Contraloría General de la República del Perú?

#### **1.5. Hipótesis**

A través de un estudio de detección de vulnerabilidades de seguridad de información basado en la aplicación de controles de la NTP ISO/IEC 27001:2014, se establecerán mecanismos adecuados para mitigar riesgos de seguridad de la información que se puedan presentar en la línea de producción de Microformas de la Contraloría General de la República del Perú.

#### **1.6. Delimitación de la investigación.**

La investigación se realizó en la Región de Lima, Provincia de Lima, distrito de Jesús María, en el Dpto. de Gestión Documentaria de la sede Central de la Contraloría General de la República del Perú.

##### **Sujetos / objetos que participaron en la investigación.**

**Sujetos:** Operarios, Supervisores, Profesionales de control de calidad, Fedatarios y Gerente General

**Objetos:** Accesos, procesos, reportes, usuarios, microformas y otros.

##### **Período de tiempo en el que se realizó la investigación.**

Enero – Julio de 2017

#### **1.7. Justificación e importancia de la investigación.**

##### **Académica:**

Agregar nuevo material que refleje el crecimiento de los conocimientos, y prácticas en el análisis de aplicación de normas de seguridad de la información, y de esa manera ampliar el conocimiento en el uso de técnicas de recopilación y evaluación de información, que ayudará a futuros estudiantes a cuantificar y mejorar el nivel de cumplimiento de los indicadores establecidos para la determinación del estado actual de la situación problema.



**Social:**

La seguridad de la información es una responsabilidad y compromiso de gran relevancia intrínseca de la Contraloría General de la República, teniendo como referencia los diferentes temas de importancia que se desarrollan en la entidad, razón por la cual se debe adoptar los mecanismos esenciales para la protección de la información y no estar expuesta a ataques informáticos.

**Tecnológica:**

La información digital que se maneja, es el activo más importante de la organización, para lo cual las personas encargadas de la seguridad de información, deben establecer procedimientos y herramientas eficientes para el envío de datos de una forma segura.

Las normas técnicas establecen un determinado nivel de calidad y seguridad y por tanto su cumplimiento garantiza la obtención de una calidad final uniforme. Las normas técnicas evolucionan a menor velocidad que las transformaciones tecnológicas, por lo tanto, los responsables de aplicar estas normas deben utilizar las ediciones apropiadas junto con una apropiada tecnología de seguridad.

**Económica:**

En el corto plazo pueden existir costos vinculados a la implantación de controles de seguridad, pero estos deben ser vistos como inversiones a mediano y largo plazo. La implementación de dichos controles suele redundar en mejoras. Los beneficios surgen de, por ejemplo, la reducción de gastos de reparación o reconstrucción de información digital almacenada en los servidores, esto debido al ataque de hackers o de personas malintencionadas.

**Institucional:**

La realización del estudio para la detección de vulnerabilidades de seguridad de información en la línea de producción de microformas de la CGR, permitirá conocer las condiciones actuales de seguridad de información de la línea, y la posterior aplicación de controles referidos a la NTP ISO/IEC 27001:2014 ayudará a establecer mecanismos para la mitigación de riesgos y la elaboración de un manual de seguridad de la información, para



que tanto en el presente como en el futuro puedan mantener un sistema de gestión de la información confiable, íntegra y disponible, que además prevendrá los riesgos a los cuales estarían expuestos, conllevando a mejorar los servicios que brindan la organización y mantener así los principios de reserva y confiabilidad, así como darle un mejor ciclo de vida a la seguridad de la información, activo muy importante en la entidad que motivará a los ciudadanos en apostar y creer en la Contraloría General de la República, que tendrá como fortaleza la seguridad de la información que se maneja, factor resaltante a tener en cuenta cuando requiera de sus servicios de la Institución.

La presente investigación permitirá realizar el análisis de seguridad detectando vulnerabilidades en la línea de producción de microformas, a través de la aplicación de controles de la NTP ISO/IEC 27001:2014, y así evaluar el riesgo y las posibilidades reales de acceder, interceptar y modificar la información digital de la Contraloría General de la República; para que posteriormente a través de la elaboración de un manual de seguridad de la información se pueda prevenir y mejorar la seguridad en el control de accesos de la Línea de Producción de Microformas.

## **1.8. Limitaciones de la investigación.**

Para el desarrollo del presente trabajo se necesitó el respaldo de la alta dirección, puesto que, se tenía que contar con el compromiso y apoyo de los mismos, y la limitación estaba en la disponibilidad de tiempo con la que contaban para las reuniones y las previas autorizaciones de ingreso.

No todos los trabajadores se encuentran laborando en la Sede central (Lima), por lo que se tiene que hacer coordinaciones con personal de provincias, y esto, limitó en el avance de la investigación.

## **1.9. Objetivos.**

### **Objetivo general.**

Detectar las vulnerabilidades de seguridad del software de la línea de producción de microformas de la Contraloría General de la República a través de la aplicación de la NTP ISO/IEC 27001:2014.

**Objetivos específicos.**

- a) Realizar un análisis de la seguridad de información de la línea de producción de microformas de la Contraloría General de la República.
- b) Seleccionar los controles recomendados por la norma técnica peruana NTP ISO/IEC 27001:2014 que servirán para la mitigación de vulnerabilidades de seguridad de información de la línea de producción de microformas de la Contraloría General de la República.
- c) Listar las vulnerabilidades encontradas e identificar las de alto índice de riesgo y el tratamiento que se le deben dar a través de planes de acciones correctivas y preventivas.
- d) Elaborar un Manual de Seguridad de la Información para la Línea de Producción de Microformas de la Contraloría General de la República.

# **CAPÍTULO II. MATERIALES Y MÉTODOS**

## 2.1. Tipo y diseño de la investigación

### 2.1.1. Tipo:

Investigación Cuantitativa: Este tipo de investigación se apoya en la información levantada, obtenida mediante encuestas en el lugar donde se desarrolla cada proceso, basándose en la recopilación y análisis de datos numéricos obtenidos del proceso de recolección de información.

### 2.1.2. Diseño:

El diseño de la investigación es experimental, ya que se realiza la aplicación de controles de la NTP ISO/IEC 27001:2014 para detectar vulnerabilidades en la seguridad de información de la línea de producción de microformas de la Contraloría General de la República del Perú.

## 2.2. Población y muestra.

### 2.2.1. Población:

La población que se está considerando en la presente investigación son la totalidad de trabajadores del Departamento de Gestión Documentos de la Contraloría General de la República que operan con los softwares de la línea de producción de Microformas, tales como: operarios de preparación, digitalizadores, profesionales de control de calidad, asistentes de fedatario, fedatario informático, operarios de armado, monitores, supervisores y gerente del área. Cuya población se totaliza en 60 empleados.

### 2.2.2. Muestra:

Para el estudio y análisis de datos, se realizó un muestreo basado en la fórmula para la población finita:

$$n = \frac{N * Z_{\infty}^2 * p * q}{d^2 * (N - 1) + Z_{\infty}^2 * p * q}$$

n = Muestra

N = Población

p = Proporción esperada, para este caso el 50% (0.5)

q = Proporción no esperada, para este caso el 50 % (0.5)

d = Nivel de error, para este caso 5%

Z = Coeficiente según el nivel de confianza, para este caso el 95% (1.96)

Sustituyendo valores:

n = ?

N = 60

p = 0.5

q = 0.5

d = 0.05

Z = 1.96

$$n = \frac{N * Z_{\infty}^2 * p * q}{d^2 * (N - 1) + Z_{\infty}^2 * p * q}$$

$$n = \frac{60 * (1.96)^2 * 0.5 * 0.5}{(0.05)^2 * (60 - 1) + (1.96)^2 * 0.5 * 0.5}$$

$$n = \frac{57.624}{0.1475 + 0.9604}$$

$$n = \frac{57.62}{1.1079}$$

$$n = 52$$

Es factible que con un número de 52 colaboradores a entrevistar y encuestar se puede lograr una apreciación muy real de la situación actual.

### 2.3. Variables

#### Variable Independiente

Estudio para detectar vulnerabilidades de seguridad.

#### Variable Dependiente

Seguridad de información



## 2.4. Operacionalización

*Tabla 1. Operacionalización de variables*

Variables	Dimensiones	Indicadores	Técnicas e Instrumentos de Recolección de Datos
Estudio para detectar vulnerabilidades de seguridad.	<ul style="list-style-type: none"> <li>• Establecer los controles que se usaran para la detección de vulnerabilidades</li> <li>• Elaborar los planes de acciones que se usarán para la mitigación de riesgos.</li> <li>• Vulnerabilidades de Sistemas de Información</li> </ul>	<ul style="list-style-type: none"> <li>• Frecuencia de cumplir con las políticas de seguridad.</li> <li>• Frecuencia de riesgos a los recursos de información</li> <li>• Incidencias de seguridad de los usuarios.</li> <li>• Nivel de gestión de la seguridad de la información del software de la línea de producción de Microformas.</li> </ul>	<ul style="list-style-type: none"> <li>• Encuestas aplicadas al personal del área o conocimientos de Ingeniería de sistemas y computación</li> <li>• Entrevistas aplicadas al personal del área o conocimientos de Ingeniería de sistemas y computación</li> </ul>
Seguridad de información	<ul style="list-style-type: none"> <li>• Puntos débiles</li> <li>• Aplicaciones</li> <li>• Red</li> <li>• Riesgos</li> <li>• Establecer el diseño de un Sistema de gestión de Seguridad de la Información.</li> </ul>	<ul style="list-style-type: none"> <li>• Accesos definidos a los tipos de usuarios.</li> <li>• Filtración de información de contraseñas.</li> <li>• Roles de Usuarios, operarios como supervisores.</li> <li>• Normas Técnicas Peruanas ISO/IEC 27001:2014</li> </ul>	<ul style="list-style-type: none"> <li>• Análisis de las encuestas.</li> <li>• Cuadros estadísticos</li> </ul>

**Nota.** Fuente: Elaborado por el autor

## 2.5. Métodos, técnicas e instrumento de recolección de datos.

Para la recolección de datos se utilizó:

**Encuestas:** Se realizó a colaboradores del Departamento de Gestión Documentaria que hayan trabajado con el software de producción de Microformas.



**Entrevistas:** Es un instrumento importante de la investigación y permite obtener resultados subjetivos del encuestado, es personal y no anónimo, se aplicó principalmente a personal supervisor, profesionales de control de calidad y fedatarios informáticos.

**Análisis documentario (AD):** el AD, es una investigación que se basa en documentación reunida, seleccionada y analizada debido a que están en presentación de “documentos” generados por la sociedad para analizar un determinado fenómeno. Es también llamada como estudio basado en fuentes secundarias, se trabajó a través de la recolección de estudios realizados anteriormente como tesis de grado que se han realizado, información registrada en documentos y material impreso: libros, revistas especializadas, informes técnicos, bibliotecas, archivos.

#### **En las técnicas de investigación:**

**Bibliográficas:** Se realizó por medio de campo.

**Análisis de documentación y el Fichaje:** A través de encuestas y reuniones.

#### **2.6.Procedimiento para la recolección de datos**

Para el presente proyecto de investigación se empleó instrumentos para el levantamiento de la información tales como las encuestas, entrevistas y análisis documentario.

**Encuesta:** Con el fin de obtener un análisis estadístico se realizó 114 preguntas a 65 colaboradores del Departamento de Gestión Documentaria que hayan trabajado con el software para la producción de microformas, las encuestas se realizaron diariamente, 04 encuestas por día, además, dichas encuestas se realizaron en los ambientes del Dpto. de Gestión Documentaria de la Contraloría General de la República, durante los días de lunes a viernes y a través de correo electrónico para el caso de las sedes provinciales.

**Entrevista:** Se aplicó principalmente a personal supervisor, profesionales de control de calidad y fedatarios informáticos, para los profesionales de control de calidad de las sedes provinciales se realizó entrevistas a través de video llamadas y correo electrónico.

**Análisis documentario:** Se analizó diferentes fuentes bibliográficas tales como: libros, tesis, informes, etc., relacionados a la aplicación de controles de normas técnicas para la detección vulnerabilidades de seguridad.

## 2.7. Análisis Estadístico e Interpretación de los datos

Los datos obtenidos de las entrevistas y revisión bibliográfica, permitieron elaborar cuadros estadísticos pertinentes lo cual permitió tener una idea amplia en todo lo relacionado al estudio para detectar vulnerabilidades en la seguridad del software de la línea de producción de microformas.

## 2.8. Criterios éticos

Los criterios éticos son:

**Tabla 2.** *Criterios éticos*

Criterios	Características éticas del criterio
Confidencialidad	Se asegurará la protección de la identidad de la institución y las personas que participan como informantes de la investigación.
Objetividad	El análisis de la situación encontrada se basará en criterios técnicos e imparciales.
Originalidad	Se citarán las fuentes bibliográficas de la información mostrada, a fin de demostrar la inexistencia de plagio intelectual.
Veracidad	La información mostrada será verdadera, cuidando la confidencialidad de ésta.
Derechos laborales	La propuesta de solución propiciará el respeto a los derechos laborales en la entidad de estudio.

**Nota.** Fuente: Elaborado por el autor

Por consiguiente: La confidencialidad, indica que los datos personales de los encuestados no serán publicados, para evitar la privacidad de los encuestados, las entrevistas que se realicen se consultarán al entrevistado para considerarla y que sea parte del trabajo, de lo contrario, solo se agregará un resumen de dichas entrevistas.

## CAPÍTULO III. RESULTADOS

### 3.1. Resultado en tablas, gráficos y documentación.

De la encuesta aplicada a los 60 trabajadores de la Línea de Producción de Microformas se obtuvo los siguientes resultados:

**Tabla 3.** Consolidado de respuestas de los trabajadores

N° de Pregunta		N° de Cláusula		CANTIDAD	
				SI	NO
P1	1.1	A.5	A. 5.1.1	54	6
	1.2		A. 5.1.2	50	10
P2	2.1	A.6	A. 6.1.1	59	1
	2.2		A. 6.1.2	52	8
	2.3		A. 6.1.3	50	10
	2.4		A. 6.1.4	54	6
	2.5		A. 6.1.5	50	10
	2.6		A. 6.2.1	6	54
	2.7		A. 6.2.2	53	7
P3	3.1	A.7	A. 7.1.1	54	6
	3.2		A. 7.1.2	52	8
	3.3		A. 7.2.1	54	6
	3.4		A. 7.2.2	0	60
	3.5		A. 7.2.3	54	6
	3.6		A. 7.3.1	53	7
P4	4.1	A. 8	A. 8.1.1	52	8
	4.2		A. 8.1.2	53	7
	4.3		A. 8.1.3	51	9
	4.4		A. 8.1.4	11	49
	4.5		A. 8.2.1	57	3
	4.6		A. 8.2.2	56	4
	4.7		A. 8.2.3	52	8
	4.8		A. 8.3.1	55	5
	4.9		A. 8.3.2	49	11
	4.10		A. 8.3.3	7	53
P5	5.1	A. 9	A. 9.1.1	57	3
	5.2		A. 9.1.2	5	55
	5.3		A. 9.2.1	50	10
	5.4		A. 9.2.2	49	11
	5.5		A. 9.2.3	54	6
	5.6		A. 9.2.4	53	7
	5.7		A. 9.2.5	49	11
	5.8		A. 9.2.6	50	10
	5.9		A. 9.3.1	56	4

	5.10		A. 9.4.1	11	49
	5.11		A. 9.4.2	12	48
	5.12		A. 9.4.3	54	6
	5.13		A. 9.4.4	52	8
	5.14		A. 9.4.5	6	54
P6	6.1	A. 10	A. 10.1.1	50	10
	6.2		A. 10.1.2	54	6
P7	7.1	A. 11	A. 11.1.1	8	52
	7.2		A. 11.1.2	9	51
	7.3		A. 11.1.3	55	5
	7.4		A. 11.1.4	53	7
	7.5		A. 11.1.5	51	9
	7.6		A. 11.1.6	50	10
	7.7		A. 11.2.1	53	7
	7.8		A. 11.2.2	11	49
	7.9		A. 11.2.3	54	6
	7.10		A. 11.2.4	53	7
	7.11		A. 11.2.5	55	5
	7.12		A. 11.2.6	56	4
	7.13		A. 11.2.7	3	57
	7.14		A. 11.2.8	11	49
	7.15		A. 11.2.9	50	10
P8	8.1	A. 12	A. 12.1.1	53	7
	8.2		A. 12.1.2	52	8
	8.3		A. 12.1.3	51	9
	8.4		A. 12.1.4	51	9
	8.5		A. 12.2.1	53	7
	8.6		A. 12.3.1	58	2
	8.7		A. 12.4.1	6	54
	8.8		A. 12.4.2	55	5
	8.9		A. 12.4.3	56	4
	8.10		A. 12.4.4	57	3
	8.11		A. 12.5.1	52	8
	8.12		A. 12.6.1	53	7
	8.13		A. 12.6.2	9	51
	8.14		A. 12.7.1	52	8
P9	9.1	A. 13	A. 13.1.1	7	53
	9.2		A. 13.1.2	48	12
	9.3		A. 13.1.3	49	11
	9.4		A. 13.2.1	6	54
	9.5		A. 13.2.2	55	5
	9.6		A. 13.2.3	55	5
P10	9.7	A. 14	A. 13.2.4	52	8
	10.1		A. 14.1.1	53	7

	10.2		A. 14.1.2	50	10
	10.3		A. 14.1.3	49	11
	10.4		A. 14.2.1	54	6
	10.5		A. 14.2.2	48	12
	10.6		A. 14.2.3	49	11
	10.7		A. 14.2.4	54	6
	10.8		A. 14.2.5	57	3
	10.9		A. 14.2.6	52	8
	10.10		A. 14.2.7	51	9
	10.11		A. 14.2.8	49	11
	10.12		A. 14.2.9	50	10
	10.13		A. 14.3.1	50	10
P11	11.1	A. 15	A. 15.1.1	53	7
	11.2		A. 15.1.2	49	11
	11.3		A. 15.1.3	52	8
	11.4		A. 15.2.1	50	10
	11.5		A. 15.2.2	52	8
P12	12.1	A. 16	A. 16.1.1	53	7
	12.2		A. 16.1.2	50	10
	12.3		A. 16.1.3	11	49
	12.4		A. 16.1.4	57	3
	12.5		A. 16.1.5	52	8
	12.6		A. 16.1.6	51	9
	12.7		A. 16.1.7	52	8
P13	13.1	A. 17	A. 17.1.1	9	51
	13.2		A. 17.1.2	52	8
	13.3		A. 17.1.3	50	10
	13.4		A. 17.2.1	52	8
P14	14.1	A. 18	A. 18.1.1	55	5
	14.2		A. 18.1.2	52	8
	14.3		A. 18.1.3	10	50
	14.4		A. 18.1.4	52	8
	14.5		A. 18.1.5	51	9
	14.6		A. 18.2.1	50	10
	14.7		A. 18.2.2	49	11
	14.8		A. 18.2.3	52	8

**Nota.** Fuente: Elaborado por el autor

En la tabla 3 se puede apreciar la cantidad de respuestas afirmativas y negativas de los 60 trabajadores de la LPM por pregunta, cada una de las interrogantes están relacionadas a una de las cláusulas del Anexo A de la NTP ISO/IEC 27001:2014.



Posteriormente se elaboró la tabla 4, con la finalidad de convertir las cantidades numéricas en cantidades porcentuales, para luego aplicar de manera general la condición de vulnerabilidad que nos indicará si se considerará cada uno de los controles de la NTP ISO/IEC 27001:2014 como “Control Conforme” o “Vulnerabilidad”.

La fórmula empleada para la conversión de las cantidades numéricas en cantidades porcentuales es la siguiente:

Fórmula:

$$(Cantidad\ de\ Respuestas * 100) / Total\ de\ trabajadores$$

$$Total, de trabajadores = 60$$

Condición de vulnerabilidad:

$$Meta = 80\%$$

$$Si \% es \geq 80\% = "Control\ Conforme"$$

$$Si \% es < 80\% = "Vulnerabilidad"$$

**Tabla 4.** Consolidado de respuestas de los trabajadores

CLÁUSULAS DEL ANEXO A - NTP ISO/IEC 27001:2014		PREGUNTA						RESULTADO
		N° de Pregunt a	Cant. De Resp. positivas	Cant. De Resp. Negativas	% de Trabajadore s con conocimien to	% de Trabajador es sin conocimie nto		
DESCRIPCIÓN	N°							
Políticas de seguridad de la información	A.5	A. 5.1.1	1.1	54	6	90,00%	10,00%	Control Conforme
		A. 5.1.2	1.2	50	10	83,33%	16,67%	Control Conforme
Organización de la seguridad de la información	A.6	A. 6.1.1	2.1	59	1	98,33%	1,67%	Control Conforme
		A. 6.1.2	2.2	52	8	86,67%	13,33%	Control Conforme
		A. 6.1.3	2.3	50	10	83,33%	16,67%	Control Conforme
		A. 6.1.4	2.4	54	6	90,00%	10,00%	Control Conforme
		A. 6.1.5	2.5	50	10	83,33%	16,67%	Control Conforme
		A. 6.2.1	2.6	6	54	10,00%	90,00%	Vulnerabilidad
		A. 6.2.2	2.7	53	7	88,33%	11,67%	Control Conforme
		A. 7.1.1	3.1	54	6	90,00%	10,00%	Control Conforme
Seguridad de los recursos humanos	A.7	A. 7.1.2	3.2	52	8	86,67%	13,33%	Control Conforme
		A. 7.2.1	3.3	54	6	90,00%	10,00%	Control Conforme
		A. 7.2.2	3.4	0	60	0,00%	100,00%	Vulnerabilidad

		A. 7.2.3	3.5	54	6	90,00%	10,00%	Control Conforme
		A. 7.3.1	3.6	53	7	88,33%	11,67%	Control Conforme
		A. 8.1.1	4.1	52	8	86,67%	13,33%	Control Conforme
		A. 8.1.2	4.2	53	7	88,33%	11,67%	Control Conforme
		A. 8.1.3	4.3	51	9	85,00%	15,00%	Control Conforme
		A. 8.1.4	4.4	11	49	18,33%	81,67%	Vulnerabilidad
		A. 8.2.1	4.5	57	3	95,00%	5,00%	Control Conforme
		A. 8.2.2	4.6	56	4	93,33%	6,67%	Control Conforme
		A. 8.2.3	4.7	52	8	86,67%	13,33%	Control Conforme
		A. 8.3.1	4.8	55	5	91,67%	8,33%	Control Conforme
		A. 8.3.2	4.9	49	11	81,67%	18,33%	Control Conforme
		A. 8.3.3	4.10	7	53	11,67%	88,33%	Vulnerabilidad
		A. 9.1.1	5.1	57	3	95,00%	5,00%	Control Conforme
		A. 9.1.2	5.2	5	55	8,33%	91,67%	Vulnerabilidad
		A. 9.2.1	5.3	50	10	83,33%	16,67%	Control Conforme
		A. 9.2.2	5.4	49	11	81,67%	18,33%	Control Conforme
		A. 9.2.3	5.5	54	6	90,00%	10,00%	Control Conforme
		A. 9.2.4	5.6	53	7	88,33%	11,67%	Control Conforme
		A. 9.2.5	5.7	49	11	81,67%	18,33%	Control Conforme
		A. 9.2.6	5.8	50	10	83,33%	16,67%	Control Conforme
		A. 9.3.1	5.9	56	4	93,33%	6,67%	Control Conforme
		A. 9.4.1	5.10	11	49	18,33%	81,67%	Vulnerabilidad
		A. 9.4.2	5.11	12	48	20,00%	80,00%	Vulnerabilidad
		A. 9.4.3	5.12	54	6	90,00%	10,00%	Control Conforme
		A. 9.4.4	5.13	52	8	86,67%	13,33%	Control Conforme
		A. 9.4.5	5.14	6	54	10,00%	90,00%	Vulnerabilidad
		A. 10.1.1	6.1	50	10	83,33%	16,67%	Control Conforme
		A. 10.1.2	6.2	54	6	90,00%	10,00%	Control Conforme
		A. 11.1.1	7.1	8	52	13,33%	86,67%	Vulnerabilidad
		A. 11.1.2	7.2	9	51	15,00%	85,00%	Vulnerabilidad
		A. 11.1.3	7.3	55	5	91,67%	8,33%	Control Conforme
		A. 11.1.4	7.4	53	7	88,33%	11,67%	Control Conforme
		A. 11.1.5	7.5	51	9	85,00%	15,00%	Control Conforme
		A. 11.1.6	7.6	50	10	83,33%	16,67%	Control Conforme
		A. 11.2.1	7.7	53	7	88,33%	11,67%	Control Conforme
		A. 11.2.2	7.8	11	49	18,33%	81,67%	Vulnerabilidad
		A. 11.2.3	7.9	54	6	90,00%	10,00%	Control Conforme
		A. 11.2.4	7.10	53	7	88,33%	11,67%	Control Conforme
		A. 11.2.5	7.11	55	5	91,67%	8,33%	Control Conforme
		A. 11.2.6	7.12	56	4	93,33%	6,67%	Control Conforme
		A. 11.2.7	7.13	3	57	5,00%	95,00%	Vulnerabilidad
		A. 11.2.8	7.14	11	49	18,33%	81,67%	Vulnerabilidad
		A. 11.2.9	7.15	50	10	83,33%	16,67%	Control Conforme
		A. 12.1.1	8.1	53	7	88,33%	11,67%	Control Conforme



	12	A. 12.1.2	8.2	52	8	86,67%	13,33%	Control Conforme
		A. 12.1.3	8.3	51	9	85,00%	15,00%	Control Conforme
		A. 12.1.4	8.4	51	9	85,00%	15,00%	Control Conforme
		A. 12.2.1	8.5	53	7	88,33%	11,67%	Control Conforme
		A. 12.3.1	8.6	58	2	96,67%	3,33%	Control Conforme
		A. 12.4.1	8.7	54	6	10,00%	90,00%	Vulnerabilidad
		A. 12.4.2	8.8	55	5	91,67%	8,33%	Control Conforme
		A. 12.4.3	8.9	56	4	93,33%	6,67%	Control Conforme
		A. 12.4.4	8.10	57	3	95,00%	5,00%	Control Conforme
		A. 12.5.1	8.11	52	8	86,67%	13,33%	Control Conforme
		A. 12.6.1	8.12	53	7	88,33%	11,67%	Control Conforme
		A. 12.6.2	8.13	9	51	15,00%	85,00%	Vulnerabilidad
		A. 12.7.1	8.14	52	8	86,67%	13,33%	Control Conforme
Seguridad de las comunicaciones	A. 13	A. 13.1.1	9.1	7	53	11,67%	88,33%	Vulnerabilidad
		A. 13.1.2	9.2	48	12	80,00%	20,00%	Control Conforme
		A. 13.1.3	9.3	49	11	81,67%	18,33%	Control Conforme
		A. 13.2.1	9.4	6	54	10,00%	90,00%	Vulnerabilidad
		A. 13.2.2	9.5	55	5	91,67%	8,33%	Control Conforme
		A. 13.2.3	9.6	55	5	91,67%	8,33%	Control Conforme
		A. 13.2.4	9.7	52	8	86,67%	13,33%	Control Conforme
Adquisición, desarrollo y mantenimiento de sistemas	A. 14	A. 14.1.1	10.1	53	7	88,33%	11,67%	Control Conforme
		A. 14.1.2	10.2	50	10	83,33%	16,67%	Control Conforme
		A. 14.1.3	10.3	49	11	81,67%	18,33%	Control Conforme
		A. 14.2.1	10.4	54	6	90,00%	10,00%	Control Conforme
		A. 14.2.2	10.5	48	12	80,00%	20,00%	Control Conforme
		A. 14.2.3	10.6	49	11	81,67%	18,33%	Control Conforme
		A. 14.2.4	10.7	54	6	90,00%	10,00%	Control Conforme
		A. 14.2.5	10.8	57	3	95,00%	5,00%	Control Conforme
		A. 14.2.6	10.9	52	8	86,67%	13,33%	Control Conforme
		A. 14.2.7	10.10	51	9	85,00%	15,00%	Control Conforme
		A. 14.2.8	10.11	49	11	81,67%	18,33%	Control Conforme
Relaciones con los proveedores	A. 15	A. 14.2.9	10.12	50	10	83,33%	16,67%	Control Conforme
		A. 14.3.1	10.13	50	10	83,33%	16,67%	Control Conforme
		A. 15.1.1	11.1	53	7	88,33%	11,67%	Control Conforme
		A. 15.1.2	11.2	49	11	81,67%	18,33%	Control Conforme
		A. 15.1.3	11.3	52	8	86,67%	13,33%	Control Conforme
Gestión de incidentes de seguridad de la información	A. 16	A. 15.2.1	11.4	50	10	83,33%	16,67%	Control Conforme
		A. 15.2.2	11.5	52	8	86,67%	13,33%	Control Conforme
		A. 16.1.1	12.1	53	7	88,33%	11,67%	Control Conforme
		A. 16.1.2	12.2	50	10	83,33%	16,67%	Control Conforme
		A. 16.1.3	12.3	11	49	18,33%	81,67%	Vulnerabilidad
		A. 16.1.4	12.4	57	3	95,00%	5,00%	Control Conforme
		A. 16.1.5	12.5	52	8	86,67%	13,33%	Control Conforme
		A. 16.1.6	12.6	51	9	85,00%	15,00%	Control Conforme



Aspectos de seguridad de la información en la gestión de continuidad del negocio	A. 17	A. 16.1.7	12.7	52	8	86,67%	13,33%	Control Conforme
		A. 17.1.1	13.1	9	51	15,00%	85,00%	Vulnerabilidad
		A. 17.1.2	13.2	52	8	86,67%	13,33%	Control Conforme
		A. 17.1.3	13.3	50	10	83,33%	16,67%	Control Conforme
Cumplimiento	A. 18	A. 17.2.1	13.4	52	8	86,67%	13,33%	Control Conforme
		A. 18.1.1	14.1	55	5	91,67%	8,33%	Control Conforme
		A. 18.1.2	14.2	52	8	86,67%	13,33%	Control Conforme
		A. 18.1.3	14.3	10	50	16,67%	83,67%	Vulnerabilidad
		A. 18.1.4	14.4	52	8	86,67%	13,33%	Control Conforme
		A. 18.1.5	14.5	51	9	85,00%	15,00%	Control Conforme
		A. 18.2.1	14.6	50	10	83,33%	16,67%	Control Conforme
		A. 18.2.2	14.7	49	11	81,67%	18,33%	Control Conforme
		A. 18.2.3	14.8	52	8	86,67%	13,33%	Control Conforme

**Nota.** Fuente: Elaborado por el autor

Luego, de haber aplicado en cada interrogante la condición de vulnerabilidad, se obtuvo como resultado 20 registros porcentuales menores al 80%, considerados como vulnerabilidades de seguridad de la información de la Línea de Producción de Microformas, en referencia a diferentes controles de la NTP ISO/IEC 27001:2014.

**Tabla 5.** Vulnerabilidades advertidas

N°	N° DE PREGUNTA	CLÁUSULAS DEL ANEXO A - NTP ISO/IEC 27001:2014		% TRABAJADORES CON CONOCIMIENTO EN:	RESULTADO	INDICADOR
		N° CLÁUSULA	DESCRIPCIÓN			
1	2.6	A. 6.2.1	Políticas de dispositivos móviles	10,00%	Vulnerabilidad	Carencia de medidas de seguridad en el acceso y uso de dispositivos móviles.
2	3.4	A. 7.2.2	Conciencia, educación y capacitación sobre la seguridad de la información	0,00%	Vulnerabilidad	No hay una capacitación a los trabajadores sobre conciencia de seguridad de la información
3	4.4	A. 8.1.4	Retorno de los activos	18,33%	Vulnerabilidad	No se retorna los activos de la manera adecuada una vez culminado el vínculo contractual
4	4.10	A. 8.3.3	Transferencia de medios físicos	11,67%	Vulnerabilidad	No se protege los medios de información contra el acceso no autorizado durante el transporte
5	5.2	A. 9.1.2	Acceso a redes y servicios de red	8,33%	Vulnerabilidad	Existe usuarios con demasiados accesos a los servicios de red
6	5.10	A. 9.4.1	Restricción de acceso a la información	18,33%	Vulnerabilidad	No existe una restricción en el acceso a la información.
7	5.11	A. 9.4.2	Procedimientos de ingreso seguro	20,00%	Vulnerabilidad	No existe un procedimiento de ingreso seguro a los



						sistemas de LPM
8	5.14	A.9.4.5	Control de Acceso al código fuente de los programas	10.00%	Vulnerabilidad	Carencia de restricción el acceso al código fuente de los programas
9	7.1	A. 11.1.1	Perímetro de seguridad física	13,33%	Vulnerabilidad	No hay un perímetro de seguridad definido en las sedes provinciales
10	7.2	A. 11.1.2	Controles de ingreso físico	15,00%	Vulnerabilidad	No existe un control de acceso restringido en las sedes provinciales
11	7.8	A.11.2.2	Servicios de suministro	18.33 %	Vulnerabilidad	Los equipos de LPM no están protegidos en caso de fallas de electricidad u otras alteraciones.
12	7.13	A.11.2.7	Disposición o reutilización segura de equipos	5.00 %	Vulnerabilidad	No se verifica oportunamente los equipos a reutilizar o en desuso.
13	7.14	A.11.2.8	Equipos de usuario desatendidos	18.33 %	Vulnerabilidad	No existe una protección adecuada para los equipos desatendidos
14	8.7	A.12.4.1	Registro de eventos	10.00 %	Vulnerabilidad	Carencia de registro de eventos de actividades de usuarios, excepciones, fallas y otros
15	8.13	A. 12.6.2	Restricciones sobre la instalación de software	15,00%	Vulnerabilidad	Falta de implementación de reglas de instalación de software por parte de los usuarios.
16	9.1	A.13.1.1	Controles de Red	11.37 %	Vulnerabilidad	No existe una protección adecuada de los servidores de red.
17	9.4	A. 13.2.1	Políticas y procedimientos de transferencia de información	10,00%	Vulnerabilidad	Los procedimientos formales establecidos para la transferencia de información no se cumplen
18	12.3	A. 16.1.3	Reporte de debilidades de seguridad de la información	18,33%	Vulnerabilidad	No se advierte oportunamente sospechas observadas en cuanto a la seguridad de información
19	13.1	A. 17.1.1	Planificación de continuidad de seguridad de la información	15,00%	Vulnerabilidad	No existe una planificación de continuidad en caso de situaciones adversas
20	14.3	A.18.1.3	Protección de registros	16,67%	Vulnerabilidad	Los registros carecen de protección contra pérdida, eliminación, alteración y otros.

**Nota.** Fuente: Elaborado por el autor

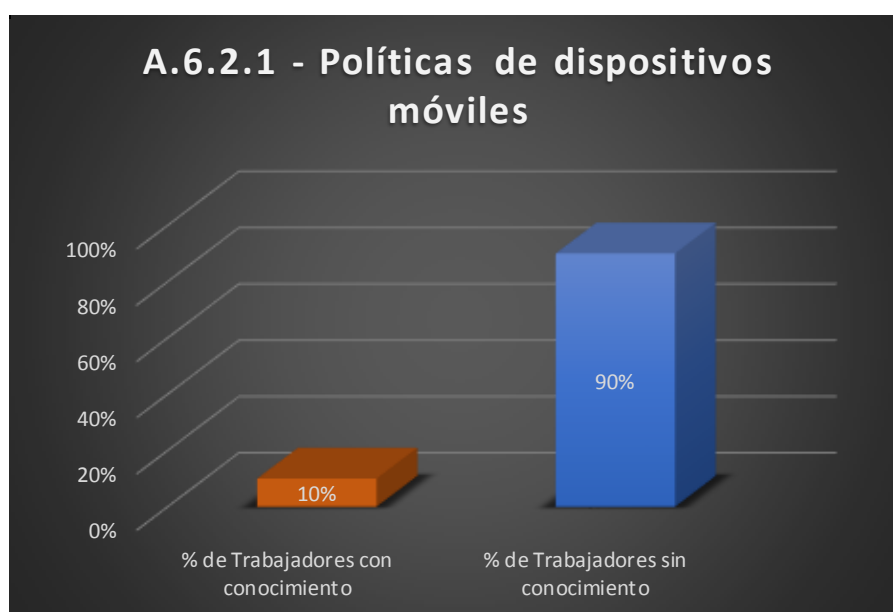


## Tablas, gráficos y documentación – Vulnerabilidades

**Tabla 6.** Vulnerabilidad N° 01, Políticas de dispositivos móviles

CLÁUSULAS DEL ANEXO A - NTP ISO/IEC 27001:2014			PREGUNTA					RESULTADO
			N° de Pregunta	Cant. De Resp. positivas	Cant. De Resp. Negativas	% de Trabajadores con conocimiento	% de Trabajadores sin conocimiento	
DESCRIPCIÓN	N°							
Organización de la seguridad de la información	A.6	A. 6.2.1	2.6	6	54	10,00%	90,00%	Vulnerabilidad

**Fuente:** Elaborado por el autor

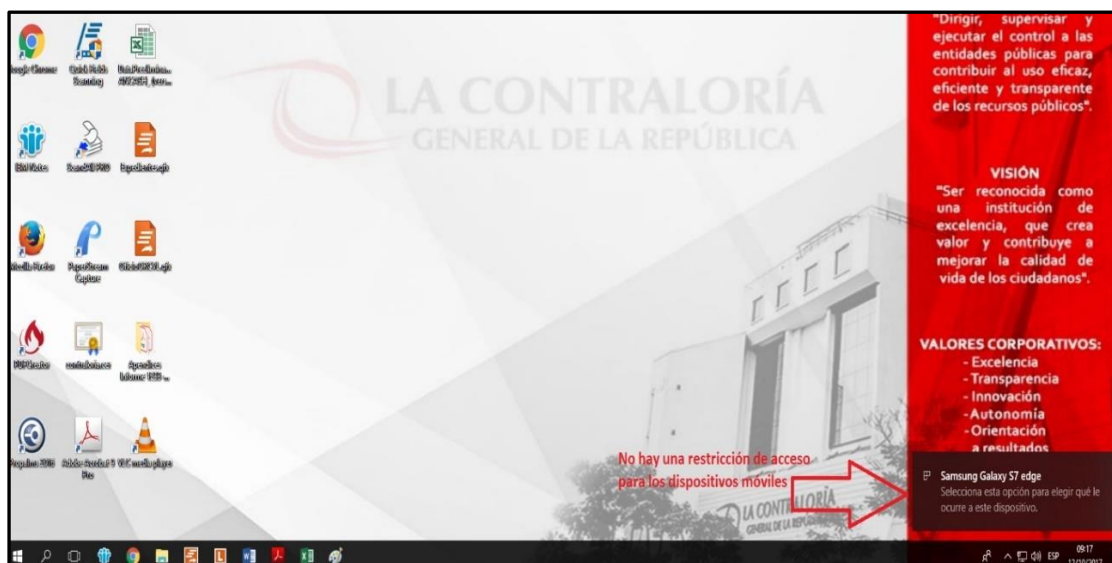


**Figura 5.** Gráfico porcentual de la Vulnerabilidad N° 01

**Fuente:** Elaborado por el autor



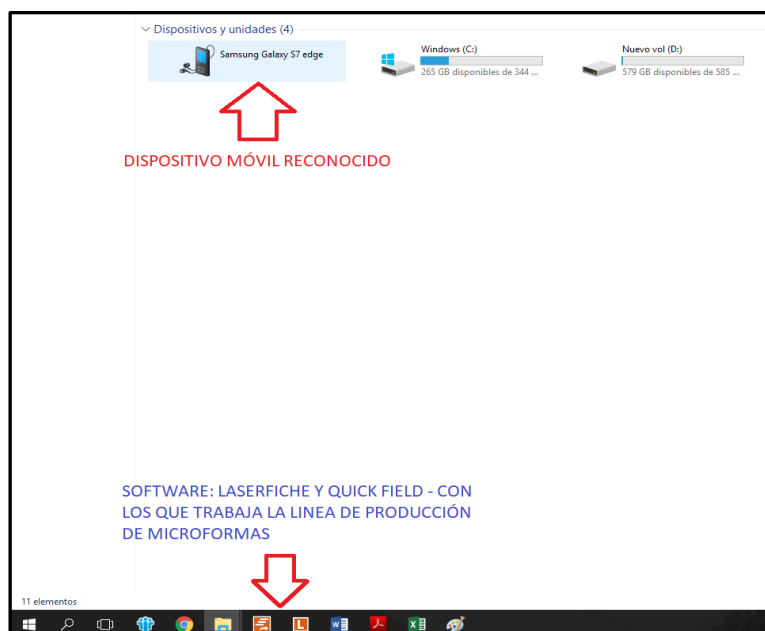
*Documentación – Vulnerabilidad N° 01- A.6.2.1 Políticas de Dispositivos móviles*



**Figura 6.** Captura de pantalla de una PC asignada a LPM de microformas

**Fuente:** Elaborado por el autor

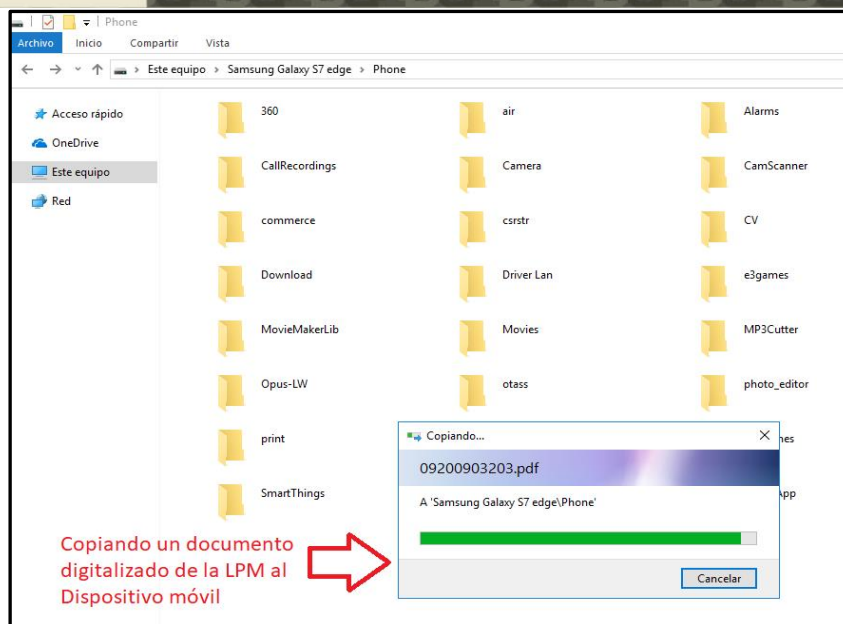
En la Figura 6, se evidencia el reconocimiento al dispositivo móvil (“Samsung Galaxy S7 Edge”), sin ningún tipo de restricción de acceso.



**Figura 7.** Captura de pantalla, reconocimiento del dispositivo móvil

**Fuente:** Elaborado por el autor

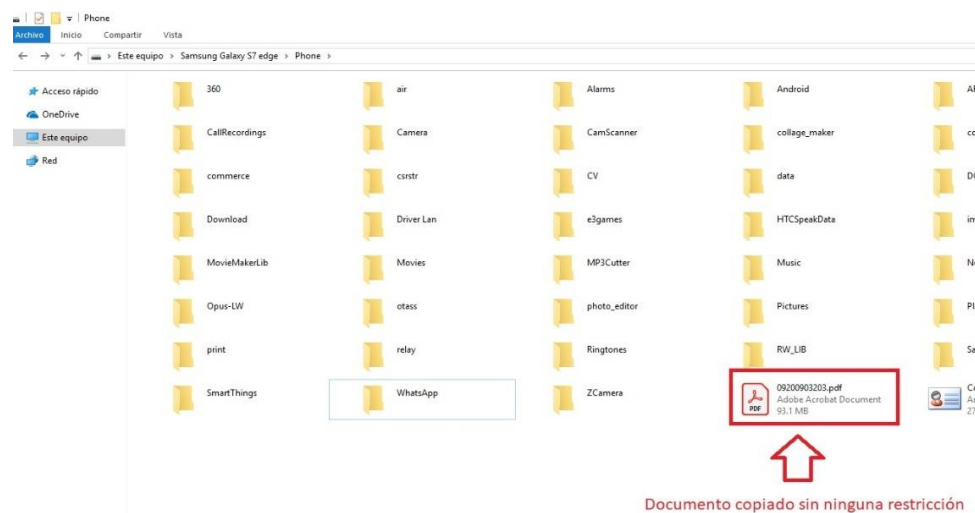
En la Figura 6, se puede evidenciar el reconocimiento del dispositivo móvil como una unidad de almacenamiento.



**Figura 8.** Captura de pantalla, transferencia de información

**Fuente:** Elaborado por el autor

En la Figura 8, se puede apreciar la transferencia de contenidos, vulnerando claramente la seguridad de la información.



**Figura 9.** Captura de pantalla, culminación de transferencia de información.

**Fuente:** Elaborado por el autor

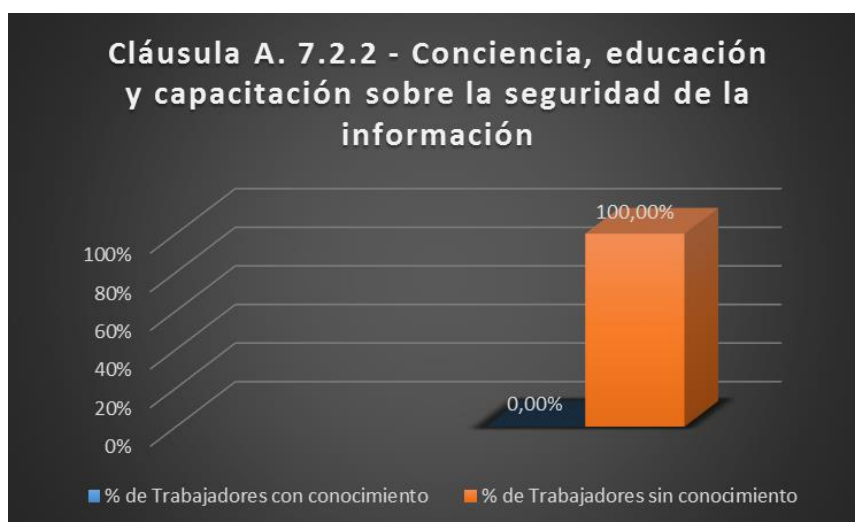
En la Figura 9, se aprecia que la información fue copiada desde el ordenador al dispositivo móvil sin ningún problema o restricción en el proceso.

De la cláusula A.6.2.1 “Políticas de dispositivos móviles” de la NTP ISO/IEC 27001, se advierte que no existe medidas de seguridad respecto al uso de dispositivos móviles, las cuales deben ser adoptadas para la gestión de riesgos en el uso de estos dispositivos.

**Tabla 7.** Vulnerabilidad N° 02 – A. 7.2.2 Conciencia, educación y capacitación sobre la seguridad de la información.

CLÁUSULAS DEL ANEXO A - NTP ISO/IEC 27001:2014			PREGUNTA					RESULTADO
			N° de Pregunta	Cant. De Resp. positivas	Cant. De Resp. Negativas	% de Trabajadores con conocimiento	% de Trabajadores sin conocimiento	
Seguridad de los recursos humanos	A.7	A. 7.2.2	3.4	0	60	0,00%	100,00%	Vulnerabilidad

**Nota.** Fuente: Elaborado por el autor

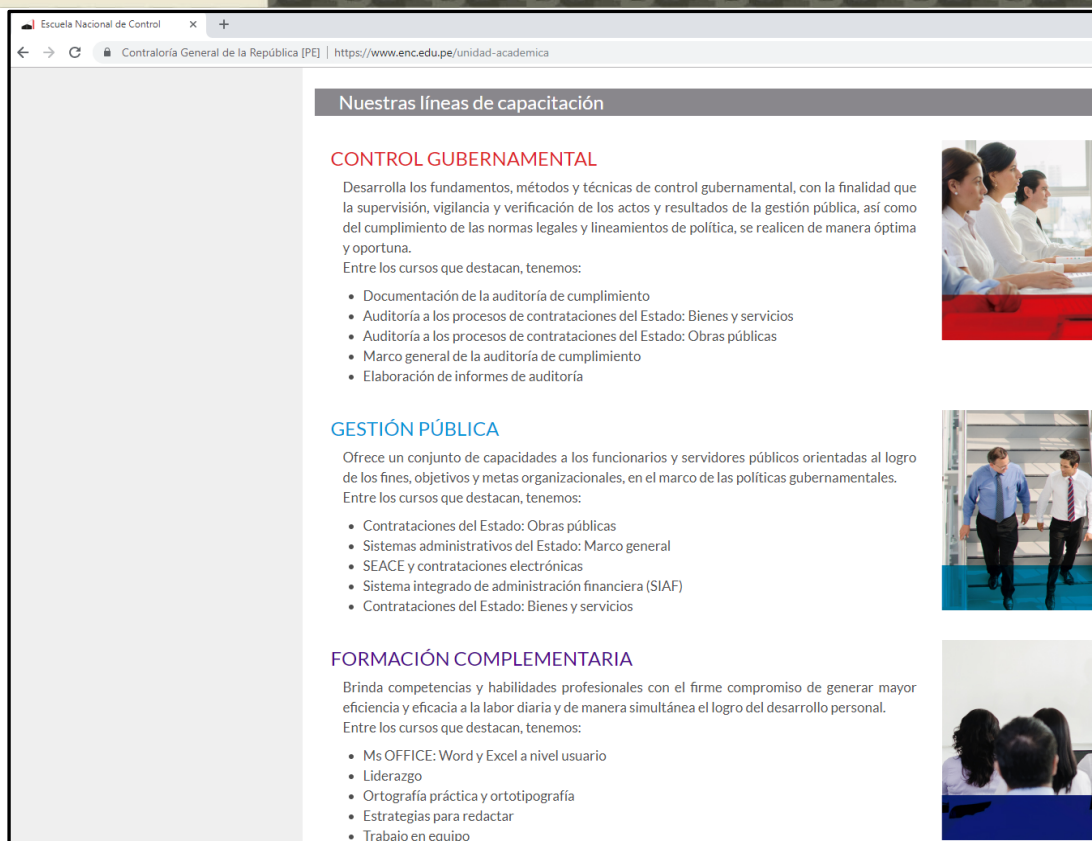


**Figura 10.** Gráfico porcentual de la Vulnerabilidad N° 02

**Fuente:** Elaborado por el autor

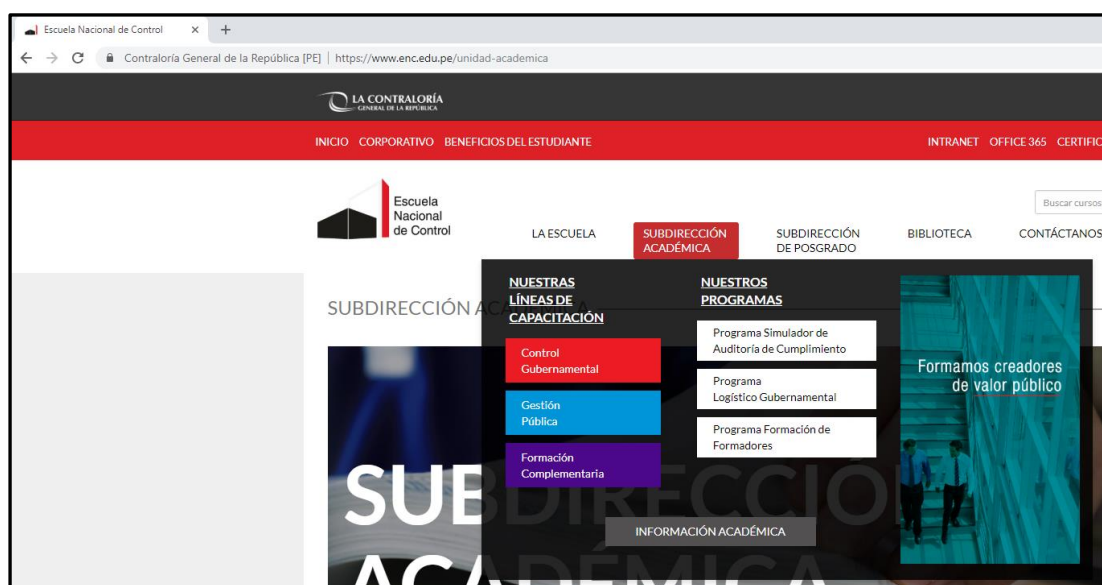
*Documentación - Vulnerabilidad N° 02 – A. 7.2.2 Conciencia, educación y capacitación sobre la seguridad de la información.*

Todos los cursos, capacitaciones u otro tipo de actividad de aprendizaje dirigida a los colaboradores de la CGR, se realizan a través de la Escuela Nacional de Control (ENC) de la Contraloría General de la República.



**Figura 11.** Captura de pantalla, página web de la ENC – Sección: Líneas de capacitación

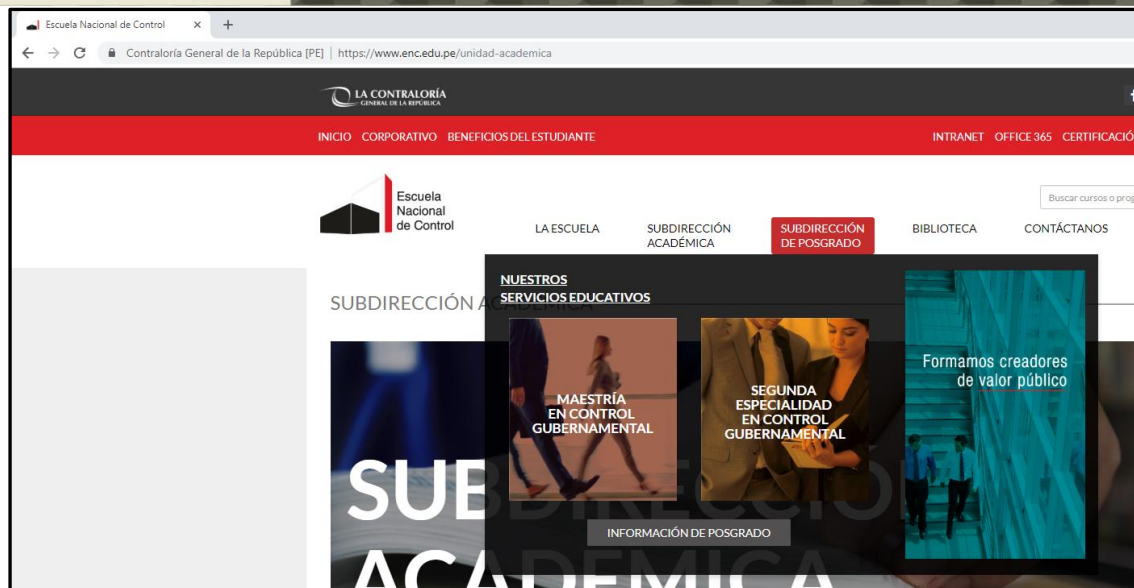
**Fuente:** Escuela Nacional de Control



**Figura 12.** Captura de pantalla, página web de la ENC – Sección: Subdirección Académica

**Fuente:** Escuela Nacional de Control





**Figura 13.** Captura de pantalla, página web de la ENC – Sección: Subdirección Posgrado  
Fuente: Escuela Nacional de Control

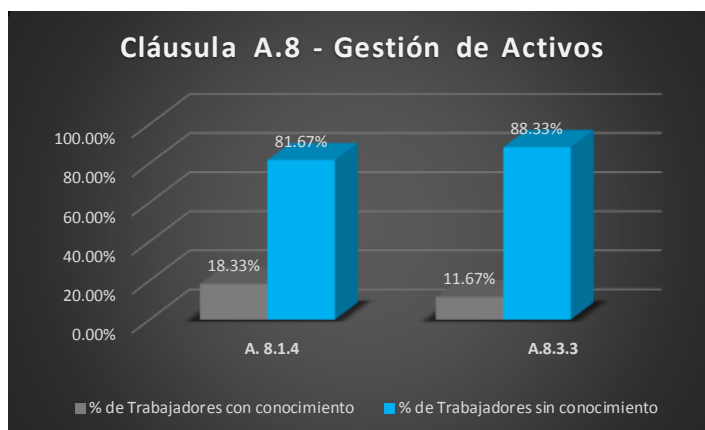
En las Figura 11,12 y 13, se puede apreciar que no se existe la programación de algún curso, taller o capacitación respecto al tema de Seguridad de la Información.

Por lo tanto, se advierte una vulnerabilidad en relación a la Capacitación sobre temas en Seguridad de la Información hacia los trabajadores de la LPM de la CGR, vulnerando la cláusula A.7.2.2 “Conciencia, educación y capacitación sobre la seguridad de la información” de la NTP ISO/IEC 27001, esto, al no existir un curso y/o actividad académica programado por la Escuela Nacional de Control respecto al tema de Seguridad de Información.

**Tabla 8.** Vulnerabilidad N° 03 – A.8.1.4 Retorno de activos y Vulnerabilidad N° 04 – A.8.3.3 Transferencia de medios físicos

CLÁUSULAS DEL ANEXO A - NTP ISO/IEC 27001:2014			PREGUNTA					RESULTADO
			N° de Pregunta	Cant. De Resp. positivas	Cant. De Resp. Negativas	% de Trabajadores con conocimiento	% de Trabajadores sin conocimiento	
Gestión de Activos	A. 8	A. 8.1.4	4.4	11	49	18,33%	81,67%	Vulnerabilidad
		A. 8.3.3	4.10	7	53	11,67%	88,33%	Vulnerabilidad

**Nota.** Fuente: Elaborado por el autor



**Figura 14.** Gráfico porcentual de las Vulnerabilidades N° 03 y 04

**Fuente:** Elaborado por el autor

**Documentación - Vulnerabilidad N° 03 – A.8.1.4 Retorno de activos**



**Figura 15.** Estación de trabajo LPM – Sede Provincial

**Fuente:** Elaborado por el autor

En la Figura 15, se puede evidenciar que uno de los recursos tecnológicos (Escáner) que perteneció a un ex colaborador, no se retornó al área competente.

De la Cláusula A.8.1.4 “Retorno de activos” de la NTP ISO/IEC 27001, se advierte que no se retorna los activos una vez extinto el vínculo contractual, exponiendo a los activos a riesgos de daños físicos y funcionales.



*Documentación - Vulnerabilidad N° 04 – A.8.3.3 Transferencia de medios físicos*



**Figura 16.** Ordenadores en desuso de la LPM en almacén de útiles

**Fuente:** Elaborado por el autor

En la Figura 16, se aprecia que los ordenadores en desuso pertenecientes a la Línea de Producción de Microformas, se encuentran expuestos a daños físicos y al uso de personal no autorizado, almacenados en un ambiente inapropiado para su resguardo.

De la Cláusula A.8.3.3 “Transferencia de medios físicos” de la NTP ISO/IEC 27001, se advierte que los equipos en desuso que contienen información de la LPM, no se encuentran

protegidos contra el acceso no autorizado, al mal uso o a la corrupción, durante el proceso de transporte.

**Tabla 9.** Vulnerabilidad N° 05 – N° 08

Vulnerabilidad N° 05 – A.9.1.2 Acceso a redes y a servicios de red

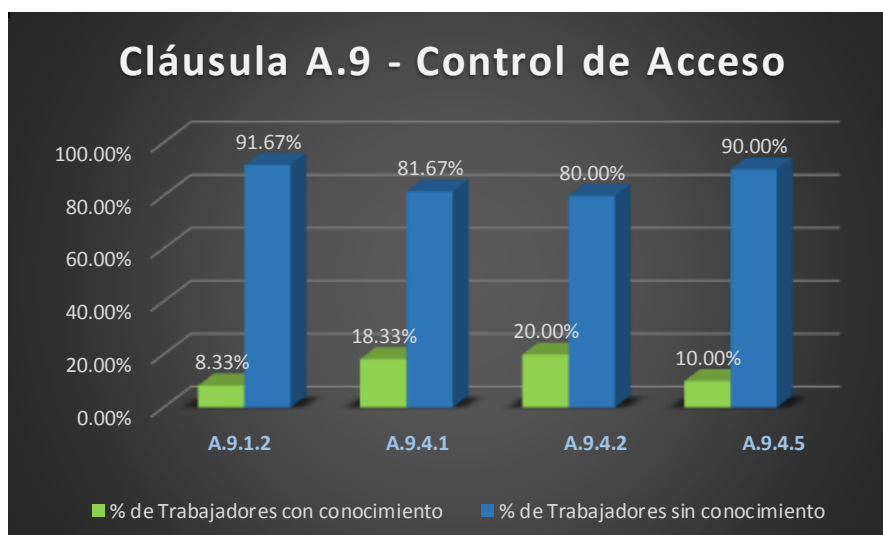
Vulnerabilidad N° 06 – A.9.4.1 Restricción de acceso a la información

Vulnerabilidad N° 07 – A.9.4.2 Procedimiento de ingreso seguro

Vulnerabilidad N° 08 – A.9.4.5 Control de acceso al código fuente de los programas.

CLÁUSULAS DEL ANEXO A - NTP ISO/IEC 27001:2014		PREGUNTA					RESULTADO
		N° de Pregunta	Cant. De Resp. positivas	Cant. De Resp. Negativas	% de Trabajadores con conocimiento	% de Trabajadores sin conocimiento	
DESCRIPCIÓN	N°						
Control de acceso	A. 9	A. 9.1.2	5.2	5	55	8,33%	91,67%
		A. 9.4.1	5.10	11	49	18,33%	81,67%
		A. 9.4.2	5.11	12	48	20,00%	80,00%
		A. 9.4.5	5.14	6	54	10,00%	90,00%

**Nota.** Fuente: Elaborado por el autor

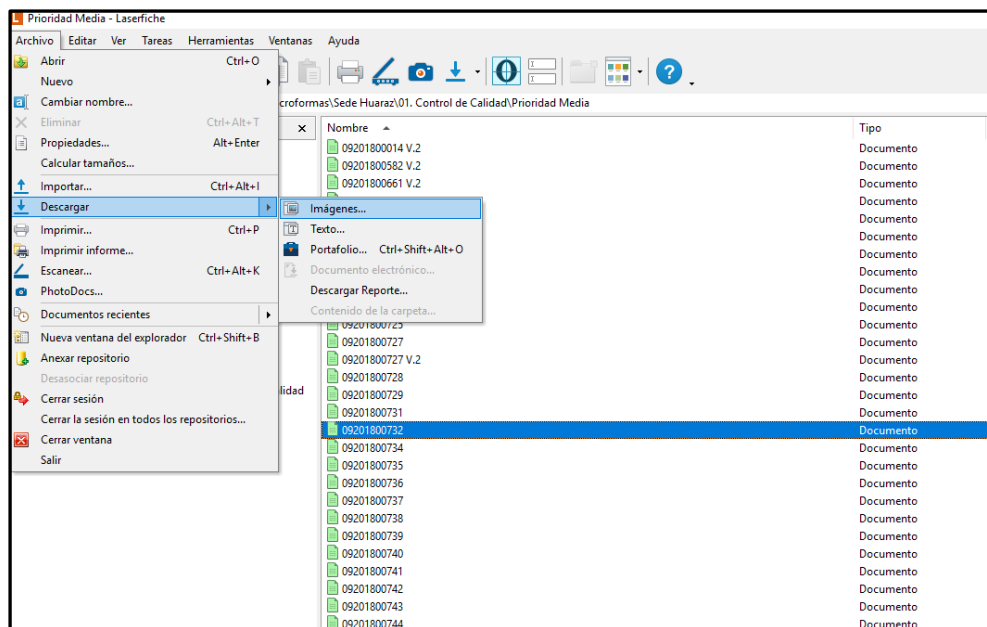


**Figura 17.** Gráfico porcentual de las Vulnerabilidades N° 05 al 08

Fuente: Elaborado por el autor

De la Cláusula A.9 – Control de Acceso, se advirtieron diferentes tipos de vulnerabilidades, desde el acceso a redes y servicios de red, hasta el código fuente de los programas; a continuación, se procedió a documentar las más importantes.

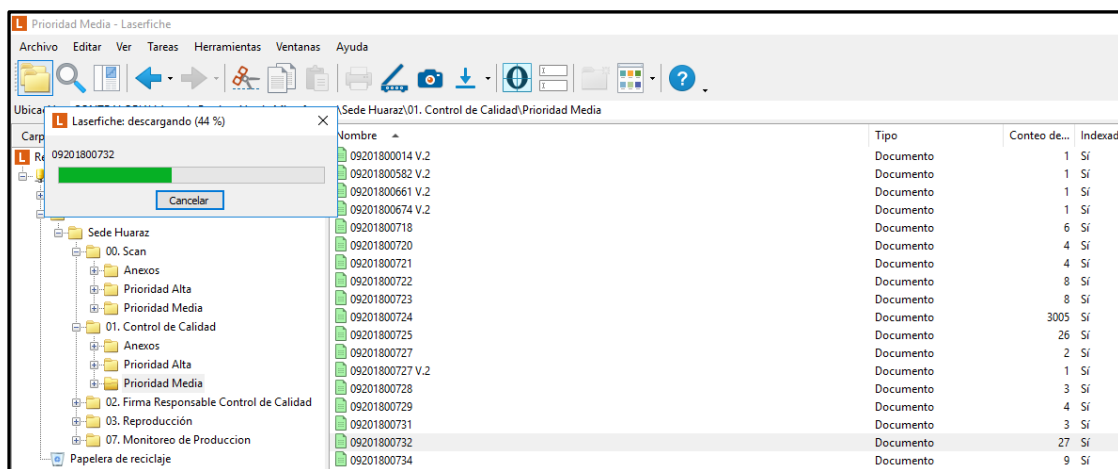
### Documentación - Vulnerabilidad N° 06 – A.9.4.1 Restricción de acceso a la información



**Figura 18.** Captura de pantalla – Software de LPM: Laserfiche Rio 10.2

Fuente: Elaborado por el autor

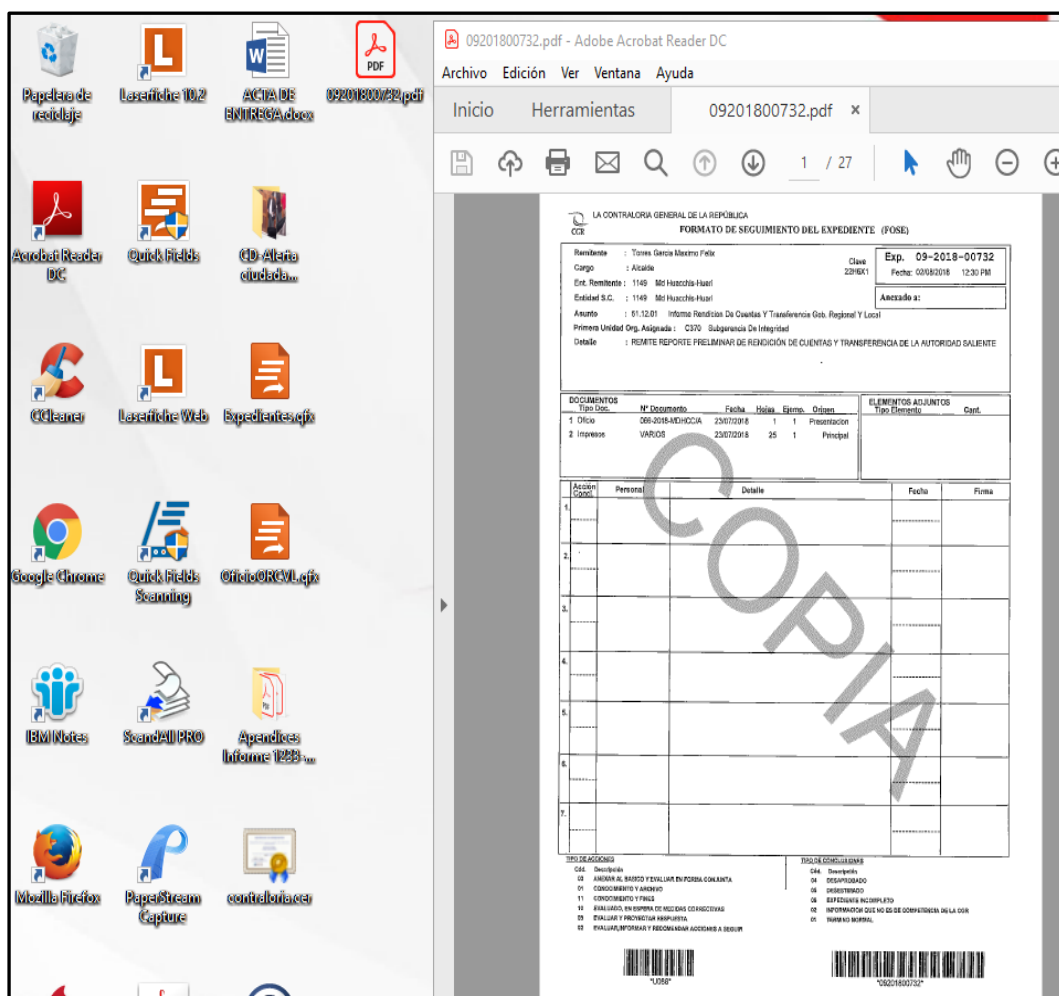
En la Figura 18, se aprecia que no existe una restricción en el acceso de información, evidencia de ello, es la opción de descargar todo tipo de documento digitalizado desde una cuenta de usuario básico.



**Figura 19.** Captura de pantalla – Descarga de documento digital.

Fuente: Elaborado por el autor

En la Figura 19, se evidencia que el documento digitalizado puede se descarga sin ningún tipo de restricción o permiso.



**Figura 20.** Captura de pantalla – Documento “09201800732” descargado

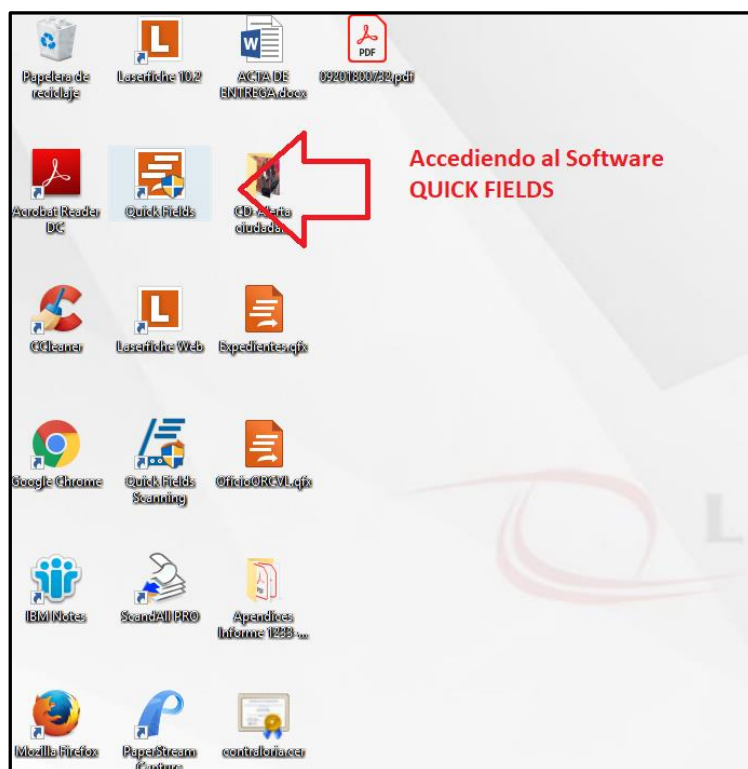
Fuente: Elaborado por el autor

En las Figuras 18,19 y 20, se puede evidenciar que el documento fue descargado sin ninguna restricción y se puede hacer uso del mismo.

De la Cláusula A.9.4.1 “Restricción de acceso a la información” de la NTP ISO/IEC 27001, se advierte que en el software Laserfiche se puede descargar todo tipo de información, esto, sin ningún tipo de autorización o restricción, vulnerando el acceso de la información de la LPM de la CGR.

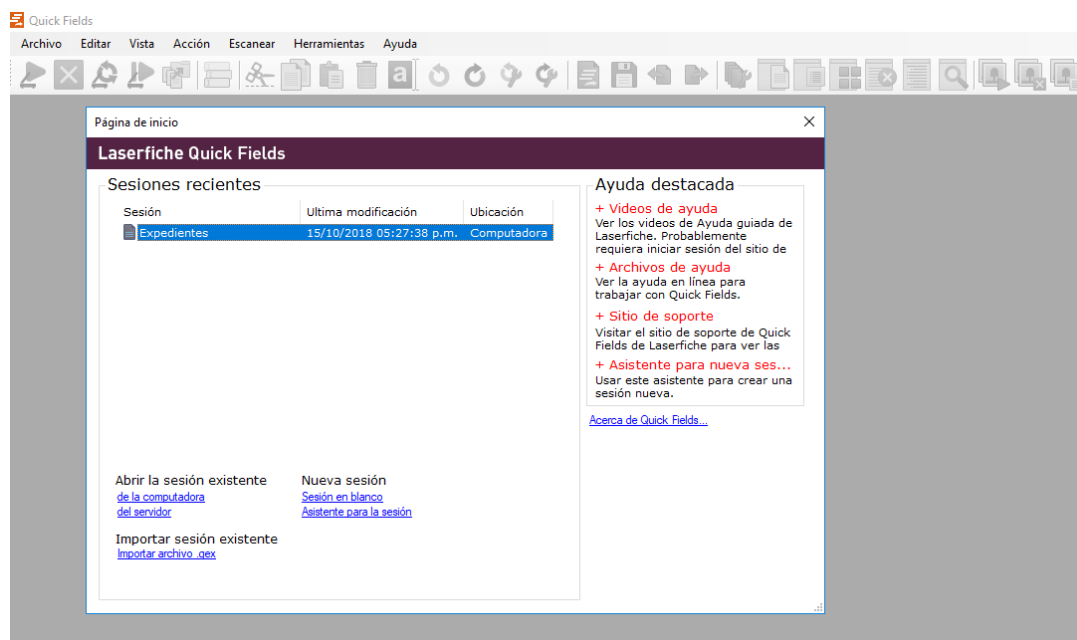


**Documentación - Vulnerabilidad N° 07 – A.9.4.2 Procedimiento de ingreso seguro**



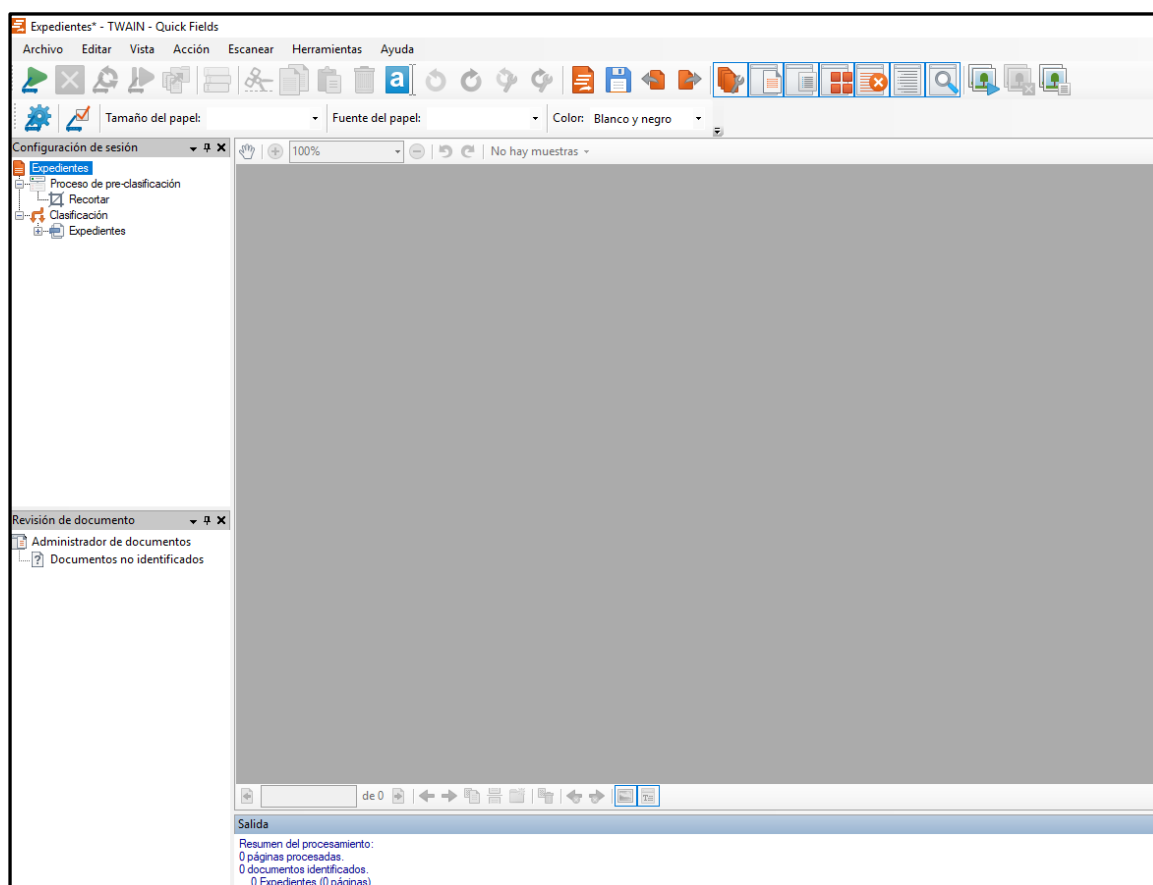
**Figura 21.** Captura de pantalla – Ingreso al Software Quick Fields

**Fuente:** Elaborado por el autor



**Figura 22.** Captura de pantalla – Inicio de sesión al Software Quick Fields

**Fuente:** Elaborado por el autor



**Figura 23.** Captura de pantalla – Interfaz de Software Quick Fields

Fuente: Elaborado por el autor

En las Figuras 21, 22 y 23 se aprecia que no existe un procedimiento seguro, ni sistema de gestión de contraseñas para el ingreso al software Quick Field, vulnerando gravemente la cláusula A.9.4.2 “Procedimiento de ingreso seguro” de la NTP ISO/IEC 27001, que establece que el acceso a los sistemas y a las aplicaciones debe ser controlado por un procedimiento de ingreso seguro y prevenir el acceso no autorizado a los sistemas de información.



**Tabla 10.** Vulnerabilidad N° 09 Y N° 13

Vulnerabilidad N° 09 – A.11.1.1 Perímetros de seguridad física

Vulnerabilidad N° 10 – A.11.1.2 Controles de ingreso físico

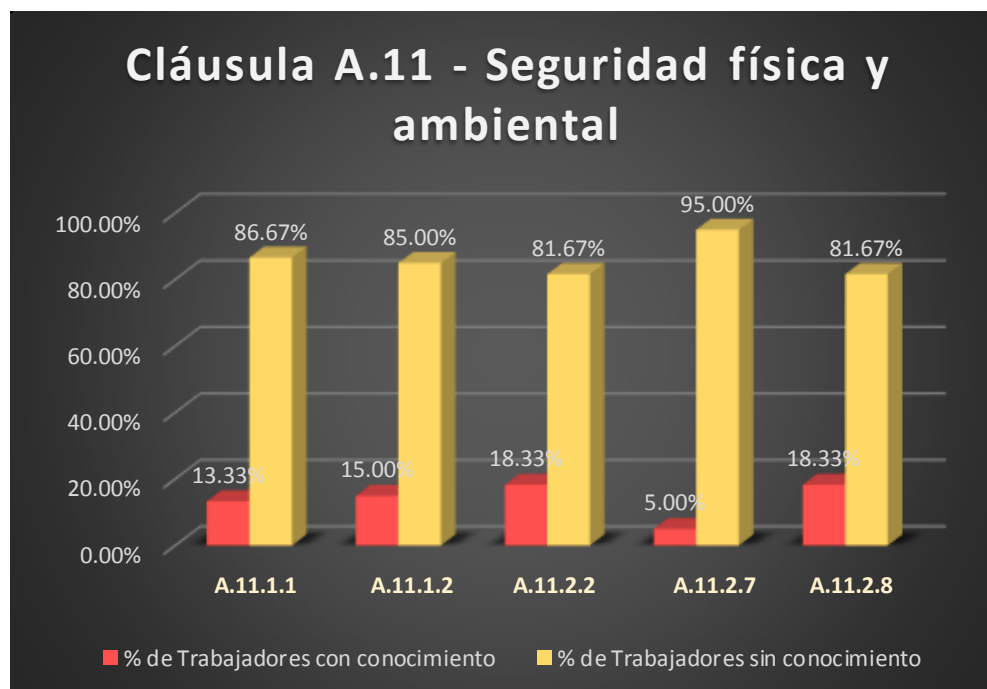
Vulnerabilidad N° 11 – A.11.2.2 Servicios de suministro

Vulnerabilidad N° 12 – A.11.2.7 Disposición o reutilización segura de equipos

Vulnerabilidad N° 13 – A.11.2.8 Equipos de usuario desatendidos

CLÁUSULAS DEL ANEXO A - NTP ISO/IEC 27001:2014			PREGUNTA					RESULTADO
DESCRIPCIÓN	N°		N° de Pregunta	Cant. De Resp. positivas	Cant. De Resp. Negativas	% de Trabajadores con conocimiento	% de Trabajadores sin conocimiento	
Seguridad física y ambiental	A. 11	A. 11.1.1	7.1	8	52	13,33%	86,67%	Vulnerabilidad
		A. 11.1.2	7.2	9	51	15,00%	85,00%	Vulnerabilidad
		A. 11.2.2	7.8	11	49	18,33%	81,67%	Vulnerabilidad
		A. 11.2.7	7.13	3	57	5,00%	95,00%	Vulnerabilidad
		A. 11.2.8	7.14	11	49	18,33%	81,67%	Vulnerabilidad

**Nota.** Fuente: Elaborado por el autor



**Figura 24.** Gráfico porcentual de las Vulnerabilidades N° 09 al 13

**Fuente:** Elaborado por el autor

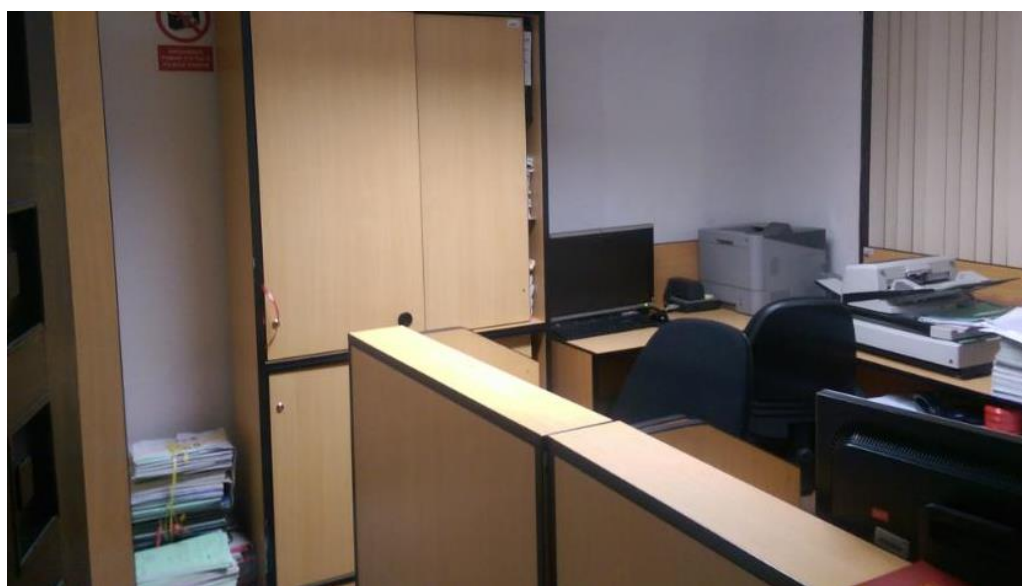
De la Cláusula A.11 – Seguridad física y ambiental, se advirtieron diferentes tipos de vulnerabilidades, desde los perímetros de seguridad física, hasta equipos de usuarios desatendidos; a continuación, se procedió a documentar las más importantes.

**Documentación - Vulnerabilidad N° 09 – A.11.1.1 Perímetros de seguridad física y Vulnerabilidad N° 10 – A.11.1.2 Controles de ingreso físico**



**Figura 25.** Ingreso a oficina de trámite documentario – Estación de LPM

**Fuente:** Elaborado por el autor



**Figura 26.** Oficina de trámite documentario – Estación de LPM

**Fuente:** Elaborado por el autor

En las Figuras 25 y 26 se aprecia que no se ha establecido un perímetro de seguridad y ningún tipo de control de acceso a personal no autorizado, lo que vulnera claramente las Cláusulas A.11.1.1 “Perímetros de seguridad física” y A.11.1.2 “Controles de ingreso físico” de la NTP ISO/IEC 27001, los cuales establecen el impedimento del acceso físico no autorizado, daño e interferencia a la información y a las instalaciones de procesamiento de la información de la entidad.

***Documentación - Vulnerabilidad N° 11 – A.11.2.2 Servicios de suministro***



***Figura 27. Pc de LPM - Oficina de trámite documentario***

**Fuente:** Elaborado por el autor

En la Figura 27, se evidencia que el equipo de la LPM no cuenta con UPS o un sistema de alimentación eléctrica ininterrumpida, lo que vulnera claramente la Cláusula A.11.2.2 “Servicios de suministro” de la NTP ISO/IEC 27001, el cual establece la prevención de



fallas eléctricas u otras alteraciones causadas por fallas en los servicios de suministro y se prevenga interrupciones en las operaciones de la entidad.

**Documentación - Vulnerabilidad N° 13 – A.11.2.8 Equipos de usuario desatendidos**



**Figura 28.** Equipos desatendidos - Oficina de trámite documentario  
**Fuente:** Elaborado por el autor

En la Figura 28, se aprecia equipos desatendidos de la LPM que no cuentan con la debida protección, colocados en un lugar de libre acceso y expuestos a daños físicos, lo que vulnera la Cláusula A.11.2.8 “Equipos de usuario desatendidos” de la NTP ISO/IEC 27001, el cual establece que los usuarios que hicieron uso de algún equipo, deben asegurarse que se encuentre adecuadamente protegido.

**Tabla 11. Vulnerabilidad N° 14 - N° 15**

*Vulnerabilidad N° 14 – A.12.4.1 Registro de eventos*

*Vulnerabilidad N° 15 – A.12.6.2 Restricciones sobre la instalación de software*

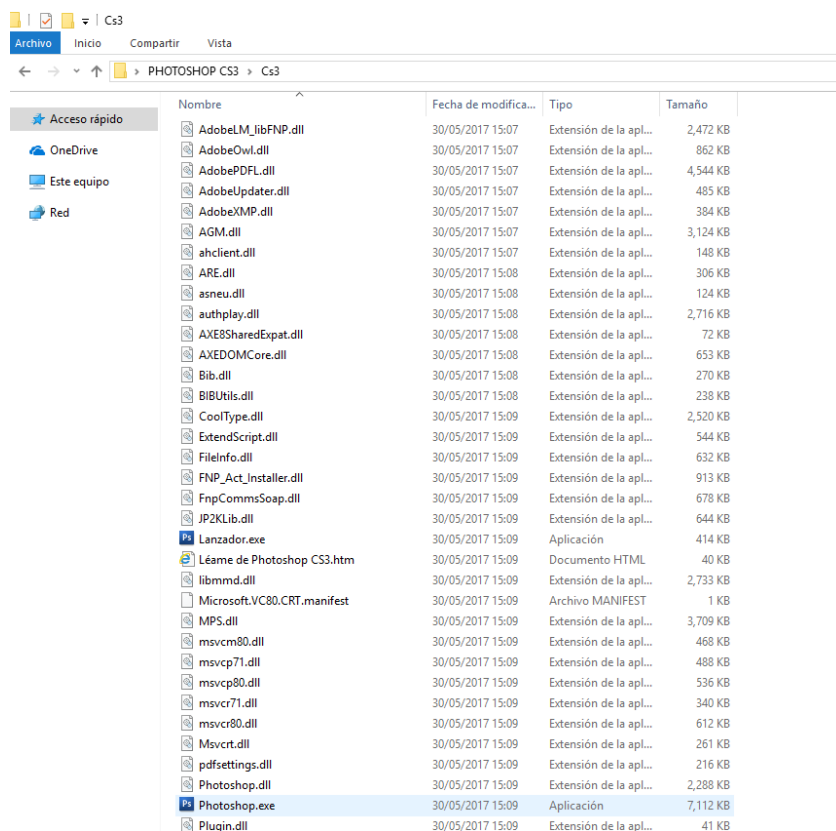
CLÁUSULAS DEL ANEXO A - NTP ISO/IEC 27001:2014			PREGUNTA					RESULTADO
			N° de Pregunta	Cant. De Resp. positivas	Cant. De Resp. Negativas	% de Trabajadores con conocimiento	% de Trabajadores sin conocimiento	
DESCRIPCIÓN	N°							
Seguridad de las operaciones	A. 12	A. 12.4.1	8.7	54	6	10,00%	90,00%	Vulnerabilidad
		A. 12.6.2	8.13	9	51	15,00%	85,00%	Vulnerabilidad

**Nota.** Fuente: Elaborado por el autor

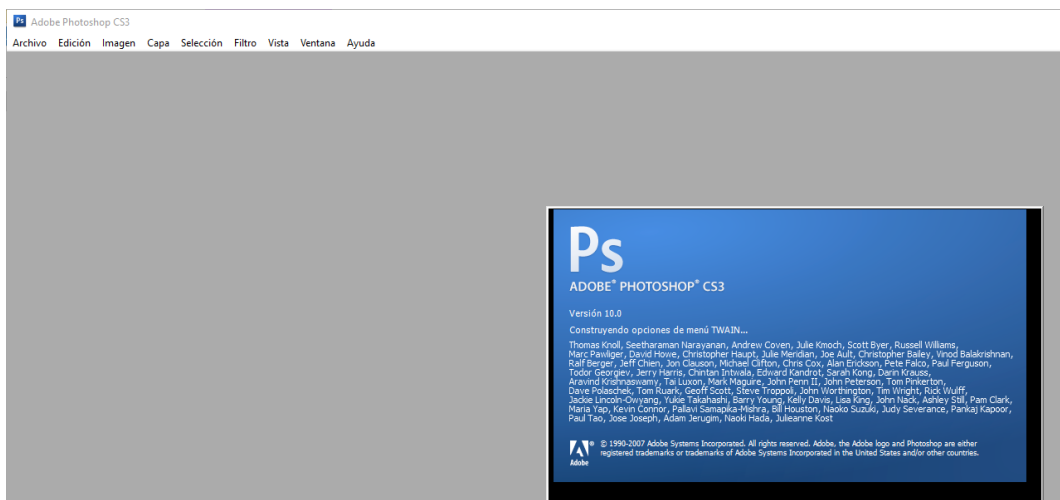


**Figura 29:** Gráfico porcentual de las Vulnerabilidades N° 14 y 15  
Fuente: Elaborado por el autor

### *Documentación - Vulnerabilidad N° 15 – A. 12.6.2 Restricciones sobre la instalación de software*

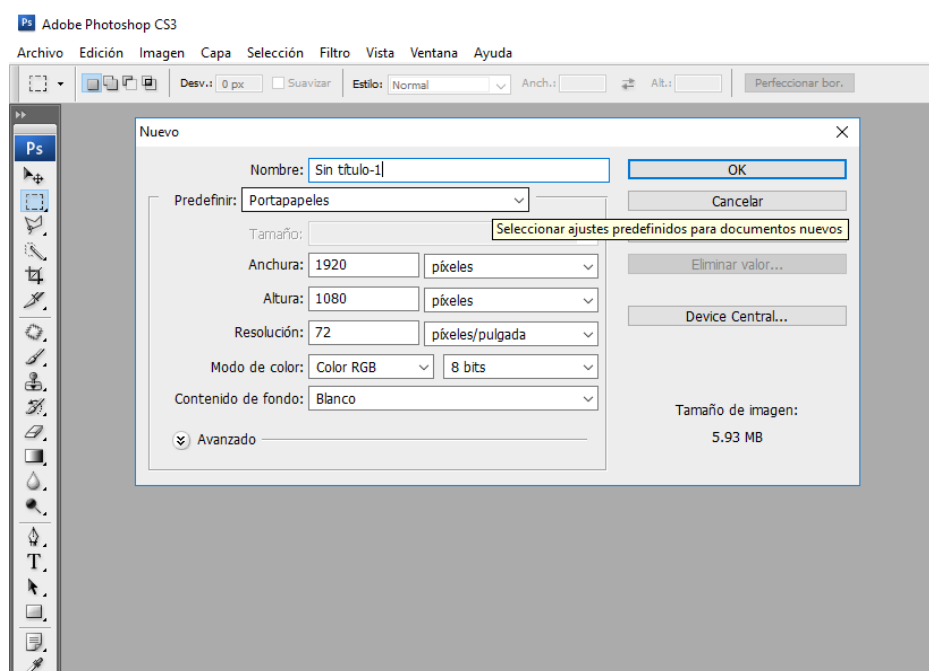


**Figura 30:** Captura de pantalla – Instalación de Software Photoshop CS3  
Fuente: Elaborado por el autor



**Figura 29.** Captura de pantalla – Procedimiento de instalación de Software Photoshop CS3

**Fuente:** Elaborado por el autor



**Figura 30.** Captura de pantalla – Interfaz de Software Photoshop CS3

**Fuente:** Elaborado por el autor

En las Figuras 30,31 y 32 se aprecia que no se ha establecido reglas que gobiernen la instalación de programas por parte de los usuarios, lo que vulnera claramente la Cláusula A.12.6.2 “Restricciones sobre la instalación de software” de la NTP ISO/IEC 27001, que



establece la implementación de restricciones en la instalación de algún software y prevenir la explotación de vulnerabilidades técnicas.

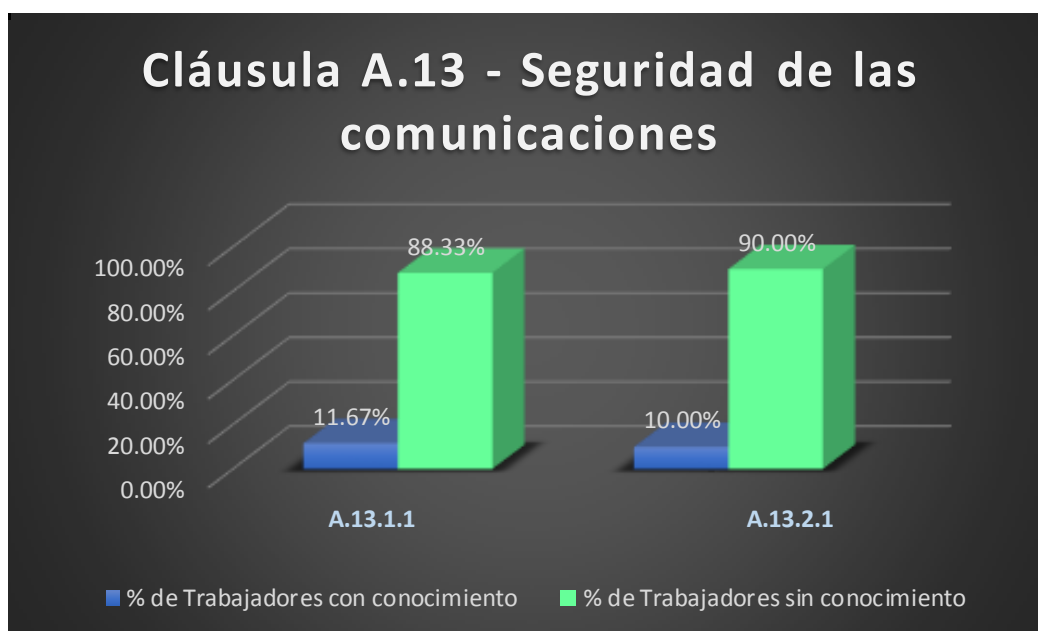
**Tabla 12.** Vulnerabilidad N° 16 - N° 17

Vulnerabilidad N° 16 – A.13.1.1 Controles de la red

Vulnerabilidad N° 17 – A.13.2.1 Políticas y procedimientos de transferencia de la información.

CLÁUSULAS DEL ANEXO A - NTP ISO/IEC 27001:2014			PREGUNTA					RESULTADO
			N° de Pregunta	Cant. De Resp. positivas	Cant. De Resp. Negativas	% de Trabajadores con conocimiento	% de Trabajadores sin conocimiento	
Seguridad de las comunicaciones	A. 13	A. 13.1.1	9.1	7	53	11,67%	88,33%	Vulnerabilidad
		A. 13.2.1	9.4	6	54	10,00%	90,00%	Vulnerabilidad

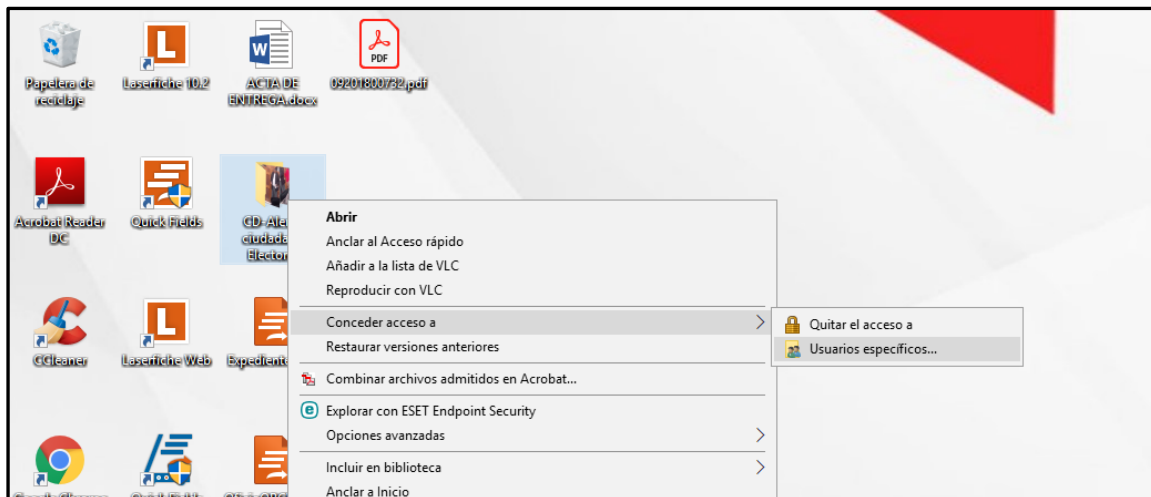
**Nota.** Fuente: Elaborado por el autor



**Figura 31.** Gráfico porcentual de la Vulnerabilidad N° 16 y 17

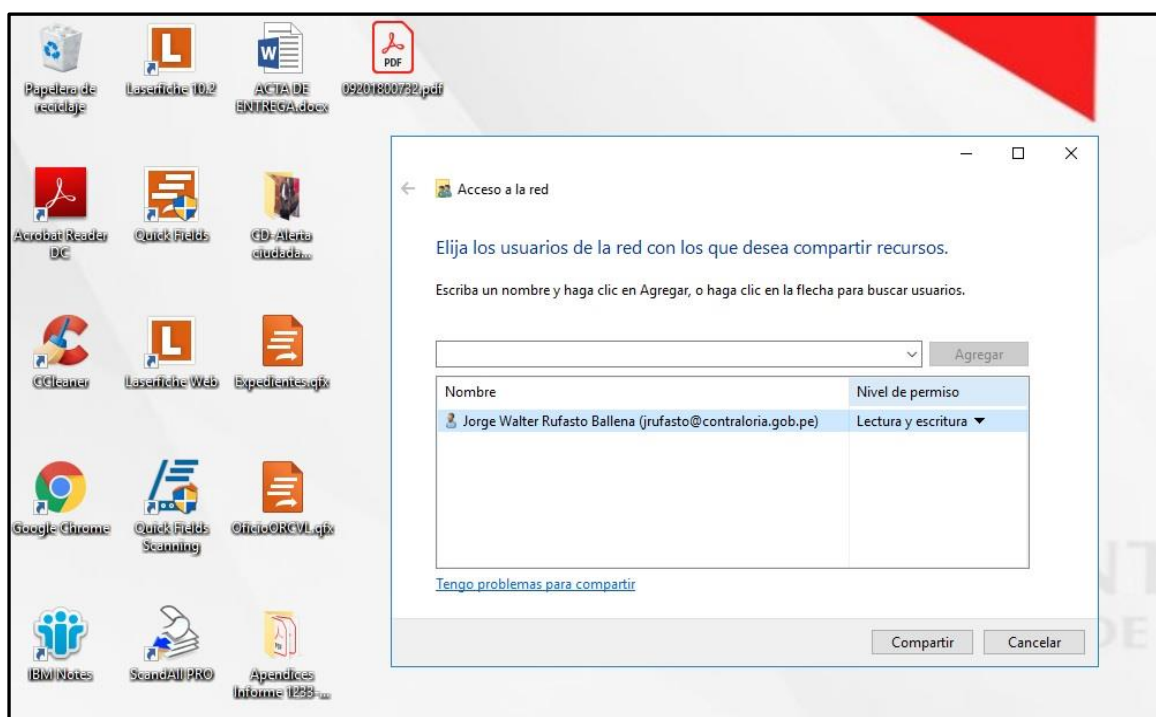
Fuente: Elaborado por el autor

**Documentación - Vulnerabilidad N° 17 – A.13.2.1 Políticas y procedimientos de transferencia de la información.**



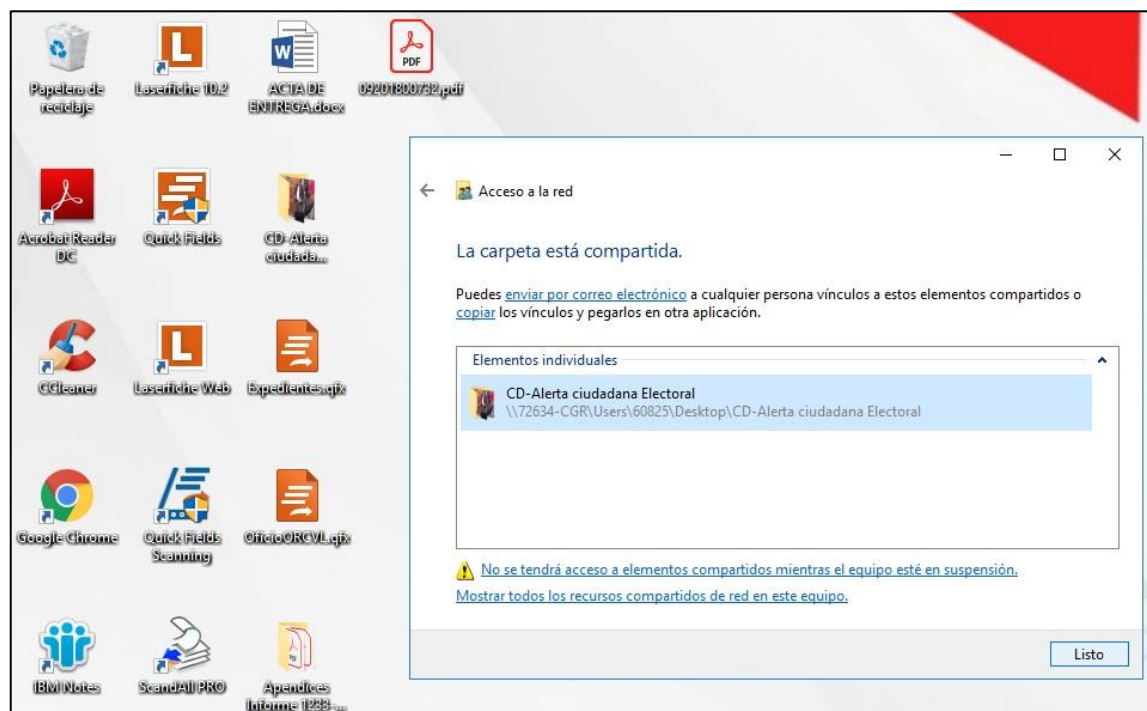
**Figura 32.** Captura de pantalla – Transferencia de información a otros usuarios

**Fuente:** Elaborado por el autor



**Figura 33.** Captura de pantalla – Otorgando permisos de lectura y escritura

**Fuente:** Elaborado por el autor



**Figura 34.** Captura de pantalla – Culminación de transferencia de información

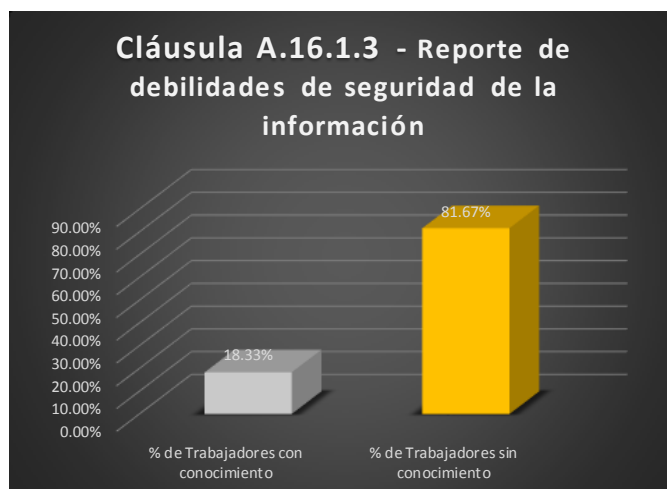
**Fuente:** Elaborado por el autor

En las Figuras 34,35 y 36 se puede evidenciar que no se ha establecido ninguna política o procedimiento para la transferencia formal de información, vulnerando claramente la Cláusula A.13.2.1 “Políticas y procedimientos de transferencia de la información” de la NTP ISO/IEC 27001.

**Tabla 13.** Vulnerabilidad N° 18 – A.16.1.3 Reporte de debilidades de seguridad de la información

CLÁUSULAS DEL ANEXO A - NTP ISO/IEC 27001:2014			PREGUNTA					RESULTADO
			N° de Pregunta	Cant. De Resp. positivas	Cant. De Resp. Negativas	% de Trabajadores con conocimiento	% de Trabajadores sin conocimiento	
Gestión de incidentes de seguridad de la información	A. 16	A. 16.1.3	12.3	11	49	18,33%	81,67%	Vulnerabilidad

**Nota.** Fuente: Elaborado por el autor



**Figura 35.** Gráfico porcentual de la Vulnerabilidad N° 1836

**Fuente:** Elaborado por el autor

**Documentación - Vulnerabilidad N° 18 – A.16.1.3 Reporte de debilidades de seguridad de la información**




**LA CONTRALORÍA**  
GENERAL DE LA REPÚBLICA  
DEPARTAMENTO DE GESTIÓN DOCUMENTARIA

**MEMORANDO CIRCULAR N° 00039-2016-CG/TD**

**Asunto :** Control de Incidencias  
**Referencia :** Memorando circular N° 00012-2016-CG/DC  
**Fecha :** Jesús María, 03 de noviembre de 2016

---

Tengo el agrado de dirigirme a ustedes, con relación al memorando de la referencia, en el cual el Contralor solicita la implementación del Diagnóstico, Plan de Acción y Cronograma de Implementación del Sistema de Control Interno de la Contraloría General de la República formulado por Ernest & Young Asesores S. Civil R.L.

Al respecto, producto de la mencionada evaluación, se determinó planes de acciones, a fin de fortalecer el control interno en los procesos de esta Institución, entre ellas, PA-099 "Llevar un control de los incidentes ocurridos relacionados con la interrupción por la caída o falla de sistemas y los tiempos de remediación de los mismos, a fin de identificar las causas, y de evaluar la necesidad de elaborar planes de continuidad operativa del proceso".

En consecuencia, se remite el formato "Control de Incidentes en Trámite Documentario", a fin de que, en caso ocurra un incidente (suceso que sucede de manera inesperada y pueda afectar el desarrollo de una actividad), puedan registrarlo en este formato, precisando algunas características, como fecha, hora, descripción, acción inmediata, entre otros.

Dicha información deberá ser remitido a los supervisores de cada proceso, para la implementación de medidas correctivas, a fin de evitar o minimizar la ocurrencia de incidencias.

Atentamente,

  
**Sonia Nakao**  
 Gerente  
 Departamento de Gestión Documentaria

/fpm

**Figura 37.** Memorando Circular N° 00039-2016-CG/TD – Control de Incidencias

**Fuente:** Sistema Chasqui CGR

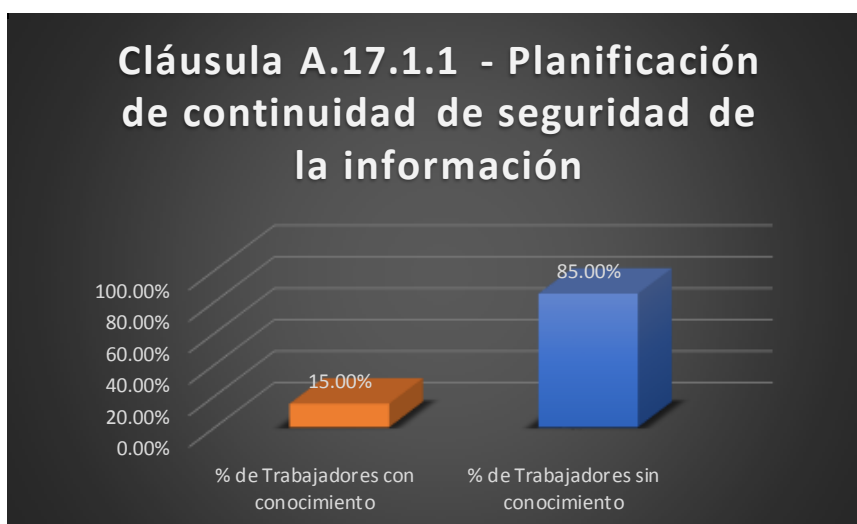


En la Figura 37, correspondiente al Memorando Circular N° 00039-2016-CG/TD, respecto a la implementación del diagnóstico realizado por la empresa Ernest & Young Asesores S. Civil R.L, se determinó deficiencias respecto al reporte de incidentes o debilidades que sucedan de manera inesperada y pueda afectar al desarrollo de las actividades de la LPM, lo que vulnera claramente la Cláusula A.16.1.3 “Reporte de debilidades de seguridad de la información” de la NTP ISO/IEC 27001, que establece que el personal debe ser exigido para advertir y reportar cualquier debilidad en cuanto a la seguridad de la información.

**Tabla 14.** Vulnerabilidad N° 19 – A.17.1.1 Planificación de continuidad de seguridad de la información

CLÁUSULAS DEL ANEXO A - NTP ISO/IEC 27001:2014			PREGUNTA					RESULTADO
			N° de Pregunta	Cant. De Resp. positivas	Cant. De Resp. Negativas	% de Trabajadores con conocimiento	% de Trabajadores sin conocimiento	
DESCRIPCIÓN	N°							
Aspectos de seguridad de la información en la gestión de continuidad del negocio	A. 17	A. 17.1.1	13.1	9	51	15,00%	85,00%	Vulnerabilidad

**Nota.** Fuente: Elaborado por el autor



**Figura 38.** Gráfico porcentual de la Vulnerabilidad N° 19

Fuente: Elaborado por el autor

**Tabla 15.** Vulnerabilidad N° 20 – A.18.1.3 Protección de registros

CLÁUSULAS DEL ANEXO A - NTP ISO/IEC 27001:2014			PREGUNTA					RESULTADO
			N° de Pregunta	Cant. De Resp. positivas	Cant. De Resp. Negativas	% de Trabajadores con conocimiento	% de Trabajadores sin conocimiento	
DESCRIPCIÓN	N°							
Cumplimiento	A. 18	A. 18.1.3	14.3	10	50	16,67%	83,67%	Vulnerabilidad

**Nota.** Fuente: Elaborado por el autor

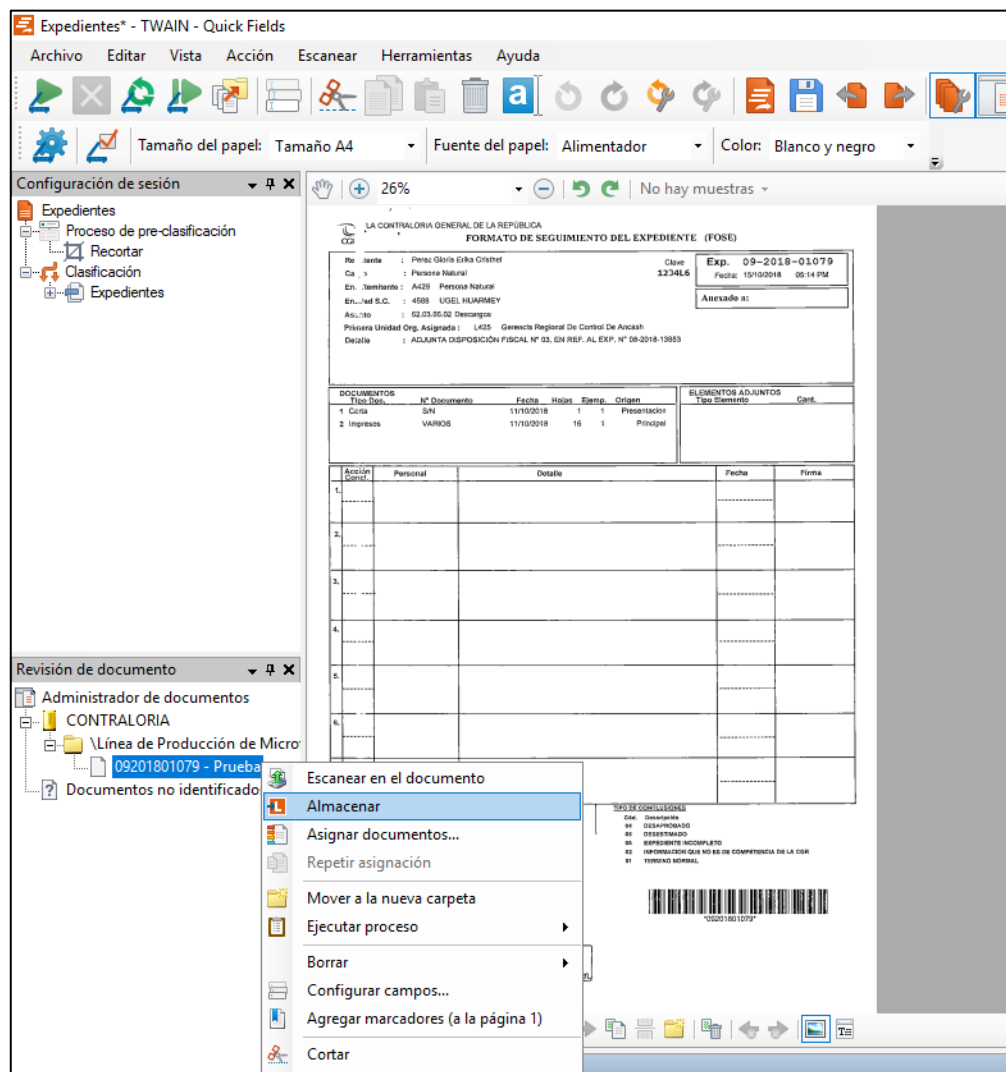


**Figura 39.** Gráfico porcentual de la Vulnerabilidad N° 20

Fuente: Elaborado por el autor



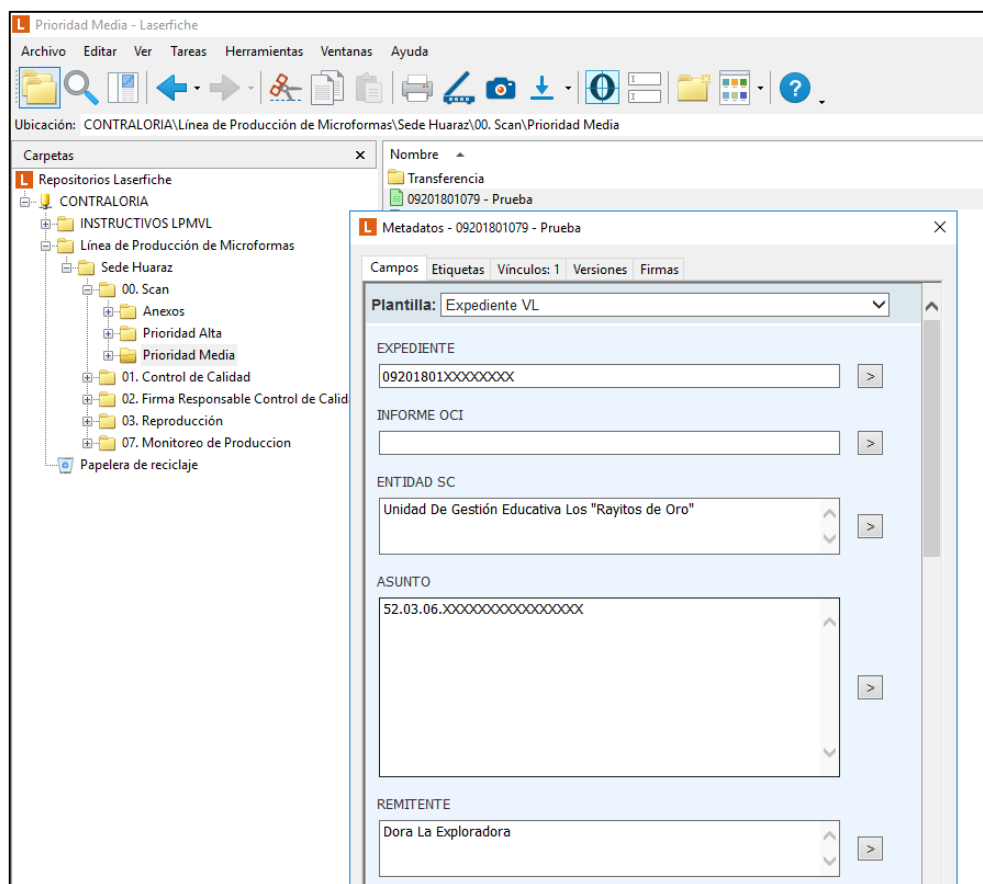
**Documentación - Vulnerabilidad N° 20 – A.18.1.3 Protección de registros**



**Figura 40.** Captura de pantalla, Software QuickField – Digitalización de prueba

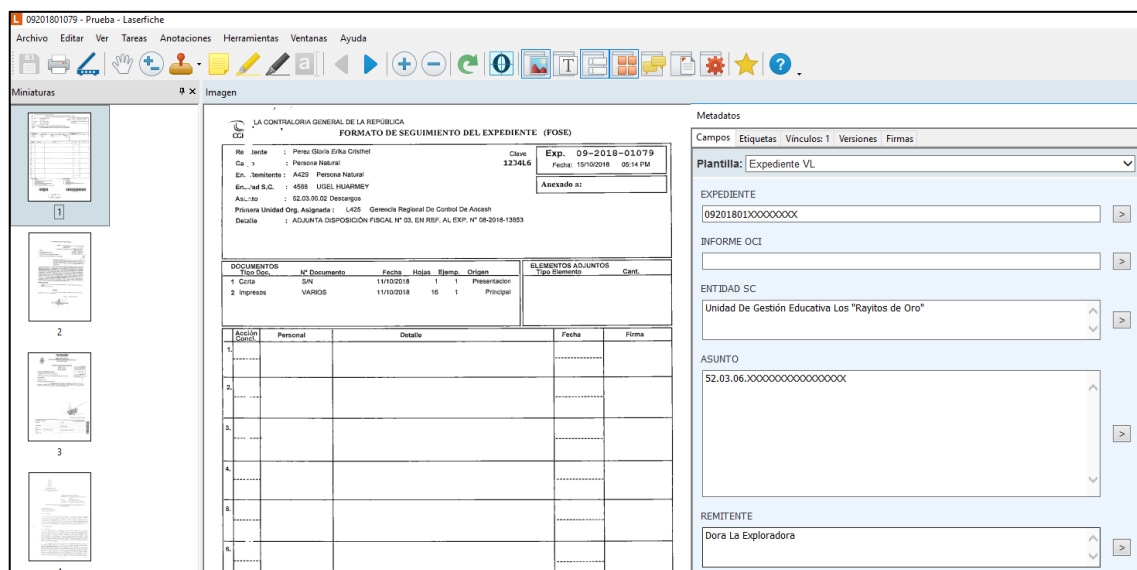
**Fuente:** Elaborado por el autor

En la Figura 40, se realizó la digitalización de un documento en calidad de prueba desde el software Quick Field, con la finalidad de advertir las vulnerabilidades en seguridad de la información del software Laserfiche que sirve como repositorio de todos los documentos digitalizados.



**Figura 41.** Captura de pantalla, Software Laserfiche – Digitalización de prueba

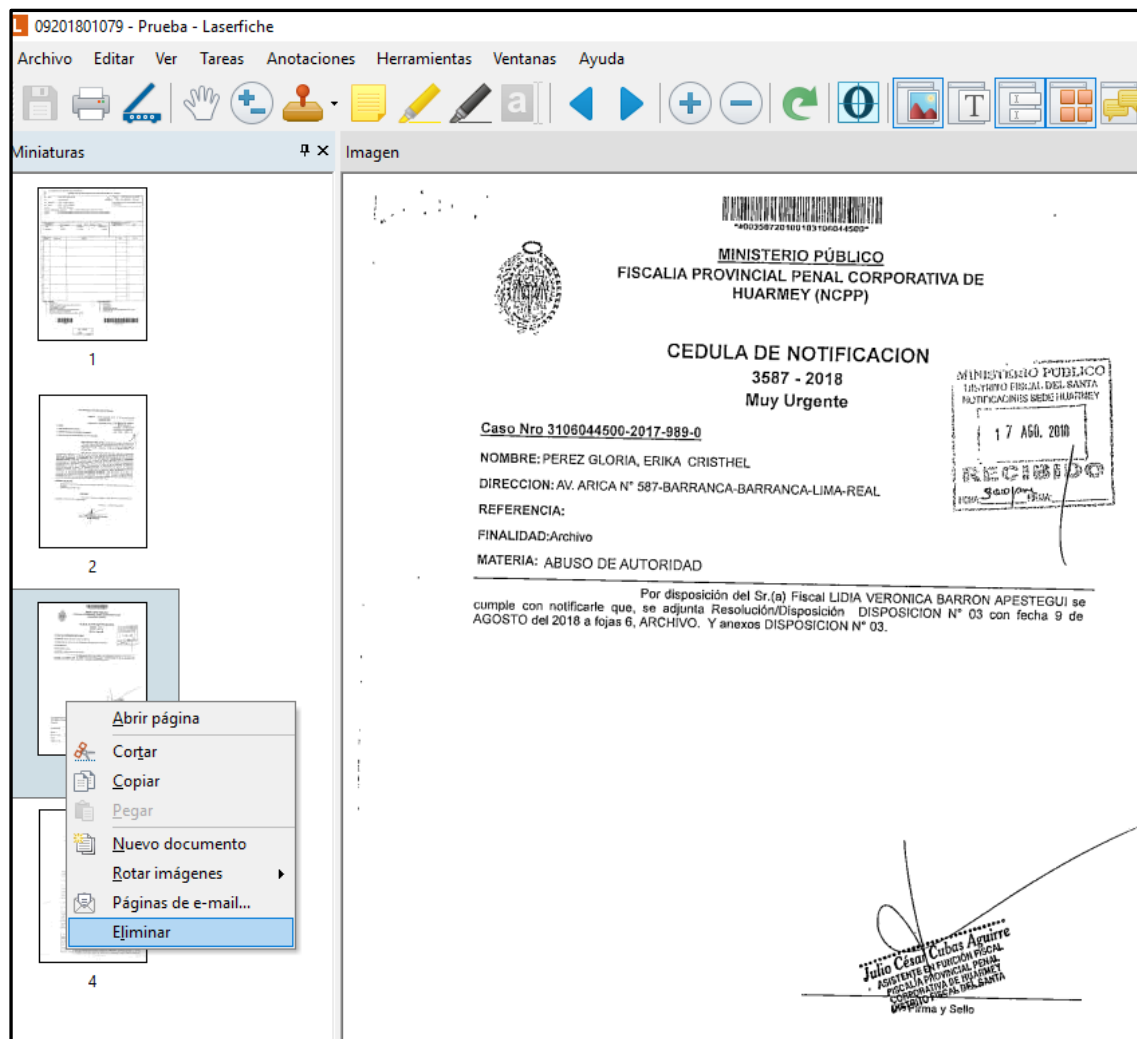
**Fuente:** Elaborado por el autor



**Figura 42.** Captura de pantalla, Software Laserfiche – Digitalización de prueba

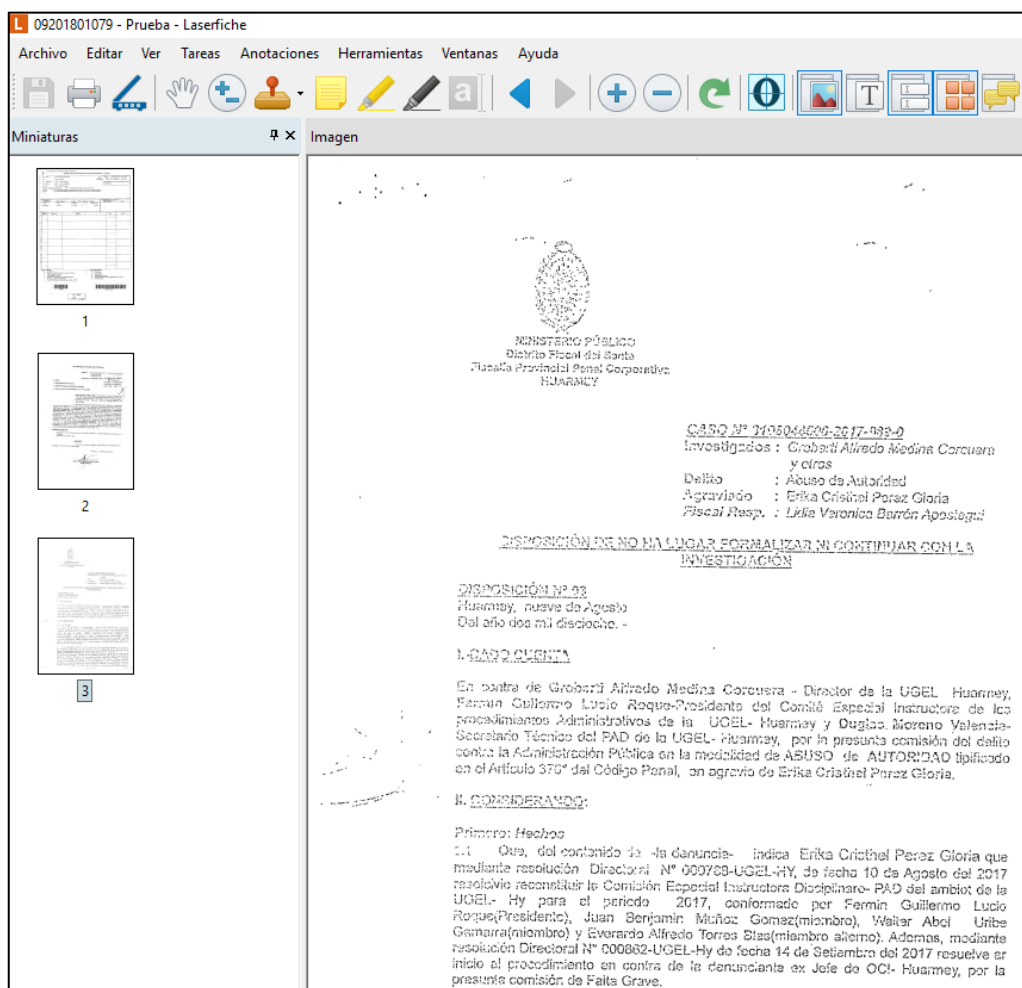
**Fuente:** Elaborado por el autor

En la Figura 41, se advierte que la plantilla del documento de prueba, la cual contiene todos los datos del documento, puede ser fácilmente adulterada, sin ningún tipo de restricción al momento de sobrescribir los registros, prueba de ello, se refleja en la Figura 42, donde se puede visualizar el contenido del documento con la información adulterada.



**Figura 43.** Captura de pantalla, Software Laserfiche – Eliminación de imágenes

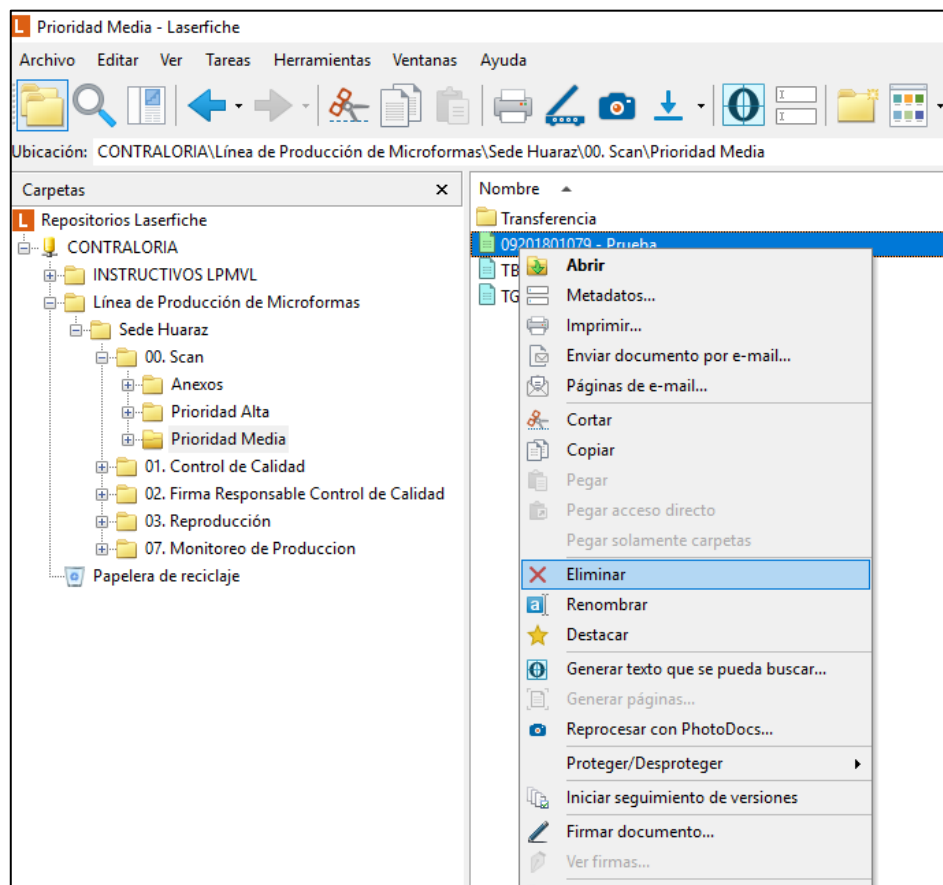
**Fuente:** Elaborado por el autor



**Figura 44.** Captura de pantalla, Software Laserfiche – Eliminación de imágenes

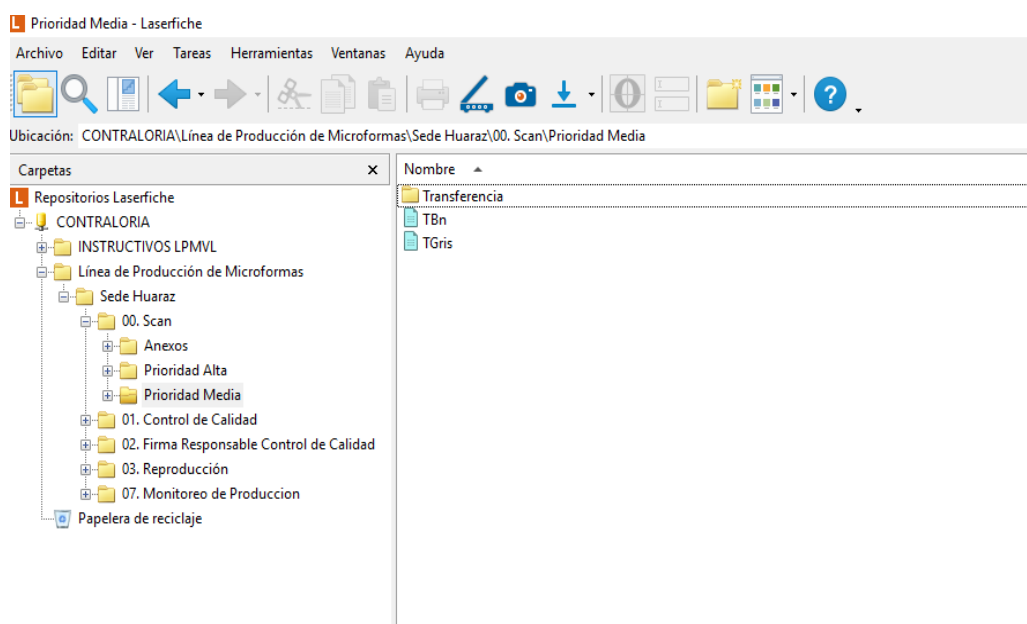
**Fuente:** Elaborado por el autor

En la Figura 43, se advierte que el contenido del documento digitalizado (cantidad de imágenes) puede ser eliminado sin ningún tipo de restricción o autorización, prueba de ello, se refleja en la Figura 44, donde se muestra que el documento digitalizado contiene menos imágenes que las digitalizadas en primera instancia.



**Figura 45.** Captura de pantalla, Software Laserfiche – Eliminación de documento

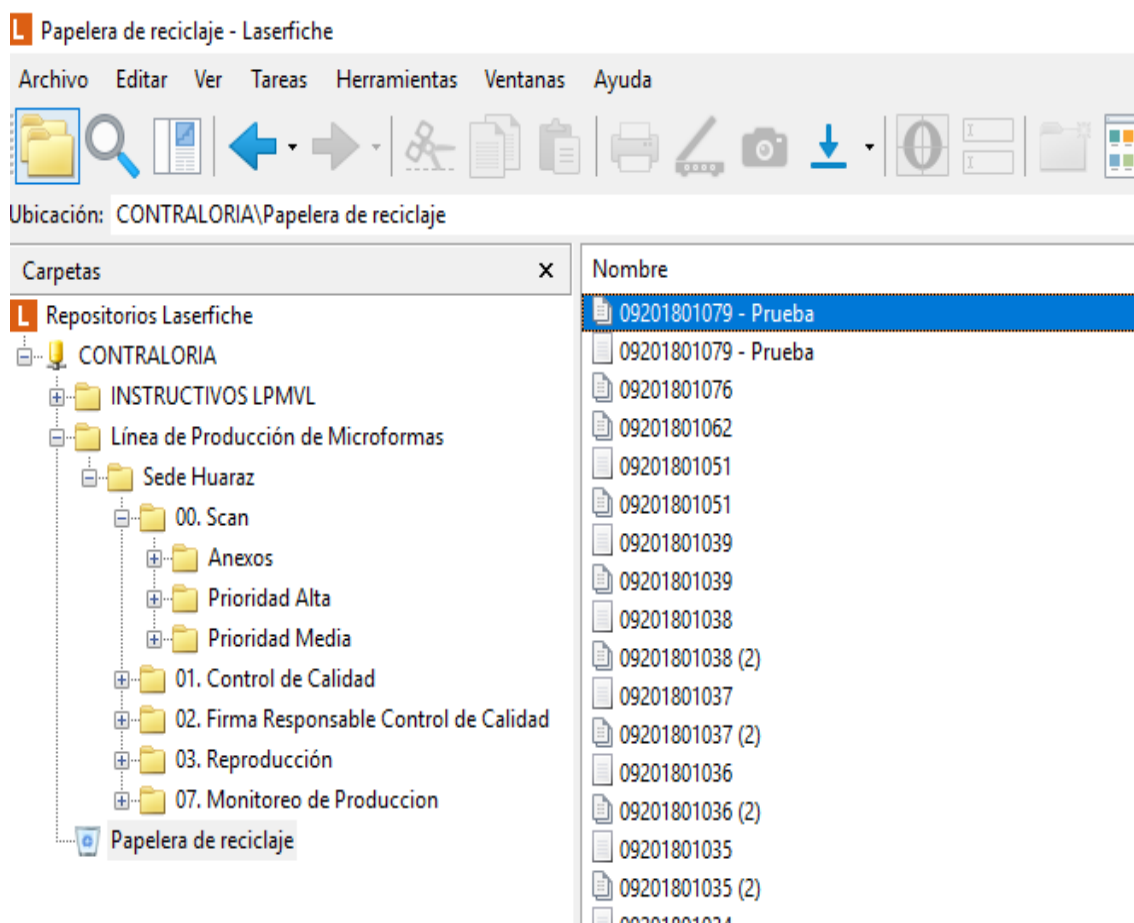
**Fuente:** Elaborado por el autor



**Figura 46.** Captura de pantalla, Software Laserfiche – Eliminación de documento

**Fuente:** Elaborado por el autor





**Figura 47.** Captura de pantalla, Software Laserfiche – Papelera de reciclaje

Fuente: Elaborado por el autor

En las Figura 45,46 y 47, se puede advertir que cualquier documento de la LPM que se encuentre almacenado en el software Laserfiche puede ser eliminado parcialmente o en su totalidad, vulnerando claramente la Cláusula A.18.1.3 “Protección de registros” de la NTP ISO/IEC 27001, que establece que los registros deben ser protegidos de cualquier pérdida, destrucción, falsificación y divulgación no autorizada.

### Vulnerabilidades de Seguridad de Información en el Software de la LPM

De las 20 vulnerabilidades de seguridad de información advertidas, se pudo identificar que 04 de ellas están relacionadas al software de la Línea de Producción de Microformas de la Contraloría General de la República.

Las vulnerabilidades advertidas relacionadas al software de la LPM son las siguientes:



***Vulnerabilidad N° 06 – A.9.4.1 Restricción de acceso a la información***

Documentada con las Figuras 18, 19 y 20 (Págs.54-55)

***Vulnerabilidad N° 07 – A.9.4.2 Procedimiento de ingreso seguro***

Documentada con las Figuras 21, 22 y 23 (Págs.56-57)

***Vulnerabilidad N° 17 – A.13.2.1 Políticas y procedimientos de transferencia de la información.***

Documentada con las Figuras 34, 35 y 36 (Págs.65-66)

***Vulnerabilidad N° 20 – A.18.1.3 Protección de registros***

Documentada con las Figuras 41 al 48 (Págs.70-75)

# CAPÍTULO IV. DISCUSIÓN

#### 4.1. Discusión de resultados

En el objetivo realizar un análisis de la seguridad de información de la línea de producción de microformas de la Contraloría General de la República; se obtuvo como resultado 20 registros porcentuales menores al 80%, considerados como vulnerabilidades de seguridad de la información de la Línea de Producción de Microformas, en referencia a diferentes controles de la NTP ISO/IEC 27001:2014.

Este resultado se contrasta con lo que nos explica Guerrero, Garcés, & Muñoz (2015) en su tesis de pregrado busco formalizar y plantear estrategias para mitigar los riesgos hallados para prevenir y fortalecer la seguridad para controlar el acceso de Sistema de Gestión Documental. Se aplicó un software libre Open VAS, la cual evidencia las posibles vulnerabilidades y seguridad existentes en los sistemas dentro de la empresa.

Asimismo, los hallazgos encontrados son de suma importancia porque nos ayudaran a mejorar la seguridad de la información dentro de la empresa, a la vez que con el estudio tomado como referencia que nos indica cómo prevenir y fortalecer la seguridad de sus sistemas mediante el Open VAS.

En el objetivo seleccionar los controles recomendados por la norma técnica peruana NTP ISO/IEC 27001:2014 que servirán para la mitigación de vulnerabilidades de seguridad de información de la línea de producción de microformas de la Contraloría General de la República; se logró la mitigación de los 15 fallos considerados prioritarios, esto, gracias a la implementación de los controles de la NTP ISO/IEC 27001:2014 sobre las deficiencias encontradas.

Por lo que Alexander (2007), explica que el modelo ISO 27001: 2014 fue elaborado bajo la visión de procesos. SGSI tiene la finalidad de funcionar en todo tipo de empresa, desarrollándose bajo el enfoque de proceso. El modelo ISO 27001: 2014, en su desarrollo de procesos permite que las empresas influyeran en el rendimiento del paradigma mediante las consideraciones estratégicas, estos son conocidos como las política y objetivos. Por lo que coincidimos que se realizó la medición de la eficiencia de los controles aplicados, culminado con la elaboración de planes de acciones preventivas y correctivas; aplicando esta ISO 27001:2014 los procesos mejorarán, las vulnerabilidades se reducirán dentro de las áreas de la empresa y sus sistemas.

En el objetivo listar las vulnerabilidades encontradas e identificar las de alto índice de riesgo y el tratamiento que se le deben dar a través de planes de acciones correctivas y preventivas.

Se obtuvo como primer resultado la detección de 20 vulnerabilidades en la seguridad de información de la Línea de Producción de Microformas, estas vulnerabilidades resultaron del procesamiento de información de las encuestas aplicadas a los 60 trabajadores del Dpto. De Gestión documentaria; cada vulnerabilidad encontrada está relacionada a una pregunta específica que tiene como referencia un control de la NTP ISO/IEC 27001:2014. Cada una de las vulnerabilidades encontradas se encuentra relacionada a una sola pregunta y está asignada a una única cláusula, por lo que no puede una pregunta ser aplica a más de un control, no obstante, se realizó una segunda verificación, con el propósito de que las vulnerabilidades advertidas correspondan a las cláusulas anteriormente identificadas. Luego de una segunda revisión de las vulnerabilidades encontradas, se procedió a su tratamiento, comenzando con la identificación de posibles riesgos y el impacto que tuvieran, y luego, a través del análisis y evaluación de riesgos se pudo advertir que, de las 20 vulnerabilidades, 15 de ellas son consideradas de gravedad muy alta y de índice de prioridad de riesgo entre 25 y 75.

Este resultado obtenido se contrasta con los que nos explica Ríos (2014) en su investigación nos brinda una visión de manera general de la situación actual de las herramientas que se encuentran disponibles para la exploración y análisis de las vulnerabilidades en sistemas de información y de manera concreta en redes de computadoras. Los resultados que se obtuvo han confirmado que la detección y análisis de vulnerabilidades por parte del que administra la red de sistemas de manera eficaz permite a la empresa ofrecer en asuntos de mejorar las técnicas para mejorar la seguridad de información y evitar potenciales ataques al sistema.

Cabe mencionar que el tratamiento adecuado de las vulnerabilidades de seguridad de la información, se mencionan de forma detallada en el Cap. V – Propuesta de investigación del presente trabajo, teniendo como resultado final la elaboración de un Manual de Seguridad de la Información para la Línea de Producción de Microformas.

# **CAPÍTULO V. PROPUESTA DE INVESTIGACIÓN**



## 5.1. Introducción

La propuesta de investigación para el presente proyecto está dividida en tres etapas, las cuales se indican a continuación:

- Entradas
- Proceso y
- Salida

La primera etapa la conforman los ingresos que conciernen a la información de los Sistemas de Información, Recursos Tecnológicos y los datos de las encuestas aplicadas al personal de la Línea de Producción de Microformas, la segunda etapa está relacionada a los procedimientos, que busca promover la adopción de la técnica PHVA (Planear – Hacer - Verificar – Actuar); en la cual se tendrá como referencia las vulnerabilidades encontradas como producto de la interpretación de resultados de las encuestas aplicadas, para que través de la mitigación de riesgos mejorar la Seguridad de la Información en la Línea de Producción de Microformas; y por último, la tercera etapa que es la salida, donde tendremos como producto final el Manual de Seguridad de la Información para la Línea de Producción de Microformas.

## 5.2. Entradas

### Plantilla para los Recursos Tecnológicos.

Esta plantilla mostrará los principales campos características de los recursos tecnológicos, que se encuentran en el Dpto. de Gestión Documentaria; necesarios para las labores cotidianas.

**Tabla 16.** *Plantilla – Recursos Tecnológicos*

Nº	Marca	Modelo o Procesador	HD	RAM	Sistema Operativo	Servicio	Equipo	Fecha de Ingreso	Estado (O, OL, NO) a
1	XEROX	WORK CENTRE 5755	N/A	N/A	N/A	Impresiones	Impresora	30/03/2011	O
2	IBM-LENOVO	THINKPAD T430	1 TB	4GB	Windows 7	Multioperaciones	LAPTOP	30/03/2011	OL
3	HP-COMP AQ	8100 Elite CMT PC	500 GB	2GB	Windows 7	Multioperaciones	CPU	30/03/2011	O
4	HP-COMP AQ	KB-0316	N/A	N/A	N/A	Escritura	Teclado	30/03/2011	O
5	HP-COMP AQ	LA2405wg	N/A	N/A	N/A	Lectura	Monitor	30/03/2011	O
6	MOTO	LS2208	N/A	N/A	N/A	Lecturas de códigos	Lectora de	30/03/	O

	ROLA					de barra	Código de Barras	2011	
7	FUJITSU	Fi-6240Z	N/A	N/A	N/A	Capturador de imagen	Escáner	30/03/2011	O
8	FUJITSU	Fi-6800	N/A	N/A	N/A	Capturador de imagen	escáner	30/03/2011	OL
9	ELISE	LEDA POWER	N/A	N/A	N/A	Estabilizador de energía	Estabilizador	30/03/2011	O
10	EPSON	L800	N/A	N/A	N/A	Impresiones	Impresora	30/03/2011	O
11	CONTEX	SD4490	N/A	N/A	N/A	Capturador de imagen	escáner	30/03/2011	OL
12	RSA	SAJENET 4000	N/A	N/A	N/A	Aplicador de Firma digital	TOKEN	30/03/2011	O

**Nota.** Fuente: Elaborado por el autor,

O = Operativo; OL = Operativo con limitaciones; NO = No operativo

## Plantilla para los Sistemas de Información

Esta plantilla describe las características de los sistemas de información que se manejan en el Dpto. de Gestión Documentaria.

**Tabla 17.** Plantilla – Sistemas de Información

Nº	Tipo de Sistema	Nombre	Proveedor	Versión	Responsable	Fecha de Ingreso	Estado (O, OL, NO) a
1	Software	Laserfiche Server	Laserfiche	9.0.1	Supervisor de LPM	04/04/2011	O
2	Software	Laserfiche Audit Trail Advanced	Laserfiche	9.0.1	Supervisor de LPM	04/04/2011	O
3	Software	Laserfiche Web Access	Laserfiche	9.0.1	Supervisor de LPM	04/04/2011	O
4	Software	Laserfiche Email	Laserfiche	9.0.1	Supervisor de LPM	04/04/2011	O
5	Software	Laserfiche Snapshot	Laserfiche	9.0.1	Supervisor de LPM	04/04/2011	O
6	Software	Laserfiche ScanConnect	Laserfiche	9.0.1	Supervisor de LPM	04/04/2011	O
7	Software	Laserfiche Toolkit	Laserfiche	9.0.1	Supervisor de LPM	04/04/2011	O
8	Software	Laserfiche Use Full Named	Laserfiche	9.0.1	Supervisor de LPM	04/04/2011	O
9	Software	Laserfiche CD	Laserfiche	9.0.1	Supervisor de	04/04/2011	O

		Plus	LPM				
10	Software	Laserfiche Quick Fields	Laserfiche	9.0.1	Supervisor de LPM	04/04/2011	O
11	Software	Cosign For Laserfiche	Laserfiche	9.0.1	Supervisor de LPM	04/04/2011	O
12	Correo	Lotus Notes 8.0	Lotus Notes	8.0	Supervisor de LPM	04/04/2011	O
13	Sistema Operativo	Windows 7	Windows	7	Supervisor de LPM	04/04/2011	O

**Nota.** Fuente: Elaborado por el autor,

O = Operativo; OL = Operativo con limitaciones; NO = No operativo, SI = Sistema de Información.

### Base de Datos de las encuestas aplicadas.

Esta entrada comprende la información consolidada de todas las respuestas obtenidas al aplicar las encuestas al personal de la LPM, donde cada pregunta esta enlazada a un control específico de la NTP ISO/IEC 27001:2014. Ver Listado de preguntas en el Anexo

**Tabla 18.** Consolidado de respuestas afirmativas y negativas por cláusula

N° de Pregunta		N° de Cláusula		CANTIDAD	
				SI	NO
P1	1.1	A.5	A. 5.1.1	54	6
	1.2		A. 5.1.2	50	10
P2	2.1	A.6	A. 6.1.1	59	1
	2.2		A. 6.1.2	52	8
	2.3		A. 6.1.3	50	10
	2.4		A. 6.1.4	54	6
	2.5		A. 6.1.5	50	10
	2.6		A. 6.2.1	6	54
	2.7		A. 6.2.2	53	7
P3	3.1	A.7	A. 7.1.1	54	6
	3.2		A. 7.1.2	52	8
	3.3		A. 7.2.1	54	6
	3.4		A. 7.2.2	0	60
	3.5		A. 7.2.3	54	6
	3.6		A. 7.3.1	53	7
P4	4.1	A. 8	A. 8.1.1	52	8
	4.2		A. 8.1.2	53	7
	4.3		A. 8.1.3	51	9
	4.4		A. 8.1.4	11	49
	4.5		A. 8.2.1	57	3
	4.6		A. 8.2.2	56	4
	4.7		A. 8.2.3	52	8
	4.8		A. 8.3.1	55	5

		4.9		A. 8.3.2	49	11
		4.10		A. 8.3.3	7	53
	P5	5.1	A. 9	A. 9.1.1	57	3
		5.2		A. 9.1.2	5	55
		5.3		A. 9.2.1	50	10
		5.4		A. 9.2.2	49	11
		5.5		A. 9.2.3	54	6
		5.6		A. 9.2.4	53	7
		5.7		A. 9.2.5	49	11
		5.8		A. 9.2.6	50	10
		5.9		A. 9.3.1	56	4
		5.10		A. 9.4.1	11	49
		5.11		A. 9.4.2	12	48
		5.12		A. 9.4.3	54	6
		5.13		A. 9.4.4	52	8
		5.14		A. 9.4.5	6	54
	P6	6.1	A. 10	A. 10.1.1	50	10
		6.2		A. 10.1.2	54	6
	P7	7.1	A. 11	A. 11.1.1	8	52
		7.2		A. 11.1.2	9	51
		7.3		A. 11.1.3	55	5
		7.4		A. 11.1.4	53	7
		7.5		A. 11.1.5	51	9
		7.6		A. 11.1.6	50	10
		7.7		A. 11.2.1	53	7
		7.8		A. 11.2.2	11	49
		7.9		A. 11.2.3	54	6
		7.10		A. 11.2.4	53	7
		7.11		A. 11.2.5	55	5
		7.12		A. 11.2.6	56	4
		7.13		A. 11.2.7	3	57
		7.14		A. 11.2.8	11	49
	P8	8.1	A. 12	A. 11.2.9	50	10
		8.2		A. 12.1.1	53	7
		8.3		A. 12.1.2	52	8
		8.4		A. 12.1.3	51	9
		8.5		A. 12.1.4	51	9
		8.6		A. 12.2.1	53	7
		8.7		A. 12.3.1	58	2
		8.8		A. 12.4.1	54	6
		8.9		A. 12.4.2	55	5
		8.10		A. 12.4.3	56	4
		8.11		A. 12.4.4	57	3
		8.12		A. 12.5.1	52	8
		8.13		A. 12.6.1	53	7
		8.14		A. 12.6.2	9	51
	P9	9.1	A. 13	A. 12.7.1	52	8
		9.2		A. 13.1.1	7	53
		9.3		A. 13.1.2	48	12
		9.4		A. 13.1.3	49	11
		9.5		A. 13.2.1	6	54
		9.6		A. 13.2.2	55	5
				A. 13.2.3	55	5



	9.7		A. 13.2.4	52	8
P10	10.1	A. 14	A. 14.1.1	53	7
	10.2		A. 14.1.2	50	10
	10.3		A. 14.1.3	49	11
	10.4		A. 14.2.1	54	6
	10.5		A. 14.2.2	48	12
	10.6		A. 14.2.3	49	11
	10.7		A. 14.2.4	54	6
	10.8		A. 14.2.5	57	3
	10.9		A. 14.2.6	52	8
	10.10		A. 14.2.7	51	9
	10.11		A. 14.2.8	49	11
	10.12		A. 14.2.9	50	10
	10.13		A. 14.3.1	50	10
P11	11.1	A. 15	A. 15.1.1	53	7
	11.2		A. 15.1.2	49	11
	11.3		A. 15.1.3	52	8
	11.4		A. 15.2.1	50	10
	11.5		A. 15.2.2	52	8
P12	12.1	A. 16	A. 16.1.1	53	7
	12.2		A. 16.1.2	50	10
	12.3		A. 16.1.3	11	49
	12.4		A. 16.1.4	57	3
	12.5		A. 16.1.5	52	8
	12.6		A. 16.1.6	51	9
	12.7		A. 16.1.7	52	8
P13	13.1	A. 17	A. 17.1.1	9	51
	13.2		A. 17.1.2	52	8
	13.3		A. 17.1.3	50	10
	13.4		A. 17.2.1	52	8
P14	14.1	A. 18	A. 18.1.1	55	5
	14.2		A. 18.1.2	52	8
	14.3		A. 18.1.3	10	50
	14.4		A. 18.1.4	52	8
	14.5		A. 18.1.5	51	9
	14.6		A. 18.2.1	50	10
	14.7		A. 18.2.2	49	11
	14.8		A. 18.2.3	52	8

**Nota.** Fuente: Elaborado por el autor

### 5.3. Proceso

El proceso dentro de la propuesta de investigación está basado en el Ciclo PDCA; de la metodología propuesta se desprende el estudio realizado para la detección de las 20 vulnerabilidades en la seguridad de la información, advertidas en la primera fase, estas vulnerabilidades son producto del resultado de aplicar la encuesta al personal de la Línea de Producción de Microformas, para posteriormente mitigar los riesgos encontrados a través de herramientas y elaborar un Manual de Seguridad de la Información para la Línea de Producción de Microformas.







**Figura 48.** Ciclo PDCA para el Manual de Seguridad

**Fuente:** Elaborado por el autor

La figura 48 contiene un resumen general de la fase proceso, donde se profundiza cada entregable de las diferentes etapas del ciclo, lo que sirve de ayuda a desarrollar herramientas para mitigar las vulnerabilidades advertidas.

### 5.3.1. Planear

En esta fase se define el alcance del Manual de Seguridad de la Información; las políticas y lineamientos sobre los que se desarrollará; también se presenta herramientas para la identificación de riesgos y del impacto, posteriormente se analizará y evaluará los riesgos encontrados, según el tipo de activo de información que se afectaría.



**Figura 49.** Proceso Planear

**Fuente:** Elaborado por el autor

### **5.3.1.1 Alcance**

Es de observancia y cumplimiento obligatorio para todos los trabajadores del Dpto. de Gestión Documentaria y de las sedes regionales que laboran en la Línea de Producción de Microformas, incluyendo los trabajadores con contratos administrativos de servicios y servicios por tercero, así como los trabajadores de empresas que mantienen una relación contractual con la institución, en tanto y en cuanto ejecuten sus actividades en la Línea de Producción de Microformas.

Asimismo, a los trabajadores de la Contraloría General de la República, que tengan contacto con los recursos e información de la Línea de Producción de Microformas.

### **5.3.1.2 Políticas de Seguridad de la Información de la Línea de Producción de Microformas.**

El Dpto. de Gestión Documentaria de la Contraloría General de la República es el órgano encargado de la producción de microformas; por lo consiguiente, debe resguardar la información que maneja y establecer las siguientes políticas de seguridad de la información en la Línea de Producción de Microformas.

Implementar medidas para resguardar la información que se maneja en la Línea de Producción de Microformas.

Asegurar la continuidad del funcionamiento de la Línea de Producción de Microformas.

Mejorar de manera continua los procesos referentes a la Seguridad de la información de la Línea de Producción de Microformas.

Promover la concientización de la seguridad de la información a los trabajadores que laboran en la Línea de Producción de Microformas.

Capacitar continuamente a los trabajadores, respecto a la seguridad de la información relacionada al Sistema de Producción de Microformas.

### **Objetivos específicos de control**

Los objetivos de control son directamente derivados del Anexo A, de la NTP ISO/IEC 27001:2014.

### **5.3.1.3 Identificación de Riesgos**

Realizado el inventario de activos de información y la aplicación de las encuestas al personal de la LPM, se logró identificar los riesgos de seguridad de información, teniendo como base la aplicación de los controles de la NTP ISO/IEC 27001:2014

En la tabla 19 se describe las vulnerabilidades advertidas con las cláusulas NTP-ISO/IEC 27001:2014; permitiendo conocer cuáles de estas cláusulas apoyaran a minimizar los riesgos encontrados.

**Tabla 19.** *Vulnerabilidades vs NTP ISO/IEC 27001:2014*

N°	Vulnerabilidades advertidas	NTP ISO/IEC 27001:2014
1	No existe una política o procedimiento definido para dispositivos móviles	A.6.2.1
2	No hay una capacitación a los trabajadores sobre conciencia de seguridad de la información	A.7.2.2
3	No siempre se retorna los activos de la manera adecuada una vez culminado el vínculo contractual	A.8.1.4
4	No se protege los medios de información contra el acceso no autorizado durante el transporte	A.8.3.3
5	Existe personal con demasiados accesos a los autorizados	A.9.1.2
6	Al no existir una política de control de acceso no hay una restricción de la información	A.9.4.1
7	No existe un procedimiento de ingreso seguro	A.9.4.2
8	Carencia de restricción de acceso al código fuente de los programas	A.9.4.5
9	No hay un perímetro de seguridad definido en las sedes provinciales	A.11.1.1
10	No existe un control de acceso restringido en las sedes provinciales	A.11.1.2
11	Los equipos de la LPM no están protegidos en caso de fallas eléctricas u otras alteraciones.	A.11.2.2
12	No se verifica oportunamente los equipos a reutilizar o en desuso	A.11.2.7
13	No existe una protección adecuada para los equipos desatendidos	A.11.2.8
14	Carencia de registro de eventos de las actividades de los usuarios, excepciones, fallas y otros.	A.12.4.1
15	No están implementadas reglas de instalación de software por parte de los usuarios	A.12.6.2
16	No existe una protección adecuada de los servidores de red	A.13.1.1
17	Los procedimientos formales establecidos para la transferencia de información no se cumplen	A.13.2.1
18	No se advierte oportunamente sospechas observadas en cuanto a la seguridad de información	A.16.1.3
19	No existe una planificación de continuidad en caso de situaciones adversas	A.17.1.1
20	Los registros carecen de protección contra pérdida, eliminación, alteración y otros.	A.18.1.3

**Nota.** Fuente: Elaborado por el autor

En la tabla 20 de Inventarios de Activos de Información se le ha adicionado el campo de las Vulnerabilidades para luego conocer el impacto que causa en ellos.

**Tabla 20.** *Inventario de Activos de información vs Vulnerabilidades*

Componentes del servicio	Identificación del activo	Vulnerabilidades	Tipo de Activo	Responsable	Ubicación	C I D
Componentes del servicio	Expedientes, cargos de oficios, informes de control, microformas, manuales y procedimientos	6,14,17 y 20	Información	Gerente, Supervisor LPM, Monitor	Dpto. De Gestión Documentaria	
	Laserfiche, Quick Fields, Cosign, etc	1,7,8 y 15	Software	Monitor LPM	Dpto. De Gestión Documentaria	
	Escáneres, Equipos de cómputo, Impresoras y Lectoras de códigos de barra	3,4,12 y 13	Físicos	Supervisor LPM	Dpto. De Gestión Documentaria	
	Servicios de mantenimiento, soporte, fedatario y custodia de microarchivo	9,10,11 y 16	Servicios	Monitor LPM	Dpto. De Gestión Documentaria	
	Gerentes, Coordinadores, Supervisores, Monitor y Responsables de procesos	2,5,18 y 19	Personal	Supervisor LPM	Dpto. De Gestión Documentaria	

**Nota.** Fuente: Elaborado por el autor,

C = Confidencialidad; I = Integridad; D = Disponibilidad, LPM = Línea de Producción de Microformas.

#### 5.3.1.4 Identificación del Impacto

Se comprenderá el impacto como el grado en el que se verá afectado determinado activo de información al alterar uno de sus componentes, Cuanto más grande sea la correlación del resultado y la alteración del activo, el impacto de ese activo será mayor.

Para La evaluación del impacto se propone 3 requisitos de los activos de información de una organización, como lo describe la NTP-ISO/IEC 27001:2014, que son Confidencialidad, Integridad y Disponibilidad.

Se estableció 5 niveles de impacto, muy alto, alto, medio, bajo, y muy bajo, según se comporte el activo de información en el momento de decidir cuál de los 5 niveles aplica para cada categoría.

**Tabla 21. Requisito de Confidencialidad (C)**

VALOR DEL ACTIVO	INTERPRETACIÓN DEL VALOR ASIGNADO DE ACUERDO AL REQUISITO DE CONFIDENCIALIDAD
Muy Alto (5)	Cuando la divulgación no autorizada de la información impacta <b>muy gravemente</b> en la operatividad, cumplimiento legal o imagen del Sistema de Producción de Microformas.
Alto (4)	Cuando la divulgación no autorizada de la información impacta <b>gravemente</b> en la operatividad, cumplimiento legal o imagen del Sistema de Producción de Microformas.
Medio (3)	Cuando la divulgación no autorizada de la información impacta <b>medianamente</b> en la operatividad, cumplimiento legal o imagen del Sistema de Producción de Microformas.
Bajo (2)	Cuando la divulgación no autorizada de la información impacta <b>levemente</b> en la operatividad, cumplimiento legal o imagen del Sistema de Producción de Microformas.
Muy Bajo (1)	Cuando la divulgación no autorizada de la información impacta <b>mínimamente</b> en la operatividad, cumplimiento legal o imagen del Sistema de Producción de Microformas.

**Nota.** Fuente: Elaborado por el autor.

**Tabla 22. Requisito de Integridad (I)**

VALOR DEL ACTIVO	INTERPRETACIÓN DEL VALOR ASIGNADO DE ACUERDO AL REQUISITO DE CONFIDENCIALIDAD
Muy Alto (5)	Cuando la modificación parcial o total de la información impacta <b>muy gravemente</b> en la operatividad, cumplimiento legal o imagen del Sistema de Producción de Microformas
Alto (4)	Cuando la modificación parcial o total de la información impacta <b>gravemente</b> en la operatividad, cumplimiento legal o imagen del Sistema de Producción de Microformas
Medio (3)	Cuando la modificación parcial o total de la información impacta <b>medianamente</b> en la operatividad, cumplimiento legal o imagen del Sistema de Producción de Microformas
Bajo (2)	Cuando la modificación parcial o total de la información impacta <b>levemente</b> en la operatividad, cumplimiento legal o imagen del Sistema de Producción de Microformas
Muy Bajo (1)	Cuando la modificación parcial o total de la información impacta <b>mínimamente</b> en la operatividad, cumplimiento legal o imagen del Sistema de Producción de Microformas

**Nota.** Fuente: Elaborado por el autor.



**Tabla 23.** Requisito de Disponibilidad (D)

VALOR DEL ACTIVO	INTERPRETACIÓN DEL VALOR ASIGNADO DE ACUERDO AL REQUISITO DE CONFIDENCIALIDAD
Muy Alto (5)	Cuando la falta de acceso a la información en el momento oportuno impacta <b>muy gravemente</b> en la operatividad, cumplimiento legal o imagen del Sistema de Producción de Microformas
Alto (4)	Cuando la falta de acceso a la información en el momento oportuno impacta <b>gravemente</b> en la operatividad, cumplimiento legal o imagen del Sistema de Producción de Microformas
Medio (3)	Cuando la falta de acceso a la información en el momento oportuno impacta <b>medianamente</b> en la operatividad, cumplimiento legal o imagen del Sistema de Producción de Microformas
Bajo (2)	Cuando la falta de acceso a la información en el momento oportuno impacta <b>levemente</b> en la operatividad, cumplimiento legal o imagen del Sistema de Producción de Microformas
Muy Bajo (1)	Cuando la falta de acceso a la información en el momento oportuno impacta <b>mínimamente</b> en la operatividad, cumplimiento legal o imagen del Sistema de Producción de Microformas

**Nota.** Fuente: Elaborado por el autor.

El desarrollo de la identificación del impacto se encuentra en la Tabla 24, donde se muestra el inventario de activos asociado a las diferentes vulnerabilidades encontradas, y con las priorizaciones de confidencialidad, integridad y disponibilidad.

**Tabla 24.** Inventario de Activos de información vs Vulnerabilidades e Impactos

Componentes del servicio	Identificación del activo	Vulnerabilidades	Tipo de Activo	Responsable	Ubicación	C	I	D
Componentes del servicio	Expedientes, cargos de oficios, informes de control, microformas, manuales y procedimientos	6,14,17 y 20	Información	Gerente, Supervisor LPM, Monitor	Dpto. De Gestión Documentaria	Muy Alto	Muy Alto	Muy Alto
	Laserfiche, Quick Fields,	1,7,8 y 15	Software	Monitor LPM	Dpto. De Gestión Documentaria	Muy Alto	Muy Alto	Muy Alto

Cosign, etc

ria

Escáneres, Equipos de cómputo, Impresoras y Lectoras de códigos de barra	3,4,12 y 13	Físicos	Supervisor LPM	Dpto. De Gestión Documenta ria	Muy Alto	Muy Alto	Muy Alto
Servicios de mantenimie nto, soporte, fedatario y custodia de microarchiv o	9,10,11 y 16	Servicios	Monitor LPM	Dpto. De Gestión Documenta ria	Muy Alto	Muy Alto	Muy Alto
Gerentes, Coordinador es, Supervisore s, Monitor y Responsable s de procesos	2,5,18 y 19	Personal	Supervisor LPM	Dpto. De Gestión Documenta ria	Muy Alto	Muy Alto	Muy Alto

**Nota.** Fuente: Elaborado por el autor,

C = Confidencialidad; I = Integridad; D = Disponibilidad, LPM = Línea de Producción de Microformas.

### 5.3.1.5 Análisis y Evaluación del Riesgo

En esta etapa se obtuvo una lista de riesgos identificados de acuerdo a la probabilidad de ocurrencia de una amenaza y de sus consecuencias de los impactos, ligadas a las vulnerabilidades existentes a los activos de información.

Para la estimación del riesgo, se empleó la matriz de Análisis Modal de Fallos y Efectos AMFE, teniendo como referencia los criterios de Detectabilidad, Frecuencia y Gravedad.

Una vez identificados los niveles de Detectabilidad, Frecuencia y Gravedad se procederá a encontrar el valor del Índice de Prioridad de Riesgo (IPR) a través de la siguiente formula:

$$IPR = D.G.F$$



La tabla 24 fue analizada de acuerdo a los límites y criterios del Manual de Seguridad de la Información, donde el objetivo principal es comparar el resultado de la estimación del riesgo con los criterios y aceptación definidos; en ese momento se priorizan las vulnerabilidades que deben ser tratadas y gestionadas, de acuerdo al resultado de la matriz AMFE.

La matriz AMFE nos permite evaluar la frecuencia, gravedad y defectibilidad de cada vulnerabilidad identificada. En este caso aplicado se dio prioridad a los IPR de valor 25 o superior con gravedad 5.

Los riesgos con un IPR de 25 o mayor presentan una gravedad alta que perjudica a la organización y a la calidad del proceso; es por esta razón que se usara el criterio de IPR.

Se encontraron 15 modos de Fallos con Gravedad 5 entre 25 y 75 de Índice de Prioridad de Riesgo; estos puntos serán los afrontados para la minimización de fallas.

**Tabla 25. Matriz AMFE**

Activos de Información	Tipo de Activo	N° de Riesgo	Modo de Fallo	Efecto	Causa	Frecuencia (F)	Gravedad (G)	Defectabilidad (D)	IPR
Expedientes, cargos de oficios, informes de control, microformas, manuales y procedimientos	Información	6	Falta de política de control de accesos	Vulnerabilidades, pérdida de información	Accesos no autorizados a los sistemas	2	5	3	30
		14	Falta de un registro de eventos o fallas	Vulnerabilidades, pérdida de información	Sin registros ni prevención de fallas	2	3	2	12
		17	Sin procedimientos establecidos para la transferencia de información	Vulnerabilidades, pérdida de información	Exposición de información	3	5	2	30
		20	Falta de una protección de los registros	Vulnerabilidad, pérdida de información	Eliminación, adulteración de información	4	5	2	40
Laserfiche, Quick Fields, Cosign, etc	Software	1	Falta de políticas de acceso a dispositivos móviles	Vulnerabilidad	Filtración de información	3	5	2	30
		7	Falta de procedimiento de ingreso seguro	Vulnerabilidades, pérdida de la confidencialidad	Filtración de información	4	5	2	40

Escáneres, Equipos de cómputo, Impresoras y Lectoras de códigos de barra	Físicos	8	Falta de control en el acceso al código fuente de los programas	Vulnerabilidades, pérdida de información	Carencia de restricción en el acceso a códigos fuentes	2	4	2	16
		15	Falta de reglas de instalación de software por parte de los usuarios	Vulnerabilidades, exposición de información	Desprevencción de vulnerabilidades técnicas	3	5	3	45
		3	Retorno inadecuado de los activos culminado el vínculo contractual	Complicaciones en la designación de responsabilidades	Verificación posterior a los activos entregados	3	5	2	30
		4	Falta de control de protección contra el acceso no autorizado durante el transporte	Activos malogrados, inservibles o de rápido deterioro	Mala manipulación de los activos	5	5	2	50
		12	Falta de verificación de los equipos a reutilizar	Activos malogrados, inservibles o de rápido deterioro	Sin políticas de reutilización de equipos	3	5	2	30
		13	Falta protección y resguardo para los equipos desatendidos	Activos malogrados, inservibles o de rápido deterioro	Sin políticas o procedimientos para equipos desatendidos	5	5	2	50
Servicios de mantenimiento, soporte, fedatario y custodia de microarchivo	Servicios	9	Sin perímetro de seguridad definido en las sedes provinciales	Perdida o adulteración de información	Información expuesta a cualquier agente desconocido	4	5	2	40
		10	Falta de control de acceso restringido en las sedes provinciales	Perdida o adulteración de información	Información expuesta a cualquier agente desconocido	3	5	2	30
		11	Falta de protección contra fallas de electricidad	Interrupción de la continuidad de las actividades	Carencia de UPS, o acumuladores de energía	4	3	2	24
		16	Falta de controles de red	Vulnerabilidades, pérdida de confidencialidad	Sin políticas de controles de acceso a red	3	4	1	12
Gerentes, Coordinadores, Supervisores, Monitores y Responsables de procesos	Personas	2	Falta capacitación a los trabajadores sobre conciencia de seguridad de la información	Posibles errores involuntarios	Personal sin conocimiento sobre temas de seguridad de la información	3	3	2	12
		5	Falta de limitación en accesos a los usuarios	Vulnerabilidades, pérdida de confidencialidad	Filtración de información	3	5	3	45

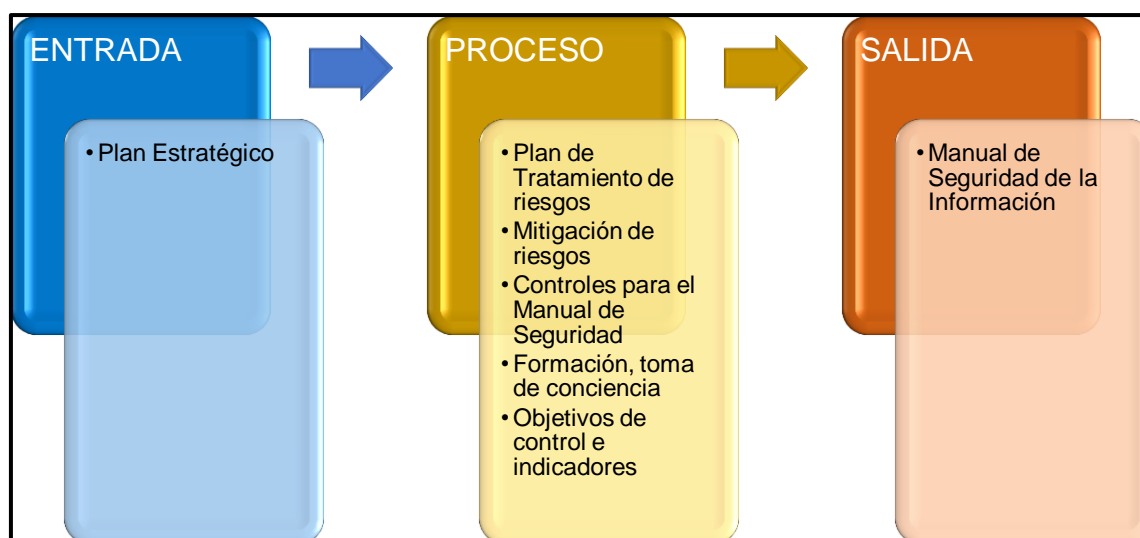
idad							
18	No se advierte oportunamente sospechas observadas en cuanto a la seguridad de información	Débil manejo de gestión de incidentes de seguridad	Carencia de reporte de debilidades	3	5	3	45
19	Falta de planificación de continuidad en caso de situaciones adversas	Equipos malogrados, pérdida de información	Sin plan de contingencia de continuidad	2	5	3	30

**Nota.** Fuente: Elaborado por el autor,

IPR = Índice de Prioridad de Riesgo

## 5.4. Hacer

En esta fase se ejecutó el Plan Estratégico determinado en la fase de PLANEAR, el cual implica analizar y desarrollar los controles que permitan mitigar los riesgos encontrados en la fase antes mencionada.



**Figura 50.** Proceso HACER

**Fuente:** Elaborado por el autor

### 5.4.1. Plan de tratamiento de riesgos

Mitigar los riesgos de las 15 vulnerabilidades de IPR > 25:

Vulnerabilidad N° 01 - Política de dispositivos móviles (Riesgo A.6.2.1)

Vulnerabilidad N° 03 - Retorno de activos (Riesgo A.8.1.4)



- Vulnerabilidad N° 04 – Transferencia de medios físicos (Riesgo A.8.3.3)
- Vulnerabilidad N° 05 - Acceso a redes y servicios de red (Riesgo A.9.1.2)
- Vulnerabilidad N° 06 - Restricción de acceso a la información (Riesgo A.9.4.1)
- Vulnerabilidad N° 07 – Procedimientos de ingreso seguro (Riesgo A.9.4.2)
- Vulnerabilidad N° 09 – Perímetro de seguridad física (Riesgo A.11.1.1)
- Vulnerabilidad N° 10 - Controles de ingreso físico (Riesgo A.11.1.2)
- Vulnerabilidad N° 12 – Disposición o reutilización segura de equipos (Riesgo A.11.2.7)
- Vulnerabilidad N° 13 – Equipos de usuarios desatendidos (Riesgo A.11.2.8)
- Vulnerabilidad N° 15 - Restricciones sobre la instalación de software (Riesgo A.12.6.2)
- Vulnerabilidad N° 17 - Políticas y procedimientos de la transferencia de la información (Riesgo A.13.2.1)
- Vulnerabilidad N° 18 - Reporte de debilidades de seguridad de la información (Riesgo A.16.1.3)
- Vulnerabilidad N° 19 - Planificación de continuidad de seguridad de la información (Riesgo A.17.1.1)
- Vulnerabilidad N° 20 – Protección de riesgos (Riesgo A.18.1.3)

Todos los riesgos deben ser asumidos por la Línea de Producción de Microformas y no transferidos a terceros por razones de seguridad interna, se recomienda eliminar los riesgos de mayor gravedad o de mitigarlos lo menos posible.

#### **5.4.2 Mitigación del riesgo**

Para el desarrollo de la mitigación de los riesgos se seleccionaron los controles de la NTP ISO/IEC 27001:2014; y se realizó verificaciones permanentes de los controles por medio de los indicadores implementados.

Para la selección de controles de la NORMA TÉCNICA PERUANA NTP ISO/IEC 27001: 2014, se usó las cláusulas advertidas en el plan de tratamiento de riesgos, descritas en el Anexo A de la presente Norma Técnica.

#### **5.4.3 Controles para las vulnerabilidades advertidas en la Línea de Producción de Microformas establecidos en la NTP ISO/IEC 27001:2014**

En este punto consideraremos las principales medidas de seguridad directamente con la Línea de Producción de Microformas del Dpto. de Gestión Documentaria, los controles y su implementación, tomando como base la NTP-ISO/IEC 27001:2014.

1. El control sobre “Política de dispositivos móviles” (A.6.2.1 del Anexo A de la NTP ISO/IEC 27001:2014) que se encuentra en la cláusula A.6.2 “DISPOSITIVOS MÓVILES Y TELETRABAJO” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2014, con el objetivo de asegurar la seguridad del teletrabajo y el uso de dispositivos móviles.

**Deficiencia:** No existe una política definida para dispositivos móviles.

**Implementación del Control:**

Establecer una política y medidas de seguridad de soporte, que deben ser adoptadas para gestionar los riesgos introducidos por el uso de dispositivos móviles.

2. El control sobre “Retorno de activos” (A.8.1.4 del Anexo A de la NTP ISO/IEC 27001:2014) que se encuentra en la cláusula A.8 “GESTIÓN DE ACTIVOS” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2014, con el objetivo de identificar los activos de la organización y definir responsabilidades de protección apropiadas.

**Deficiencia:** No siempre se retorna los activos de la manera adecuada una vez culminado el vínculo contractual

**Implementación del Control:**

Todos los empleados y usuarios de partes externas deben retornar todos los activos de la organización en su posesión a la conclusión de su empleo, contrato o acuerdo.

3. El control sobre “Transferencia de medios físicos” (A.8.3.3 del Anexo A de la NTP ISO/IEC 27001:2014) que se encuentra en la cláusula A.8 “GESTIÓN DE ACTIVOS” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC

27001:2014, con el objetivo de prevenir la divulgación, modificación, remoción o destrucción no autorizada de información almacenada en medios.

**Deficiencia:** No se protege adecuadamente los medios de información contra el acceso no autorizado durante el transporte de los activos.

**Implementación del Control:**

Los medios que contienen información deben ser protegidos contra el acceso no autorizado, el mal uso o la corrupción durante el transporte.

4. El control sobre “Acceso a redes y servicios de red” (A.9.1.2 del Anexo A de la NTP ISO/IEC 27001:2014) que se encuentra en la cláusula A.9 “CONTROL DE ACCESO” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2014, con el objetivo de limitar el acceso a la información y a las instalaciones de procesamiento de la información.

**Deficiencia:** Existe personal con demasiados accesos a los autorizados

**Implementación del Control:**

Los usuarios deben tener acceso solamente a la red y a servicios de red que hayan sido específicamente autorizados a usar.

5. El control sobre “Restricción de acceso a la información” (A.9.4.1 del Anexo A de la NTP ISO/IEC 27001:2014) que se encuentra en la cláusula A.9 “CONTROL DE ACCESO” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2014, con el objetivo de prevenir el acceso no autorizado a los sistemas y aplicaciones.

**Deficiencia:** No existe una política de control de acceso y de restricción a la información

**Implementación del Control:**

El acceso a la información y a las funciones del software de la línea de producción de microformas debe ser restringido en concordancia con la política de control de acceso.

6. El control sobre “Procedimientos de ingreso seguro” (A.9.4.2 del Anexo A de la NTP ISO/IEC 27001:2014) que se encuentra en la cláusula A.9 “CONTROL DE ACCESO” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2014, con el objetivo de prevenir el acceso no autorizado a los sistemas y aplicaciones.

**Deficiencia:** No existe un procedimiento de ingreso seguro a los sistemas de la LPM

**Implementación del Control:**

Implementar una política de control de acceso seguro a los sistemas y aplicaciones.

7. El control sobre “Perímetro de seguridad física” (A.11.1.1 del Anexo A de la NTP ISO/IEC 27001:2014) que se encuentra en la cláusula A.11 “SEGURIDAD FÍSICA Y AMBIENTAL” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2014, con el objetivo de impedir el acceso físico no autorizado, daño e interferencia a la información y a las instalaciones de procesamiento de la información de la organización.

**Deficiencia:** No existe un perímetro de seguridad física definido en las instalaciones de la LPM provinciales.

**Implementación del Control:**

Los perímetros de seguridad deben ser definidos y utilizados para proteger áreas que contienen información sensible o crítica e instalaciones de procesamiento de información.

8. El control sobre “Controles de ingreso físico” (A.11.1.2 del Anexo A de la NTP ISO/IEC 27001:2014) que se encuentra en la cláusula A.11 “SEGURIDAD FÍSICA Y AMBIENTAL” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2014, con el objetivo de impedir el acceso físico no autorizado, daño e interferencia a la información y a las instalaciones de procesamiento de la información de la organización.

**Deficiencia:** No existe un control de acceso restringido en las sedes provinciales.

**Implementación del Control:**

Las áreas seguras deben ser protegidas por medio de controles apropiados de ingreso para asegurar que se le permite el acceso sólo a personal autorizado.

9. El control sobre “Disposición o reutilización segura de equipos” (A.11.2.7 del Anexo A de la NTP ISO/IEC 27001:2014) que se encuentra en la cláusula A.11 “SEGURIDAD FÍSICA Y AMBIENTAL” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2014, con el objetivo de prevenir la pérdida, daño, robo o compromiso de activos e interrupción de las operaciones de la organización.

**Deficiencia:** No se verifica oportunamente los equipos a reutilizar o en desuso.

**Implementación del Control:**

Todos los elementos del equipo que contengan medios de almacenamiento deben ser verificados para asegurar que cualquier dato sensible y software con licencia se haya eliminado o se haya sobre escrito de manera segura antes de su disposición o reutilización.

10. El control sobre “Equipos de usuario desatendidos” (A.11.2.8 del Anexo A de la NTP ISO/IEC 27001:2014) que se encuentra en la cláusula A.11 “SEGURIDAD FÍSICA Y AMBIENTAL” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2014, con el objetivo de prevenir la pérdida, daño, robo o compromiso de activos e interrupción de las operaciones de la organización.

**Deficiencia:** No existe una protección adecuada para los equipos desatendidos.

**Implementación del Control:**

Los usuarios deben asegurarse de que el equipo desatendido tenga la protección apropiada.

11. El control sobre “Restricciones sobre instalación de software” (A.12.6.2 del Anexo A de la NTP ISO/IEC 27001:2014) que se encuentra en la cláusula A.12 “SEGURIDAD DE LAS OPERACIONES” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2014, con el objetivo de asegurar que las operaciones de instalaciones de procesamiento de la información sean correctas y seguras.



**Deficiencia:** No están implementadas reglas de instalación de software para los usuarios de la Línea de Producción de Microformas.

**Implementación del Control:**

Establecer reglas que gobiernen la instalación de software por parte de los usuarios de la Línea de Producción de Microformas.

12. El control sobre “Políticas y procedimientos de transferencia de la información” (A.13.2.1 del Anexo A de la NTP ISO/IEC 27001:2014) que se encuentra en la cláusula A.13 “SEGURIDAD DE LAS COMUNICACIONES” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2014, con el objetivo de asegurar la protección de la información en las redes y sus instalaciones de procesamiento de la información de apoyo.

**Deficiencia:** Los procedimientos formales establecidos para la transferencia de información no se cumplen

**Implementación del Control:**

Se debe hacer uso obligatorio de las políticas, procedimientos y controles de transferencia formales aplicados a proteger la transferencia de información a través del uso de todo tipo de instalaciones de comunicación.

13. El control sobre “Reporte de debilidades de seguridad de la información” (A.16.1.3 del Anexo A de la NTP ISO/IEC 27001:2014) que se encuentra en la cláusula A.16 “GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2014, con el objetivo de asegurar un enfoque consistente y efectivo a la gestión de incidentes de seguridad de la información, incluyendo la comunicación sobre eventos de seguridad y debilidades.

**Deficiencia:** No se advierte oportunamente sospechas observadas en cuanto a la seguridad de información

**Implementación del Control:**

Los empleados y contratistas que usan el sistema de la Línea de Producción de Microformas deben ser exigidos de advertir y reportar cualquier debilidad observada o de la que se sospecha en cuanto a la seguridad de la información en los sistemas o servicios.

14. El control sobre la “Planificación de continuidad de seguridad de la información” (A.17.1.1 del Anexo A de la NTP ISO/IEC 27001:2014) que se encuentra en la cláusula A.17 “ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2014, con el objetivo que la continuidad de seguridad de la información debe estar embebida en los sistemas de gestión de continuidad del negocio de la organización

**Deficiencia:** No existe una planificación de continuidad en caso de situaciones adversas

**Implementación del Control:**

La Línea de Producción de Microformas debe determinar sus requisitos de seguridad de la información y continuidad de la gestión de seguridad de la información en situaciones adversas, en casos de desastres o crisis.

15. El control sobre “Protección de registros” (A.18.1.3 del Anexo A de la NTP ISO/IEC 27001:2014) que se encuentra en la cláusula A.18 “CUMPLIMIENTO” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2014, con el objetivo de evitar infracciones de las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas a la seguridad de la información y a cualquier requisito de seguridad.

**Deficiencia:** Los registros carecen de protección contra pérdida, eliminación, alteración y otros.

**Implementación del Control:**

Los registros deben ser protegidos de cualquier pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, de acuerdo con los requisitos legislativos, regulatorios, contractuales y del negocio.

#### **5.4.4 Formación, toma de conciencia**

La Línea de Producción de Microformas implementará en su marco profesional la capacitación se su personal supervisor y monitor; personal que estará encargado de dirigir

las mejoras para la implementación del Manual de Seguridad de la Información y a su personal de Control de Calidad quienes estarán a cargo de la parte operativa en las distintas áreas en donde será implementado el Manual de Seguridad de la Información.

#### 5.4.5 Objetivos de control e indicadores

Estos son los Objetivos de Control determinados que nos ayudaran a mitigar los riesgos encontrados.

A.6.2.1 - Política de dispositivos móviles

A.8.1.4 - Retorno de activos

A.8.3.3 - Transferencia de medios físicos

A.9.1.2 - Acceso a redes y servicios de red

A.9.4.1 - Restricción de acceso a la información

A.9.4.2 - Procedimientos de ingreso seguro

A.11.1.1 - Perímetro de seguridad física

A.11.1.2 - Controles de ingreso físico

A.11.2.7 - Disposición o reutilización segura de equipos

A.11.2.8 - Equipos de usuarios desatendidos

A.12.6.2 - Restricciones sobre la instalación de software

A.13.2.1 - Políticas y procedimientos de la transferencia de la información

A.16.1.3 - Reporte de debilidades de seguridad de la información

A.17.1.1 - Planificación de continuidad de seguridad de la información

A.18.1.3 - Protección de riesgos

#### 5.4.6. Clausulas, Objetivos de control e indicadores

**Tabla 26.NTP vs Indicadores**

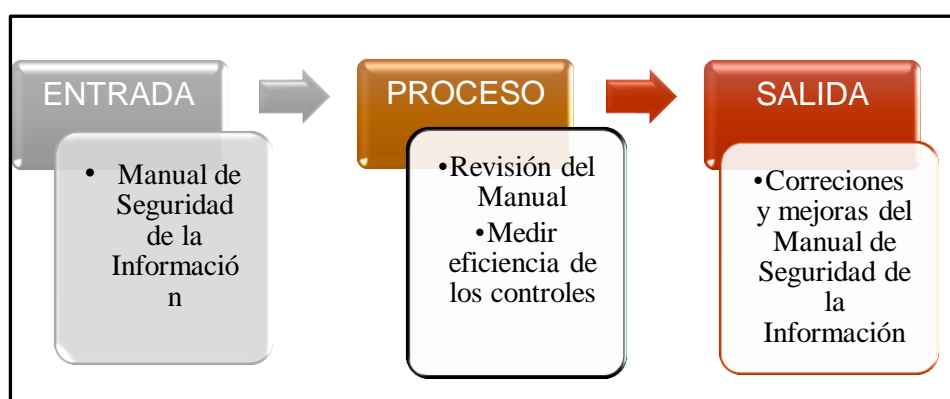
N°	NTP ISO/IEC 27001:2014	Indicadores
1	A.6.2.1	Sin políticas de dispositivos móviles
2	A.8.1.4	Sin procesos de retorno de activos
3	A.8.3.3	No se protege los medios de información contra acceso no autorizado
4	A.9.1.2	Sin control de los accesos de los usuarios
5	A.9.4.1	Escases de restricciones de acceso a la información
6	A.9.4.2	No existe un procedimiento de ingreso seguro
7	A.11.1.1	Falta un perímetro de seguridad

		física
8	A.11.1.2	Falta de controles de ingreso físico
9	A.11.2.7	No existe una verificación o control de los equipos a reutilizar
10	A.11.2.8	No existe una protección adecuada para los equipos desatendidos
11	A.12.6.2	Ausencia de restricciones sobre instalación de software
12	A.13.2.1	No se cumple con los procedimientos establecidos para la transferencia de información
13	A.16.1.3	Sin reporte de debilidades advertidas
14	A.17.1.1	No existe una planificación de continuidad de seguridad de la información
15	A.18.1.3	Carencia de protección de los registros

**Nota.** Fuente: Elaborado por el autor

## 5.5. Verificar

En esta fase verificaremos el Manual de Seguridad de la Información; y mediremos la eficiencia de los controles.



**Figura 51.** Proceso VERIFICAR

Fuente: Elaborado por el autor

### 5.5.1 Revisión de las vulnerabilidades advertidas.

En esta fase se revisó nuevamente las deficiencias encontradas en la Línea de Producción de Microformas y se verificó si cumple con los controles identificados; esta revisión sirve para encontrar nuevas deficiencias y/o controles que se ajusten. Para el presente caso no se encontraron más deficiencias por lo tanto son los mismos controles que satisfacen con los mismos.

**Tabla 27.** Check List Controladores

N°	Control	Deficiencia Encontrada	Cumple
1	A.6.2.1	Sin políticas de dispositivos móviles	<input type="checkbox"/>
2	A.8.1.4	Sin procesos de retorno de activos	<input type="checkbox"/>
3	A.8.3.3	No se protege los medios de información contra acceso no autorizado	<input type="checkbox"/>
4	A.9.1.2	Sin control de los accesos de los usuarios	<input type="checkbox"/>
5	A.9.4.1	Escases de restricciones de acceso a la información	<input type="checkbox"/>
6	A.9.4.2	No existe un procedimiento de ingreso seguro	<input type="checkbox"/>
7	A.11.1.1	Falta un perímetro de seguridad física	<input type="checkbox"/>
8	A.11.1.2	Falta de controles de ingreso físico	<input type="checkbox"/>
9	A.11.2.7	No existe una verificación o control de los equipos a reutilizar	<input type="checkbox"/>
10	A.11.2.8	No existe una protección adecuada para los equipos desatendidos	<input type="checkbox"/>
11	A.12.6.2	Ausencia de restricciones sobre instalación de software	<input type="checkbox"/>
12	A.13.2.1	No se cumple con los procedimientos establecidos para la transferencia de información	<input type="checkbox"/>
13	A.16.1.3	Sin reporte de debilidades advertidas	<input type="checkbox"/>
14	A.17.1.1	No existe una planificación de continuidad de seguridad de la información	<input type="checkbox"/>
15	A.18.1.3	Carencia de protección de los registros	<input type="checkbox"/>

**Nota.** Fuente: Elaborado por el autor



### 5.5.2 Medir eficiencia de los controles

Para medir la eficiencia de los controles, es decir, si realmente está funcionando correctamente, se debe de implementar herramientas como cartas de control, planes de verificación del Manual de Seguridad de la Información, balanced scorecard o cuadro de mando integral entre otros, que faciliten realizar el seguimiento del Manual de Seguridad de la Información y determinar su cumplimiento de acuerdo a la NTP-ISO/IEC 27001:20014.

**Tabla 28.** Plan de Verificación del Manual de Seguridad de Información

N°	Riesgo a controlar	Método de control			Objetivo de Control	Indicador
		Control Implementado	Registro	Responsable		
1	Sin políticas de dispositivos móviles	Políticas de dispositivos móviles	Registro de aprobación de políticas	Gerente del Dpto. de Gestión Documentaria	Elaborar, publicar y comunicar la política para dispositivos móviles	# de trabajadores con desconocimiento en políticas de dispositivos móviles
2	Sin procesos de retorno de activos	Procedimiento de retorno de activos	Registro de procedimiento	Monitor LPM	Elaborar y difundir al personal	# de trabajadores con desconocimiento en procedimientos de retorno de activos
3	Sin protección a los medios de información	Políticas de control de acceso	Registro de aprobación de políticas	Gerente del Dpto. de Gestión Documentaria	Elaborar, aprobar y difundir la política para controles de acceso	# de trabajadores con desconocimiento en políticas de control de acceso
4	Sin control de los accesos de					



los usuarios

5	Escases de restricciones de acceso a la información					
	No existe un procedimiento de ingreso seguro					
6	Falta un perímetro de seguridad física	Políticas de ingreso de personal y restricción de acceso.	Registro de aprobación de políticas	Gerente del Dpto. de Gestión Documentaria	Elaborar, aprobar y difundir la política de ingreso de personal	# de trabajadores con desconocimiento en políticas de ingreso de personal
	Falta de controles de ingreso físico					
7	No existe una verificación o control de los equipos a reutilizar	Política de equipos reutilizables y desatendidos	Registro de aprobación de políticas	Gerente del Dpto. de Gestión Documentaria	Elaborar, aprobar y difundir la política de equipos reutilizables y desatendidos	# de trabajadores con desconocimiento en políticas de equipos reutilizables y desatendidos
	No existe una protección adecuada para los equipos desatendidos					
8	Ausencia de restricciones sobre instalación de software	Restricciones de instalación de sw	Registro de restricciones	Monitor LPM	Elaborar, publicar y comunicar las restricciones de instalación de sw	# de trabajadores con desconocimiento en restricciones

						de instalación
12	No se cumple con los procedimientos establecidos para la transferencia de información	Reglamento de cumplimiento para los procedimientos de transferencia de información	Elaboración de Reglamento	Supervisor LPM	Exhortar el cumplimiento al personal sobre los procedimientos de transferencia de información	# de trabajadores que cumplen con el procedimiento de transferencia de información
13	Sin reporte de debilidades advertidas	Reporte de debilidades o amenazas advertidas	Elaboración de reporte de debilidades	Supervisor LPM	Elaborar, publicar y exigir la reportación de debilidades o amenazas a la seguridad de la información	# de trabajadores que no informan oportunamente debilidades respecto a la seguridad de la información
14	No existe una planificación de continuidad de seguridad de la información	Plan de continuidad de seguridad de la información	Elaboración de plan de continuidad	Gerente del Dpto. de Gestión Documentaria	Elaborar, aprobar y difundir el plan de continuidad de seguridad de la información	# de trabajadores con desconocimiento en plan de continuidad
15	Carencia de protección de registros	Implementación de restricciones y reglas para la protección de los registros	Elaboración de restricciones de acceso	Supervisor LPM	Elaborar el listado de restricciones, autorizaciones para la protección de los registros	#de eventos de registros eliminados o adulterados

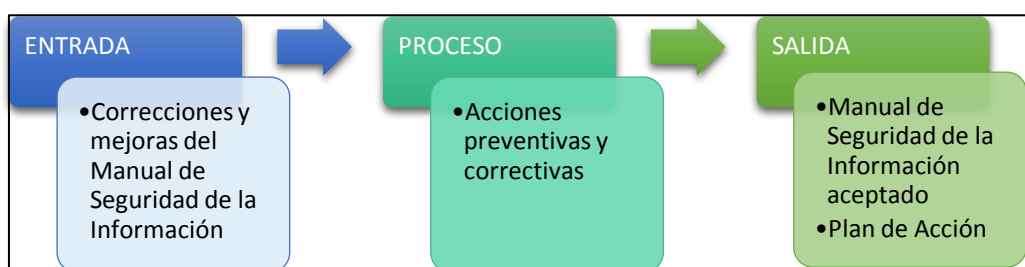
**Nota.** Fuente: Elaborado por el autor



## 5.6. Actuar

Es en esta fase se implementó las medidas preventivas y correctivas de las revisiones efectuadas y de esa manera mejorar el rendimiento del Manual de Seguridad de la Información.

Las medidas correctivas comprenden la selección de nuevos controles, la modificación de los existentes o la eliminación de los obsoletos.



**Figura 52. Proceso ACTUAR**

Fuente: Elaborado por el autor

## Entradas y Salidas del Proceso

Se utilizó la herramienta de las “5 ¿POR QUÉ?” para establecer los planes de acción efectivos al momento de resolver un problema dentro de la Línea de Producción de Microformas.

### 5.6.1 Acciones preventivas y correctivas

**Tabla 29. Plan de Acciones preventivas**

PLAN DE ACCIONES PREVENTIVAS			
N º	Riesgo a controlar	¿Por qué?	Acciones
1	Sin políticas de dispositivos móviles	1. No se ha elaborado una política de dispositivos móviles	- Elaborar y difundir una política de uso de dispositivos móviles
		2. No hay registros históricos de políticas de dispositivos móviles	- Concientizar al personal del cumplimiento de las políticas de uso dispositivos móviles
		3. El personal no se alinea a trabajar con normas	- Monitorear el cumplimiento de la política de dispositivos móviles por el personal de la Línea de Producción de Microformas
		4. No se tiene clara la importancia de las políticas del uso de dispositivos móviles	

		5. Poco interés del uso de políticas de dispositivos móviles	
2	Sin procesos de retorno de activos	1. No hay registros históricos de procesos de retorno de uso de activos	- Elaborar procesos para el retorno de los activos de la Línea de Producción de Microformas
		2. No se asignó una persona responsable para la elaboración de los procesos	- Exigir al personal el cumplimiento de los procesos de retorno de activos
		3. El personal no se alinea a trabajar con procesos definidos	- Monitorear el cumplimiento de los procesos de retorno de activos por parte del personal de la Línea de Producción de Microformas
		4. No se tiene clara la importancia de los procesos de retorno de uso de activos	
		5. Poco interés en la utilización de procesos de retorno de activos	
3	Sin protección a los medios de información	1. No se definió políticas de protección para los medios de información	- Elaborar políticas de protección a los medios de información
		2. No se asignó una persona responsable para la elaboración de las políticas de protección de medios de información	- Exigir al personal el cumplimiento de la política de protección de medios
		3. El personal no se alinea a trabajar con políticas definidas	- Monitorear el cumplimiento de la política de protección de medios de información, por parte del personal de la Línea de Producción de Microformas
		4. No se tiene clara la importancia de las políticas de protección de medios de información	
		5. Poco interés en la utilización de políticas de control de acceso	
4	Sin control de los accesos de los usuarios	1. No hay registros históricos de políticas de control de acceso	- Elaborar políticas de control de acceso para la Línea de Producción de Microformas
		2. No se asignó una persona responsable para la elaboración de las políticas de control de acceso	- Exigir al personal el cumplimiento de la política de control de acceso.
		3. El personal no se alinea a trabajar con políticas definidas	- Monitorear el cumplimiento de la política de control de acceso por parte del personal de la Línea de Producción de Microformas
		4. No se tiene clara la importancia	





		de las políticas de control de acceso	
		5. Poco interés en la utilización de políticas de control de acceso	
5	Escases de restricciones de acceso a la información	1. No hay registros históricos de políticas de control de acceso	- Elaborar políticas de control de acceso para la Línea de Producción de Microformas
		2. No se asignó una persona responsable para la elaboración de las políticas de control de acceso	- Exigir al personal el cumplimiento de la política de control de acceso.
		3. El personal no se alinea a trabajar con políticas definidas	- Monitorear el cumplimiento de la política de control de acceso por parte del personal de la Línea de Producción de Microformas
		4. No se tiene clara la importancia de las políticas de control de acceso	
		5. Poco interés en la utilización de políticas de control de acceso	
6	No existe un procedimiento de ingreso seguro	1. No hay registros de procedimientos establecidos para el ingreso seguro a las sw de la LPM	- Elaborar procedimientos para el ingreso seguro a los sistemas y aplicativos de la Línea de Producción de Microformas
		2. No se asignó una persona responsable para la elaboración de los procedimientos de ingreso seguro	- Exigir al personal el cumplimiento de los procedimientos establecidos
		3. El personal no se alinea a trabajar con procedimientos definidos	- Monitorear el cumplimiento de los procedimientos de ingreso seguro por parte del personal de la Línea de Producción de Microformas
		4. No se tiene clara la importancia de los procedimientos de ingreso seguro	
		5. Poco interés en la utilización de políticas de ingreso seguro	
7	Falta un perímetro de seguridad física	1. No hay registros históricos de perímetros de seguridad física que se hayan establecido	- Elaborar directivas o políticas para la implementación de un perímetro de seguridad para la Línea de Producción de Microformas
		2. No se asignó una persona responsable para la elaboración de directivas o políticas para la definición de un perímetro de seguridad	- Exigir al personal el cumplimiento de los procedimientos establecidos.
		3. El personal no se alinea a trabajar	- Monitorear el cumplimiento de los

		con directivas o políticas	procedimientos de perímetro de seguridad establecidos, por parte del personal de la Línea de Producción de Microformas
		4. No se tiene clara la importancia de un perímetro de seguridad	
		5. Poco interés en la utilización de un perímetro de seguridad	
8	Falta de controles de ingreso físico	1. No hay registros históricos de controles de ingreso físico	- Elaborar controles de ingreso físico para la Línea de Producción de Microformas
		2. No se asignó una persona responsable para la elaboración de los controles de ingreso físico	- Exigir al personal el cumplimiento de los controles de ingreso establecidos
		3. El personal no se alinea a trabajar con controles definidos	- Monitorear el cumplimiento de los controles de ingreso por parte del personal de la Línea de Producción de Microformas
		4. No se tiene clara la importancia de los controles de ingreso físico	
		5. Poco interés en la utilización de controles de ingreso	
9	No existe una verificación o control de los equipos a reutilizar	1. No hay registros históricos de verificaciones realizadas a equipos a reutilizar	- Elaborar una programación de verificaciones para los equipos reutilizables para la Línea de Producción de Microformas
		2. No se asignó una persona responsable para la verificación de equipos a reutilizar	- Exigir al personal encargado, el cumplimiento de las verificaciones programadas.
		3. El personal no se alinea a trabajar con verificaciones programadas	- Monitorear el cumplimiento de las verificaciones programadas por parte del personal de la Línea de Producción de Microformas
		4. No se tiene clara la importancia de la verificación de un equipo reutilizable	
		5. Poco interés en la utilización de verificaciones	
10	No existe una protección adecuada para los equipos	1. No hay registros históricos de implementación de protecciones realizadas a equipos desatendidos	- Elaborar una programación de implementaciones de protección para los equipos desatendidos de la Línea de Producción de Microformas
		2. No se asignó una persona responsable para la implementación	- Exigir al personal encargado, el cumplimiento de las protecciones y medidas de seguridad



	desatendidos	de protecciones	establecidas
		3. El personal no se alinea a trabajar con implementación de protecciones a equipos en desuso.	- Monitorear el cumplimiento de las protecciones a los equipos desatendidos, por parte del personal de la Línea de Producción de Microformas
		4. No se tiene clara la importancia de una protección a los equipos desatendidos	
		5. Poco interés en la utilización de protecciones para los equipos en desuso	
11	Ausencia de restricciones sobre instalación de software	1. No hay registros históricos de restricciones sobre instalación de sw	- Elaborar restricciones para la instalación de sw para la Línea de Producción de Microformas
		2. No se asignó una persona responsable para la elaboración de restricciones sobre instalación de sw	- Exigir al personal el cumplimiento de las restricciones establecidas
		3. El personal no se alinea a trabajar con restricciones de instalaciones	- Monitorear el cumplimiento de las restricciones de instalación de sw por parte del personal de la Línea de Producción de Microformas
		4. No se tiene clara la importancia de las restricciones de instalación	
		5. Poco interés en la utilización de restricciones de instalación de sw	
12	No se cumple con los procedimientos establecidos para la transferencia de información	1. No hay registros de procedimientos establecidos para la transferencia de información	- Elaborar procedimientos para la transferencia de información para la Línea de Producción de Microformas
		2. No se asignó una persona responsable para la elaboración de procedimientos establecidos para la transferencia de información	- Exigir al personal el cumplimiento de los procedimientos establecidos
		3. El personal no se alinea a trabajar con procedimientos establecidos	- Monitorear el cumplimiento de los procedimientos de transferencia de información por parte del personal de la Línea de Producción de Microformas
		4. No se tiene clara la importancia de los procedimientos de transferencia de información	
		5. Poco interés en la utilización de procedimientos de transferencia de información	
13	Sin reporte de	1. No hay registros históricos de reportes de debilidades advertidas	- Elaborar restricciones para la instalación de sw para la Línea de Producción de Microformas



	debilidades advertidas	2. No se asignó una persona responsable del seguimiento de las debilidades advertidas	- Exigir al personal que informen de las debilidades advertidas en la seguridad del sistema
		3. El personal no se alinea a informar las debilidades advertidas	- Monitorear al personal de la Línea de Producción de Microformas que cumplan con advertir debilidades referentes a la seguridad de la información
		4. No se tiene clara la importancia de informar las debilidades advertidas	
		5. Poco interés en informar las debilidades advertidas en la seguridad del sistema	
14	No existe una planificación de continuidad de seguridad de la información	1. No existe una planificación de continuidad de la seguridad de información	- Elaborar la planificación de continuidad de la seguridad de información para la Línea de Producción de Microformas
		2. No se asignó una persona responsable para la elaboración de planificación de continuidad de seguridad de la información	- Exigir al personal el cumplimiento de la planificación establecida.
		3. El personal no se alinea a trabajar con planificaciones programadas	- Monitorear el cumplimiento de la planificación de continuidad de la seguridad de información parte del personal de la Línea de Producción de Microformas
		4. No se tiene clara la importancia de una planificación de continuidad de seguridad de la información	
		5. Poco interés en la planificación de continuidad de seguridad de la información	
15	Carencia de protección de registros	1. No se ha elaborado una implementación de protección de registros	- Elaborar una programación de implementaciones de protección para los registros de la LPM
		2. No se asignó una persona responsable para implementación de controles de los registros	- Tener como guía la NTP ISO/IEC 27001:2014, para la programación de implementaciones de protección
		3. No se les dio la debida importancia a la implementación de controles que aseguren la protección de los registros	- Designar a personal responsable para la implementación de controles de protección para los registros de la LPM.
		4. No existe una iniciativa para la implementación de controles de los registros de la LPM	

		5. No se tiene clara la importancia de la asegurabilidad de los registros	
--	--	---	--

**Nota.** Fuente: Elaborado por el autor

Después de identificar 5 posibles causas para cada riesgo, se pudo analizar todas las causas, analizarlas y desarrollarlas, lo cual nos da una lista de Acciones Correctivas, esto es para adelantarnos al suceso de los riesgos para mitigar el riesgo.

**Tabla 30. Plan de Acciones Correctiva**

PLAN DE ACCIONES CORRECTIVAS			
Nº	Riesgo a controlar	¿Por qué?	Acciones
1	Sin políticas de dispositivos móviles	1. No se ha elaborado una política de dispositivos móviles	- Asignar la urgencia de elaboración y difundir una política de uso de dispositivos móviles
		2. No hay registros históricos de políticas de dispositivos móviles	
		3. El personal no se alinea a trabajar con normas	
		4. No se tiene clara la importancia de las políticas del uso de dispositivos móviles	
		5. Poco interés del uso de políticas de dispositivos móviles	
2	Sin procesos de retorno de activos	1. No hay registros históricos de procesos de retorno de uso de activos	- Asignar la urgencia de elaboración procesos para el retorno de los activos de la Línea de Producción de Microformas
		2. No se asignó una persona responsable para la elaboración de los procesos	
		3. El personal no se alinea a trabajar con procesos definidos	
		4. No se tiene clara la importancia de los procesos de retorno de uso de activos	
		5. Poco interés en la utilización de procesos de retorno de activos	
3	Sin protección a los medios de información	1. No se definió políticas de protección para los medios de información	- Asignar la urgencia de elaboración de una política de protección para los medios de información.
		2. No se asignó una persona responsable para la elaboración de las políticas de protección de medios de información	
		3. El personal no se alinea a trabajar con políticas definidas	
		4. No se tiene clara la importancia de las políticas de protección de medios de información	
		5. Poco interés en la utilización de políticas de control de acceso	
4	Sin control de los accesos de los usuarios	1. No hay registros históricos de políticas de control de acceso	- Asignar la urgencia de elaboración de políticas de control de acceso para la Línea de Producción de Microformas
		2. No se asignó una persona responsable para la elaboración de las políticas de control de acceso	
		3. El personal no se alinea a trabajar con políticas definidas	
		4. No se tiene clara la importancia de las políticas de control de acceso	
		5. Poco interés en la utilización de políticas de control de acceso	



5	Escases de restricciones de acceso a la información	1. No hay registros históricos de políticas de control de acceso	- Asignar la urgencia de elaborar políticas de control de acceso para la Línea de Producción de Microformas
		2. No se asignó una persona responsable para la elaboración de las políticas de control de acceso	
		3. El personal no se alinea a trabajar con políticas definidas	
		4. No se tiene clara la importancia de las políticas de control de acceso	
		5. Poco interés en la utilización de políticas de control de acceso	
6	No existe un procedimiento de ingreso seguro	1. No hay registros de procedimientos establecidos para el ingreso seguro a las sw de la LPM	-Asignar la urgencia de elaboración de procedimientos de ingreso seguro para la Línea de Producción de Microformas
		2. No se asignó una persona responsable para la elaboración de los procedimientos de ingreso seguro	
		3. El personal no se alinea a trabajar con procedimientos definidos	
		4. No se tiene clara la importancia de los procedimientos de ingreso seguro	
		5. Poco interés en la utilización de políticas de ingreso seguro	
7	Falta un perímetro de seguridad física	1. No hay registros históricos de perímetros de seguridad física que se hayan establecido	-Asignar la urgencia de implementación de un perímetro de seguridad física para la Línea de Producción de Microformas
		2. No se asignó una persona responsable para la elaboración de directivas o políticas para la definición de un perímetro de seguridad	
		3. El personal no se alinea a trabajar con directivas o políticas	
		4. No se tiene clara la importancia de un perímetro de seguridad	
		5. Poco interés en la utilización de un perímetro de seguridad	
8	Falta de controles de ingreso físico	1. No hay registros históricos de controles de ingreso físico	- Asignar la urgencia de elaborar controles de ingreso físico para la Línea de Producción de Microformas
		2. No se asignó una persona responsable para la elaboración de los controles de ingreso físico	
		3. El personal no se alinea a trabajar con controles definidos	
		4. No se tiene clara la importancia de los controles de ingreso físico	
		5. Poco interés en la utilización de controles de ingreso	
9	No existe una verificación o control de los equipos a reutilizar	1. No hay registros históricos de verificaciones realizadas a equipos a reutilizar	-Asignar la urgencia de implementación de verificaciones a los equipos de reutilización de la Línea de Producción de Microformas
		2. No se asignó una persona responsable para la verificación de equipos a reutilizar	
		3. El personal no se alinea a trabajar con verificaciones programadas	
		4. No se tiene clara la importancia de la verificación de un equipo reutilizable	
		5. Poco interés en la utilización de verificaciones	
10	No existe una protección adecuada para los equipos desatendidos	1. No hay registros históricos de implementación de protecciones realizadas a equipos desatendidos	-Asignar la urgencia de implementación de protecciones adecuadas para los equipos desatendidos de la Línea de Producción de Microformas
		2. No se asignó una persona responsable para la implementación de protecciones	
		3. El personal no se alinea a trabajar con implementación de	



		protecciones a equipos en desuso.	
		4. No se tiene clara la importancia de una protección a los equipos desatendidos	
		5. Poco interés en la utilización de protecciones para los equipos en desuso	
11	Ausencia de restricciones sobre instalación de software	1. No hay registros históricos de restricciones sobre instalación de sw	- Asignar la urgencia de elaborar restricciones para la instalación de sw para la Línea de Producción de Microformas
		2. No se asignó una persona responsable para la elaboración de restricciones sobre instalación de sw	
		3. El personal no se alinea a trabajar con restricciones de instalaciones	
		4. No se tiene clara la importancia de las restricciones de instalación	
		5. Poco interés en la utilización de restricciones de instalación de sw	
12	No se cumple con los procedimientos establecidos para la transferencia de información	1. No hay registros de procedimientos establecidos para la transferencia de información	- Asignar la urgencia de elaborar procedimientos para la transferencia de información para la Línea de Producción de Microformas
		2. No se asignó una persona responsable para la elaboración de procedimientos establecidos para la transferencia de información	
		3. El personal no se alinea a trabajar con procedimientos establecidos	
		4. No se tiene clara la importancia de los procedimientos de transferencia de información	
		5. Poco interés en la utilización de procedimientos de transferencia de información	
13	Sin reporte de debilidades advertidas	1. No hay registros históricos de reportes de debilidades advertidas	- Asignar la urgencia de elaborar restricciones para la instalación de sw para la Línea de Producción de Microformas
		2. No se asignó una persona responsable del seguimiento de las debilidades advertidas	
		3. El personal no se alinea a informar las debilidades advertidas	
		4. No se tiene clara la importancia de informar las debilidades advertidas	
		5. Poco interés en informar las debilidades advertidas en la seguridad del sistema	
14	No existe una planificación de continuidad de seguridad de la información	1. No existe una planificación de continuidad de la seguridad de información	- Asignar la urgencia de elaborar la planificación de continuidad de la seguridad de información para la Línea de Producción de Microformas
		2. No se asignó una persona responsable para la elaboración de planificación de continuidad de seguridad de la información	
		3. El personal no se alinea a trabajar con planificaciones programadas	
		4. No se tiene clara la importancia de una planificación de continuidad de seguridad de la información	
		5. Poco interés en la planificación de continuidad de seguridad de la información	
15	Carencia de protección de registros	1. No se ha elaborado una implementación de protección de registros	- Asignar la urgencia de elaborar implementaciones de protección para los registros de la LPM
		2. No se asignó una persona responsable para implementación de controles de los registros	
		3. No se les dio la debida importancia a la implementación de controles que aseguren la protección de los registros	
		4. No existe una iniciativa para la implementación de controles de los registros de la LPM	
		5. No se tiene clara la importancia de la asegurabilidad de los registros	

**Nota.** Fuente: Elaborado por el autor



Después de identificar 5 posibles causas para cada riesgo, se pudo analizar todas las causas, analizarlas y desarrollarlas, lo cual nos da una lista de Acciones Correctivas, para corregir en el instante que aparezcan la eliminación de la causa raíz del riesgo.

### **5.7. Salida**

El Manual de Seguridad de la Información para la Línea de Producción de Microformas será la salida del proceso y se desarrollará en base a la metodología vista en los puntos anteriores. (Ver Anexo F)

# **CAPÍTULO VI. CONCLUSIONES Y RECOMENDACIONES**

## 6.1. Conclusiones

1. Se realizó el análisis situacional de la seguridad de la información de la Línea de Producción de Microformas al 100%, considerando la aplicación de la totalidad de controles de la NTP ISO/IEC 27001:2014 en la elaboración de las encuestas, donde cada pregunta se relacionó a un control específico de la norma técnica.
2. Se realizó la selección de los controles de la NTP ISO/IEC 27001:2014 para cada una de las vulnerabilidades encontradas, los controles fueron seleccionados en relación a los indicadores de cada vulnerabilidad.
3. Se llevó a cabo la advertencia de 20 vulnerabilidades de seguridad de la información, cada una relacionada a diferentes controles de seguridad de la NTP ISO/IEC 27001:2014 y se realizó la identificación de 15 vulnerabilidades de gravedad e índice de prioridad de riesgo alto, por lo que se implementó planes de acciones preventivas y correctivas para la mitigación de las mismas.
4. Se realizó la elaboración del Manual de Seguridad de Información que ayudó a la entidad a establecer procedimientos de seguridad para la información y así mejorar la confidencialidad, integridad y disponibilidad de la información, mejoras que se evidencian en la disminución de la gravedad de las vulnerabilidades, esto, como resultado de una posterior aplicación de un plan de verificación de vulnerabilidades.



## 6.2. Recomendaciones

1. Al Departamento de Gestión Documentaria de la Contraloría General de la República, aplicar estrategias para la concientización del personal en temas de seguridad de la información, y velar por el correcto cumplimiento del Manual de Seguridad de la Información, así como la aseguración de la implementación de planes de acciones preventivas y correctivas para el tratamiento de las vulnerabilidades encontradas.
2. A la Contraloría General de la República, asignar un presupuesto para la gestión adecuada de los recursos de seguridad de la información, según lo dispuesto en la NTP ISO/IEC 27001:2014, y considerar la aplicación de los controles de la norma técnica en la seguridad de información de sus demás procesos por departamento.

## REFERENCIAS

- Aguilar, G. & Arboleda, O. (2011). Análisis e Implementación de un sistema automatizado de digitalización de documentos (SADO) para soluciones inteligentes. (Tesis de Título Profesional). Escuela Politécnica del Ejercito, Ecuador.
- Bestratén M. Orriols, R. Y. (2010). Análisis modal de fallos y efectos AMFE. Madrid, España.
- Catoira, F. (2013). Pruebas de penetracion para principiantes: explotando una vulnerabilidad con Metasploit FrameworkLockpicking. *Seguridad Cultura de prevencion para TI*, 36.
- Cavalcanti, A. (2012). Sistema para el Análisis y Gestión de Riesgos. (Tesis de Título Profesional). Universidad Ricardo Palma, Perú.
- Días, C. (2014). Hacking ético y Seguridad en Red.
- ESAN. (20 de Abril de 2013). Control de Calidad, Limites de control. Diplomado Six Sigma. Lima, Perú.
- Giménez Solano, V. M. (s.f.). *Hacking y Cibercriminología*. Valencia.
- Gómez Santiago , M. A., Venegas Tamayo, C. D., & Yáñez Hernández, V. (2014). HERRAMIENTAS PARA HACKING ÉTICO.
- Graves, K. (2010). Certified Ethical Hacker Review Guide. Sybex.
- Guerreo, E. et al (2015) Identificación de vulnerabilidades de seguridad en el control de acceso al Sistema de Gestión Documental, mediante pruebas de testeo de red en la empresa INGELEC S.A.S. (Tesis de Título Profesional). Universidad nacional abierta y a distancia UNAD, Colombia.
- MINSA. (2012). ANÁLISIS MODAL DE SUS FALLAS Y SUS EFECTOS AMFE.  
Recuperado de  
<http://www.minsa.gob.pe/dgsp/observatorio/documentos/herramientas/AMFE.pdf>

- Moreno, F. (2009). La ISO/IEC 27005 en la búsqueda de información más segura. Normas y Calidad. ICONTEC (Cuarta edición ed.), Colombia.
- ONGEI (2014). Aprobacion NTP ISO IEC 27001 2014. Recuperado de <http://www.ongei.gob.pe/docs/Aprobacion%20NTP%20ISO%20IEC%2027001%202014.pdf/>
- ONGEI (2014). Taller Gestión de un proyecto para la implementación de un Sistema de Gestión de Seguridad de la Información. Recuperado de [http://www.ongei.gob.pe/docs/ISO\\_27001\\_2013.pdf/](http://www.ongei.gob.pe/docs/ISO_27001_2013.pdf/)
- Ortiz, B. (15 de Mayo de 2016). Todos somos vulnerables a los ciberataques. Recuperado de <http://elcomercio.pe/tecnologia/actualidad/todos-somos-vulnerables-ciberataques-noticia-1901650>
- Perez, D. (21 de Julio de 2016). Crecen las amenazas en AutoIt: propagación de Houdrat en Latinoamérica. Recuperado de <http://www.welivesecurity.com/la-es/2016/07/21/amenazas-en-autoit-houdrat>
- Poveda, M. (2011). Gestión y tratamiento de los riesgos. Recuperado de <http://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-9.pdf>
- Ríos, J. (2014) Técnicas y herramientas de análisis de vulnerabilidades de una red. (Tesis de Título Profesional). Escuela Técnica Superior de Ingeniería y Sistemas de Telecomunicación, España.
- Salazar Carpio, K. E. (2013). Revistas Bolivianas Electronicas. La Paz, La Paz, Bolivia.
- SSL247. (2016). SSL247 THE WEB SECURITY CONSULTANTIS. Recuperado de <https://www.ssl247.es/analisis-penetracion/>
- Tola, D. (2015). Implementación de un sistema de gestión de seguridad de la información para una empresa de consultoría y auditoría, aplicando la norma ISO/IEC 27001. (Tesis de Título Profesional). Escuela Superior Politécnica del Litoral ESPOL, Ecuador
- Tori, C. (2008). *Hacking Ético*. Rosario: Mastroianni Impresiones.

Urbina, C. (2012). Certificación para la digitalización de documentos en Chile. (Tesis de Título Profesional). Universidad de Chile, Chile.

# ANEXOS



## Anexo 01. Carta para permiso de investigación

**CARGO**

Huaraz, 10 de Abril de 2017

**CARTA N° 001-2017/ADRM**

Dra. Sonia Nakao Honma  
Gerente del Dpto. de Gestión Documentaria - CGR  
Lima – Perú.-


**ASUNTO:** Permiso para investigación de proyecto de fin de carrera.

Es grato dirigirme a usted para expresarle mi cordial saludo, y a la vez presentarme como estudiante del 10mo ciclo de la carrera profesional de Ingeniería de Sistemas de la Universidad Señor de Sipán, con código universitario 2061406373 e identificado con DNI: 45746806, y que como parte del desarrollo de experiencias curriculares en mi formación profesional, solicito se me autorice el debido permiso para la realización de la investigación de mi Proyecto de Tesis en el Dpto. de Gestión Documentaria de la Contraloría General de la República, y tener acceso a las instalaciones con fines de obtener informaciones que me permitan desarrollar el proyecto de fin de carrera.

Dado que el Dpto. de Gestión Documentaria de la Contraloría General de la República es un área en la que se ha implementado diferentes procesos y uno de ellos es la línea de producción de microformas, basados en estándares internacionales, el suscrito completará su Proyecto de grado sobre el tema de investigación relacionado a: **Estudio para detectar vulnerabilidades en la seguridad del software de la línea de producción de microformas basado en la NTP ISO/IEC 27001:2014**, cuyo estudio contribuirá e impactará en su departamento de manera positiva.

En espera de su atención a la presente, aprovecho la oportunidad para reiterarle mi consideración y estimad personal.

Atentamente,

  
Armando Demetrio Romero Mas  
DNI: 45746806



LA CONTRALORIA GENERAL  
DE LA REPUBLICA  
EXPEDIENTE : 09-2017-00744  
10/04/2017 18:33 HURENO  
CLAVE : 11E300 H01RS : 1


LA CONTRALORIA GENERAL DE LA REPUBLICA  
CONTRALORIA REGIONAL HUANUCO  
10 / 04 / 2017  
LA RECEPCION DEL DOCUMENTO NO IMPIDE  
LA CONTINUACION DE LOS TRABAJOS

**Figura 53.** Carta de permiso de investigación

**Fuente:** Elaborado por el autor

## Anexo 02. Oficio N° 00056-2017-CG/D320 de respuesta a solicitud



LA CONTRALORIA  
GENERAL DE LA REPUBLICA

**OFICIO N° 00056-2017-CG/D320** Lima, 11 de Abril de 2017

Señor  
**Armando Demetrio Romero Mas**  
Jr. Alejandro Tafur N° 387 – Urb. Huarupampa  
Huaraz/ Huaraz/ Ancash

**ASUNTO** : Aceptación de Permiso para proyecto de investigación  
**REF.** : CARTA N° 001-2017/ADRM



---

Me dirijo a usted en el marco de la referencia, con la finalidad de hacer de su conocimiento que se encuentra autorizado para la realización de su investigación, con lo que respecta el tema propuesto **Estudio para detectar vulnerabilidades en la seguridad del software de la línea de producción de microformas basado en la NTP ISO/IEC 27001:2014**, agradeceré comunicarse con el Ing. Julio Gamarra Guzmán al número (01) 330-3000 anexo 2018, con la finalidad de coordinar previamente sus visitas a la institución y poder brindarle las facilidades del caso.

Es propicia la oportunidad para expresarle las seguridades de mi consideración.

Atentamente,

*Recibido  
11/04/2017  
MR. DEM. U. S. V. 2017  
/100*

**Sonia Nakao Honma**  
Gerente (e)  
Dpto. de Gestión Documentaria

Oficio N° 00056-2017-CG/D320 1 / 1

"Decenio de las Personas con Discapacidad en el Perú"  
"Año del Buen Servicio al Ciudadano"

**Figura 54.** Oficio N° 00056-2017-CG/D320 – Respuesta de solicitud

**Fuente:** Elaborado por el autor

### Anexo 03. La NTP ISO/IEC 27001:2014 – Objetivos de Control y Controles de Referencia

Tabla 31. Objetivos de control y controles

<b>A.5 Políticas de seguridad de la información</b>		
<b>A.5.1 Dirección de la gerencia para la seguridad de la información</b>		
Objetivo: Proporcionar dirección y apoyo de la gerencia para la seguridad de la información en concordancia con los requisitos del negocio y las leyes y regulaciones relevantes.		
A.5.1.1	Políticas para la seguridad de la información	<i>Control</i> Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la gerencia, publicado y comunicado a los empleados y a las partes externas relevantes.
A.5.1.2	Revisión de las políticas para la seguridad de la información	<i>Control</i> Las políticas para la seguridad de la información deben ser revisadas a intervalos planificados o si ocurren cambios significativos para asegurar su conveniencia, adecuación y efectividad continúa.
<b>A.6 Organización de la seguridad de la información</b>		
<b>A.6.1 Organización interna</b>		
Objetivo: establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.		
A.6.1.1	Roles y responsabilidades para la seguridad de la información	<i>Control</i> Todas las responsabilidades de seguridad de la información deben ser definidas y asignadas.
A.6.1.2	Segregación de funciones	<i>Control</i> Las funciones y áreas de responsabilidad en conflicto deben ser segregadas para reducir oportunidades de modificación no autorizada o no intencional o mal uso de los activos de la organización.
A.6.1.3	Contacto con autoridades	<i>Control</i> Contactos apropiados con autoridades relevantes deben ser mantenidos.

A.6.1.4	Contacto con grupos especiales de interés	<i>Control</i> Contactos apropiados con grupos especiales de interés u otros foros de especialistas en seguridad y asociaciones profesionales deben ser mantenidos.
A.6.1.5	Seguridad de la información en la gestión de proyectos	<i>Control</i> La seguridad de la información debe ser tratada en la gestión de proyectos, sin importar el tipo de proyecto.
<b>A.6.2 Dispositivos móviles y teletrabajo</b>		
Objetivo: Asegurar la seguridad del teletrabajo y el uso de los dispositivos móviles.		
A.6.2.1	Política móviles de dispositivos	<i>Control</i> Una política y medidas de seguridad de soporte deben ser adoptadas para gestionar los riesgos introducidos por el uso de dispositivos móviles.
A.6.2.2	Teletrabajo	<i>Control</i> Una política y medidas de seguridad de apoyo deben ser implementadas para proteger información a la que se accede, se procesa o almacena en sitios de teletrabajo.
<b>A.7 Seguridad de los recursos humanos</b>		
<b>A.7.1 Antes del empleo</b>		
Objetivo: Asegurar que los empleados y contratistas entienden sus responsabilidades y son convenientes para los roles para los que se les considera.		
A.7.1.1	Selección	<i>Control</i> Las verificaciones de los antecedentes de todos los candidatos a ser empleados deben ser llevadas a cabo en concordancia con las leyes, regulaciones y ética relevantes, y debe ser proporcional a los requisitos del negocio, la clasificación de la información a la que se tendrá acceso y los riesgos percibidos.
A.7.1.2	Términos y condiciones del empleo	<i>Control</i> Los acuerdos contractuales con los empleados y contratistas deben estipular responsabilidades de éstos y de la organización respecto de la seguridad de la información.
<b>A.7.2 Durante el empleo</b>		
Objetivo: Asegurar que los empleados y contratistas sean conscientes y cumplan con sus responsabilidades de seguridad de la información.		
A.7.2.1	Responsabilidades de la gerencia	<i>Control</i> La gerencia debe requerir a todos los empleados y contratistas aplicar la seguridad de la información en concordancia con las políticas y procedimientos establecidos por la organización.



A.7.2.2	Conciencia, educación y capacitación sobre la seguridad de la información	<i>Control</i> Todos los empleados de la organización y, cuando fuera relevante, los contratistas deben recibir educación y capacitación sobre la conciencia de la seguridad de la información, así como actualizaciones regulares sobre políticas y procedimientos de la organización, según sea relevante para la función del trabajo que cumplen.
A.7.2.3	Proceso disciplinario	<i>Control</i> Debe haber un proceso disciplinario formal y comunicado para tomar acción contra empleados que hayan cometido una infracción a la seguridad de la información.
<b>A.7.3 Terminación y cambio de empleo</b>		
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.		
A.7.3.1	Terminación o cambio de responsabilidades del empleo.	<i>Control</i> Las responsabilidades y deberes de seguridad de la información que siguen siendo válidos luego de la terminación o cambio de empleo deben ser definidos, comunicados al empleado o contratista y forzar su cumplimiento.
<b>A.8 Gestión de activos</b>		
<b>A.8.1 Responsabilidad por los activos</b>		
Objetivo: Identificar los activos de la organización y definir responsabilidades de protección apropiadas.		
A.8.1.1	Inventario de activos	<i>Control</i> Información, Otros activos asociados con información e instalaciones de procesamiento de información deben ser identificados y un inventario de estos activos debe ser elaborado y mantenido.
A.8.1.2	Propiedad de los activos	<i>Control</i> Los activos mantenidos en el inventario deben ser propios.
A.8.1.3	Uso aceptable de los activos	<i>Control</i> Las reglas para el uso aceptable de la información y activos asociados con la información y con las instalaciones de procesamiento de la información deben ser





A.8.1.4	Retorno de activos	<i>Control</i> Todos los empleados y usuarios de partes externas deben retornar todos los activos de la organización en su posesión a la conclusión de su empleo, contrato o acuerdo.
---------	--------------------	--

#### A.8.2 Clasificación de la información

Objetivo: Asegurar que la información recibe un nivel apropiado de protección en concordancia con su importancia para la organización.

A.8.2.1	Clasificación de la información	<i>Control</i> La información debe ser clasificada en términos de los requisitos legales, valor, criticidad y sensibilidad respecto a una divulgación o modificación no autorizada.
A.8.2.2	Etiquetado de la información	<i>Control</i> Un conjunto apropiado de procedimientos para el etiquetado de la información debe ser desarrollado e implementado en concordancia con el esquema de clasificación de la información adoptado por la organización.
A.8.2.3	Manejo de activos	<i>Control</i> Los procedimientos para el manejo de activos deben ser desarrollados e implementados en concordancia con el esquema de clasificación de la información adoptado por la organización.

#### A.8.3 Manejo de los medios

Objetivo: Prevenir la divulgación, modificación, remoción o destrucción no autorizada de información almacenada en medios.

A.8.3.1	Gestión de medios removibles	<i>Control</i> Se debe implementar procedimientos para la gestión de medios removibles en concordancia con el esquema de clasificación adoptado por la organización.
---------	------------------------------	---

A.8.3.2	Disposición de medios	<i>Control</i> Se debe poner a disposición los medios de manera segura cuando ya no se requieran, utilizando procedimientos formales.
A.8.3.3	Transferencia de medios físicos	<i>Control</i> Los medios que contienen información deben ser protegidos contra el acceso no autorizado, el mal uso o la corrupción durante el transporte.

#### A.9 Control de acceso

##### A.9.1 Requisitos de la empresa para el control de acceso



Objetivo: Limitar el acceso a la información y a las instalaciones de procesamiento de la información.

A.9.1.1	Política de control de acceso	<i>Control</i> Una política de control de acceso debe ser establecida, documentada y revisada basada en requisitos del negocio y de seguridad de la información.
A.9.1.2	Acceso a redes y servicios de red	<i>Control</i> Los usuarios deben tener acceso solamente a la red y a servicios de red que hayan sido específicamente autorizados a usar.
<b>A.9.2 Gestión de acceso de usuario</b>		
Objetivo: Asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas y servicios.		
A.9.2.1	Registro y baja de usuarios	<i>Control</i> Un proceso formal de registro y baja de usuarios debe ser implementado para permitir la asignación de derechos de acceso.
A.9.2.2	Aprovisionamiento de acceso a usuario	<i>Control</i> Un proceso formal de aprovisionamiento de acceso a usuarios debe ser implementado para asignar o revocar los derechos de acceso para todos los tipos de usuarios a todos los sistemas y servicios.
A.9.2.3	Gestión de derechos de acceso privilegiados	<i>Control</i> La asignación y uso de derechos de acceso privilegiado debe ser restringida y controlada.
A.9.2.4	Gestión de información de autenticación secreta de usuarios	<i>Control</i> La asignación de información de autenticación secreta debe ser controlada a través de un proceso de gestión formal.



A.9.2.5	Revisión de derechos acceso de usuarios	de	<i>Control</i> Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares.
A.9.2.6	Remoción o ajuste derechos de acceso	de	<i>Control</i> Los derechos de acceso a información e instalaciones de procesamientos de información de todos los empleados y de los usuarios de partes externas deben removerse al término de su empleo, contrato o acuerdo, o ajustarse según el cambio.
<b>A.9.3 Responsabilidades de los usuarios</b>			
Objetivo: Hacer que los usuarios respondan por la salvaguarda de su información de autenticación.			

A.9.3.1	Uso de información autenticación secreta	de	<i>Control</i> Los usuarios deben ser exigidos a que sigan las prácticas de la organización en el uso de información de autenticación secreta.
<b>A.9.4 Control de acceso a sistema y aplicación</b>			
Objetivo: Prevenir el acceso no autorizado a los sistemas y aplicaciones.			
A.9.4.1	Restricción de acceso a la información		<i>Control</i> El acceso a la información y a las funciones del sistema de aplicación debe ser restringido en concordancia con la política de control de acceso.
A.9.4.2	Procedimientos de ingreso seguro		<i>Control</i> Donde la política de control de acceso lo requiera, el acceso a los sistemas y a las aplicaciones debe ser controlado por un procedimiento de ingreso seguro.
A.9.4.3	Sistema de gestión de contraseñas		<i>Control</i> Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.
A.9.4.4	Uso de programas utilitarios privilegiados		<i>Control</i> El uso de programas utilitarios que podrían ser capaces de pasar por alto los controles del sistema y de las aplicaciones debe ser restringido y controlarse estrictamente.
A.9.4.5	Control de acceso al código fuente de los programas		<i>Control</i> El acceso al código fuente de los programas debe ser restringido.



<b>A.10 Criptografía</b>		
<b>A.10.1 Controles criptográficos</b>		
Objetivo: Asegurar el uso apropiado y efectivo de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.		
A.10.1.1	Política sobre el uso de controles criptográficos	<i>Control</i> Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada.
A.10.1.2	Gestión de claves	<i>Control</i> Una política sobre el uso, protección y tiempo de vida de las claves criptográficas debe ser desarrollada e implementada a través de todo su ciclo de vida.
<b>A.11 Seguridad física y ambiental</b>		
<b>A.11.1 Áreas seguras</b>		

Objetivo: Impedir acceso físico no autorizado, daño e interferencia a la información y a las instalaciones de procesamiento de la información de la organización.		
A.11.1.1	Perímetro de seguridad física	<i>Control</i> Perímetros de seguridad deben ser definidos y utilizados para proteger áreas que contienen información sensible o crítica e instalaciones de procesamiento de la información.
A.11.1.2	Controles de ingreso físico	<i>Control</i> Las áreas seguras deben ser protegidas por medio de controles apropiados de ingreso para asegurar que se le permite el acceso sólo al personal autorizado.
A.11.1.3	Asegurar oficinas, áreas e instalaciones	<i>Control</i> Seguridad física para oficinas, áreas e instalaciones debe ser diseñada e implementada.
A.11.1.4	Protección contra amenazas externas y ambientales	<i>Control</i> Protección física contra desastres naturales, ataque malicioso o accidentes debe ser diseñada y aplicada.
A.11.1.5	Trabajo en áreas seguras	<i>Control</i> Procedimientos para el trabajo en áreas seguras debe ser diseñado y aplicado.





A.11.1.6	Áreas de despacho y carga	<i>Control</i> Los puntos de acceso, como las áreas de despacho, carga y otros puntos en donde personas no autorizadas pueden ingresar al local deben ser controlados, y si fuera posible, aislarlos de las instalaciones de procesamiento de la información para evitar el acceso no autorizado.
<b>A.11.2 Equipos</b>		
Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos e interrupción de las operaciones de la organización.		
A.11.2.1	Emplazamiento y protección de los equipos	<i>Control</i> Los equipos deben ser ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado.
A.11.2.2	Servicios de suministro	<i>Control</i> Los equipos deben ser protegidos contra fallas de electricidad y otras alteraciones causadas por fallas en los servicios de suministro.
A.11.2.3	Seguridad del cableado	<i>Control</i> El cableado de energía y telecomunicaciones que llevan datos o servicios de información de soporte debe ser protegido de la interceptación, interferencia o daño.
A.11.2.4	Mantenimiento de equipos	<i>Control</i> Los equipos deben mantenerse de manera correcta para asegurar su continua disponibilidad e integridad.
A.11.2.5	Remoción de activos	<i>Control</i> Los equipos, la información o el software no deben ser retirados de su lugar sin autorización previa.
A.11.2.6	Seguridad de equipos activos fuera de las instalaciones	<i>Control</i> La seguridad debe ser aplicada a los activos que están fuera de su lugar tomando en cuenta los distintos riesgos de trabajar fuera de las instalaciones de la organización.



A.11.2.7	Disposición o reutilización segura de equipos	<i>Control</i> Todos los elementos del equipo que contengan medios de almacenamiento deben ser verificados para asegurar que cualquier dato sensible y software con licencia se haya eliminado o se haya sobre escrito de manera segura antes de su disposición o reutilización.
A.11.2.8	Equipos de usuario desatendidos	<i>Control</i> Los usuarios deben asegurarse de que el equipo desatendido tenga la protección apropiada.
A.11.2.9	Política de escritorio limpio y pantalla limpia	<i>Control</i> Una política de escritorio limpio de papeles y de medios de almacenamiento removibles, así como una política de pantalla limpia para las instalaciones de procesamiento de la información debe ser adoptada.

<b>A.12 Seguridad de las operaciones</b>		
<b>A.12.1 Procedimientos y responsabilidades operativas</b>		
Objetivo: Asegurar que las operaciones de instalaciones de procesamiento de la información sean correctas y seguras.		
A.12.1.1	Procedimientos operativos documentados	<i>Control</i> Los procedimientos operativos deben ser documentados y puestos a disposición de todos los usuarios que los necesitan.
A.12.1.2	Gestión del cambio	<i>Control</i> Los cambios en la organización, procesos de negocio, instalaciones de procesamiento de la información y sistemas que afecten la seguridad de la información deben ser controlados.
A.12.1.3	Gestión de la capacidad	<i>Control</i> El uso de recursos debe ser monitoreado, afinado y se debe hacer proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido del sistema.
A.12.1.4	Separación de los entornos de desarrollo, pruebas y operaciones	<i>Control</i> Los entornos de desarrollo, pruebas y operaciones deben ser separados para reducir los riesgos de acceso no autorizado o cambios al entorno operativo.

<b>A.12.2 Protección contra códigos maliciosos</b>		
Objetivo: Asegurar que la información y las instalaciones de procesamiento de la información estén protegidas contra códigos maliciosos.		
A.12.2.1	Controles contra códigos maliciosos	<i>Control</i> Controles de detección, prevención y recuperación para proteger contra códigos maliciosos deben ser implementados, en combinación con una concientización apropiada de los usuarios.
<b>A.12.3 Respaldo</b>		
Objetivo: Proteger contra la pérdida de datos		
A.12.3.1	Respaldo de la información	<i>Control</i> Copias de respaldo de la información, del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada.
<b>A.12.4 Registros y monitoreo</b>		
Objetivo: Registrar eventos y generar evidencia		
Objetivo: Registrar eventos y generar evidencia		
A.12.4.1	Registro de eventos	<i>Control</i> Registros (logs) de eventos de actividades de usuarios, excepciones, fallas y eventos de seguridad de la información deben ser producidos, mantenidos y regularmente revisados.
A.12.4.2	Protección de información de registros.	<i>Control</i> Las instalaciones para registros (logs) y la información de los registros (logs) deben ser protegidas contra la adulteración y el acceso no autorizado.
A.12.4.3	Registros del administrador y del operador	<i>Control</i> Las actividades del administrador del sistema y del operador del sistema deben ser registradas y los registros (logs) deben ser protegidos y revisados regularmente.
A.12.4.4	Sincronización de reloj	<i>Control</i> Los relojes de todos los sistemas de procesamiento de la información relevantes dentro de una organización o dominio de seguridad deben estar sincronizados a una fuente de tiempo de referencia única.



<b>A.12.6 Gestión de vulnerabilidad técnica</b>		
Objetivo: Prevenir la explotación de vulnerabilidades técnicas		
A.12.6.1	Gestión de vulnerabilidades técnicas	<i>Control</i> Información sobre vulnerabilidades técnicas de los sistemas de información utilizados debe ser obtenida de manera oportuna, la exposición de la organización a dichas vulnerabilidades debe ser evaluada y las medidas apropiadas deben ser tomadas para resolver el riesgo asociado.
A.12.6.2	Restricciones sobre la instalación de software	<i>Control</i> Reglas que gobiernen la instalación de software por parte de los usuarios deben ser establecidas e implementadas.
<b>A.12.7 Consideraciones para la auditoría de los sistemas de información</b>		
Objetivo: Minimizar el impacto de las actividades de auditoría en los sistemas		
A.12.7.1	Controles de auditoría de sistemas de información	<i>Control</i> Requisitos de las auditorías y las actividades que involucran la verificación de sistemas operacionales deben ser cuidadosamente planificados y acordados para minimizar la interrupción a los procesos del negocio.
<b>A.13 Seguridad de las comunicaciones</b>		
<b>A.13.1 Gestión de seguridad de la red</b>		
Objetivo: Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de la información de apoyo.		
A.13.1.1	Controles de la red	<i>Control</i> Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y las aplicaciones.
A.13.1.2	Seguridad de servicios de red	<i>Control</i> Mecanismos de seguridad, niveles de servicio y requisitos de gestión de todos los servicios de red deben ser identificados e incluidos en acuerdos de servicios de red, ya sea que estos servicios se provean internamente o sean terciarizado.
A.13.1.3	Segregación en redes	<i>Control</i> Grupos de servicios de información, usuarios y sistemas de información deben ser segregados en redes.
<b>A.13.2 Transferencia de información</b>		
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.		



A.13.2.1	Políticas y procedimientos de transferencia de la información	<i>Control</i> Políticas, procedimientos y controles de transferencia formales deben aplicarse para proteger la transferencia de información a través del uso de todo tipo de instalaciones de comunicación.
A.13.2.2	Acuerdo sobre transferencia de información	<i>Control</i> Los acuerdos deben dirigir la transferencia segura de información del negocio entre la organización y partes externas.
A.13.2.3	Mensajes electrónicos	<i>Control</i> La información involucrada en mensajería electrónica debe ser protegida apropiadamente.
A.13.2.4	Acuerdos de confidencialidad o no divulgación	<i>Control</i> Requisitos para los acuerdos de confidencialidad o no divulgación que reflejan las necesidades de la organización para la protección de la información deben ser identificados, revisados regularmente y documentados.
<b>A.14 Adquisición, desarrollo y mantenimiento de sistemas</b>		
<b>A.14.1 Requisitos de seguridad de los sistemas de información</b>		
Objetivo: Garantizar que la seguridad de la información es una parte integral de los sistemas de información a través del ciclo de vida completo. Esto también incluye los requisitos para sistemas de información que proporcionen servicios sobre redes públicas.		
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	<i>Control</i> Requisitos relacionados a la seguridad de la información deben ser incluidos dentro de los requisitos para nuevos sistemas de información o mejoras a los sistemas de información existentes.
A.14.1.2	Aseguramiento de servicios de aplicaciones sobre redes públicas	<i>Control</i> La información involucrada en servicios de aplicaciones que pasa sobre redes públicas debe ser protegida de actividad fraudulenta, disputa de contratos o divulgación no autorizada y modificación.



A.14.1.3	Protección de transacciones en servicios de aplicación	<i>Control</i> La información involucrada en las transacciones de servicios de aplicación debe ser protegida para prevenir transmisión incompleta, ruteo incorrecto, alteración no autorizada de mensajes, divulgación no autorizada, duplicación o respuesta no autorizada de mensajes.
<b>A.14.2 Seguridad en los procesos de desarrollo y soporte</b>		
Objetivo: Garantizar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.		
A.14.2.1	Política de desarrollo seguro	<i>Control</i> Reglas para el desarrollo de software y sistemas deben ser establecidas y aplicadas a desarrollos dentro de la organización.
A.14.2.2	Procedimientos de control de cambio del sistema	<i>Control</i> Cambios a los sistemas dentro del ciclo de vida del desarrollo deben ser controlados por medio del uso de procedimientos formales de control de cambios.
A.14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa	<i>Control</i> Cuando se cambian las plataformas operativas, las aplicaciones críticas para el negocio deben ser revisadas y probadas para asegurar que no haya impacto adverso en las operaciones o en la seguridad de la organización.
A.14.2.4	Restricciones sobre cambios a los paquetes de software	<i>Control</i> Modificaciones a los paquetes de software deben ser disuadidas, limitadas a los cambios necesarios y todos los cambios deben ser estrictamente controlados.
A.14.2.5	Principios de ingeniería de sistemas seguros	<i>Control</i> Principios para la ingeniería de sistemas seguros deben ser establecidos, documentados, mantenidos y aplicados a cualquier esfuerzo de implementación de sistemas de información.
A.14.2.6	Ambiente de desarrollo seguro	<i>Control</i> Las organizaciones deben establecer y proteger apropiadamente los ambientes de desarrollo seguros para los esfuerzos de desarrollo e integración de sistemas que cubren todo el ciclo de vida del desarrollo del sistema.
A.14.2.7	Desarrollo contrata do externamente	<i>Control</i> La organización debe supervisar y monitorear la actividad de desarrollo de sistemas contratado externamente.





A.14.2.9	Pruebas de aceptación del sistema	<i>Control</i> Programas de pruebas de aceptación y criterios relacionados deben ser establecidos para nuevos sistemas de información, actualizaciones y nuevas versiones.
<b>A.14.3 Datos de prueba</b>		
Objetivo: Asegurar la protección de datos utilizados para las pruebas		
A.14.3.1	Protección de datos de prueba	<i>Control</i> Los datos de prueba deben ser seleccionados cuidadosamente, protegidos y controlados.
<b>A.15 Relaciones con los proveedores</b>		
<b>A.15.1 Seguridad de la información en las relaciones con los proveedores</b>		
Objetivo: Asegurar protección a los activos de la organización que son accesibles por los proveedores		
A.15.1.1	Política de seguridad de la información para las relaciones con los proveedores	<i>Control</i> Requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso por parte del proveedor a los activos de la organización deben ser acordados con el proveedor y documentados.
A.15.1.2	Abordar la seguridad dentro de los acuerdos con proveedores	<i>Control</i> Todos los requisitos relevantes de seguridad de la información deben ser establecidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar, o proveer componentes de infraestructura de TI para la información de la organización.
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	<i>Control</i> Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.
<b>A.15.2 Gestión de entrega de servicios del proveedor</b>		
Objetivo: Mantener un nivel de seguridad de la información y entrega de servicios acordado en línea con los acuerdos con proveedores.		
A.15.2.1	Monitoreo y revisión de servicios de los proveedores	<i>Control</i> Las organizaciones deben monitorear, revisar y auditar regularmente la entrega de servicios por parte de los proveedores.

A.15.2.2	Gestión de cambios a los servicios de proveedores	<i>Control</i> Los cambios a la provisión de servicios por parte de proveedores, incluyendo el mantenimiento y mejoramiento de políticas, procedimientos y controles existentes de seguridad de la información deben ser gestionados tomando en cuenta la criticidad de la información del negocio, sistemas y procesos involucrados y una reevaluación de riesgos.
----------	---	--

**A.16 Gestión de incidentes de seguridad de la información**

**A.16.1 Gestión de incidentes de seguridad de la información y mejoras**

Objetivo: Asegurar un enfoque consistente y efectivo a la gestión de incidentes de seguridad de la información, incluyendo la comunicación sobre eventos de seguridad y debilidades.

A.16.1.1	Responsabilidades y procedimientos	<i>Control</i> Las responsabilidades de gestión y los procedimientos deben ser establecidos para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.
A.16.1.2	Reporte de eventos de seguridad de la información	<i>Control</i> Los eventos de seguridad de la información deben ser reportados a través de canales de gestión apropiados tan rápido como sea posible.
A.16.1.3	Reporte de debilidades de seguridad de la información	<i>Control</i> Empleados y contratistas que usan los sistemas y servicios de información de la organización deben ser exigidos a advertir y reportar cualquier debilidad observada o de la que se sospecha en cuanto a seguridad de la información en los sistemas o servicios.
A.16.1.4	Evaluación y decisión sobre eventos de seguridad de la información	<i>Control</i> Los eventos de seguridad de la información deben ser evaluados y debe decidirse si son clasificados como incidentes de seguridad de la información.
A.16.1.5	Respuesta a incidentes de seguridad de la información	<i>Control</i> Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	<i>Control</i> El conocimiento adquirido a partir de analizar y resolver los incidentes de seguridad de la información debe ser utilizado para reducir la probabilidad o el impacto de incidentes futuros.



A.16.1.7	Recolección de evidencia	<i>Control</i> La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
<b>A.17 Aspectos de seguridad de la información en la gestión de continuidad del</b>		
<b>A.17.1 Continuidad de seguridad de la información</b>		
Objetivo: La continuidad de seguridad de la información debe estar embebida en los sistemas de gestión de continuidad del negocio de la organización		
A.17.1.1	Planificación de continuidad de seguridad de la información	<i>Control</i> La organización debe determinar sus requisitos de seguridad de la información y continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo durante una crisis o desastre.
A.17.1.2	Implementación de continuidad de seguridad de la información	<i>Control</i> La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de seguridad de la información durante una situación adversa.
A.17.1.3	Verificación, revisión y evaluación de continuidad de seguridad de la información	<i>Control</i> La organización debe verificar los controles de continuidad de seguridad de la información que han establecido e implementado a intervalos regulares para asegurarse que son válidos y efectivos durante situaciones adversas.
<b>A.17.2 Redundancias</b>		
Objetivo: Asegurar la disponibilidad de las instalaciones y procesamiento de la información		
A.17.2.1	Instalaciones de procesamiento de información	<i>Control</i> Las instalaciones de procesamiento de la información deben ser implementadas con redundancia suficiente para cumplir con los requisitos de disponibilidad.
<b>A.18 Cumplimiento</b>		
<b>A.18.1 Cumplimiento con requisitos legales y contractuales</b>		
Objetivo: Evitar infracciones de las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas a la seguridad de la información y a cualquier requisito de seguridad.		





A.18.1.1	Identificación de requisitos contractuales y de legislación aplicables	<i>Control</i> Todos los requisitos legislativos, estatutarios, regulatorios y contractuales relevantes así como el enfoque de la organización para cumplir con estos requisitos deben ser explícitamente identificados, documentados y mantenidos al día para cada sistema de información y para
A.18.1.2	Derechos de propiedad intelectual	<i>Control</i> Procedimientos apropiados deben ser implementados para asegurar el cumplimiento de requisitos legislativos, regulatorios y contractuales relacionados a los derechos de propiedad intelectual y uso de productos de software propietario.
A.18.1.3	Protección de registros	<i>Control</i> Los registros deben ser protegidos de cualquier pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, de acuerdo con los requisitos legislativos, regulatorios, contractuales y del negocio.
A.18.1.4	Privacidad y protección de datos personales.	<i>Control</i> La privacidad y la protección de datos personales deben ser aseguradas tal como se requiere en la legislación y regulación relevantes donde sea aplicable.
A.18.1.5	Regulación de controles criptográficos	<i>Control</i> Controles criptográficos deben ser utilizados en cumplimiento con todos los acuerdos, legislación y regulación relevantes.
<b>A.18.2 Revisiones de seguridad de la información</b>		
Objetivo: Asegurar que la seguridad de la información está implementada y es operada de acuerdo con las políticas y procedimientos organizativos.		
A.18.2.1	Revisión independiente de la seguridad de la información	<i>Control</i> El enfoque de la organización para manejar la seguridad de la información y su implementación (por ejemplo objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) debe ser revisado independientemente a intervalos planeados o cuando ocurran cambios significativos.



A.18.2.2	Cumplimiento de políticas y normas de seguridad	<i>Control</i> Los gerentes deben revisar regularmente el cumplimiento del procesamiento de la información y de los procedimientos dentro de su área de responsabilidad con las políticas, normas y otros requisitos de seguridad apropiados.
A.18.2.3	Revisión del cumplimiento técnico	<i>Control</i> Los sistemas de información deben ser revisados regularmente respecto al cumplimiento de las políticas y normas de seguridad de la información de la organización.





## Anexo 04. Encuesta aplicada a personal de la Línea de Producción de Microformas

**ENCUESTA DE INVESTIGACIÓN**

Apellidos y Nombres :.....

Cargo :..... Ámbito:..... Área :.....

1. Respecto a las Políticas de Seguridad implementadas en la LPM, marque con una "X" la opción que Ud. crea conveniente en cada una de las premisas.

	SI	NO
1.1 ¿Se ha implementado Políticas de Seguridad?	<input type="checkbox"/>	<input type="checkbox"/>
1.2 ¿Se ha implementado revisiones periódicas de las Políticas de Seguridad?	<input type="checkbox"/>	<input type="checkbox"/>

2. Respecto a la Organización de la Seguridad de la Información en la LPM, marque con una "X" la opción que Ud. crea conveniente en cada una de las premisas.

	SI	NO
2.1 ¿Se le comunicó sus roles y responsabilidades?	<input type="checkbox"/>	<input type="checkbox"/>
2.2 ¿Tiene conocimiento de la separación de áreas en conflicto para prevenir el mal uso de los activos?	<input type="checkbox"/>	<input type="checkbox"/>
2.3 ¿Tiene conocimiento de una lista existente de contactos de autoridades importantes internas y externas?	<input type="checkbox"/>	<input type="checkbox"/>
2.4 ¿Tiene conocimiento de una lista existente de contactos de grupos especializados en seguridad de la información?	<input type="checkbox"/>	<input type="checkbox"/>
2.5 ¿Se aplica seguridad de información en la gestión de proyectos?	<input type="checkbox"/>	<input type="checkbox"/>
2.6 ¿Se ha implementado Políticas de dispositivos móviles?	<input type="checkbox"/>	<input type="checkbox"/>
2.7 ¿Se ha implementado Políticas y medidas de seguridad para sitios de teletrabajo?	<input type="checkbox"/>	<input type="checkbox"/>

3. Respecto a la Seguridad de los recursos humanos en la LPM, marque con una "X" la opción que Ud. crea conveniente en cada una de las premisas.

	SI	NO
3.1 ¿Se le realizó una verificación de sus antecedentes antes de ser incorporado?	<input type="checkbox"/>	<input type="checkbox"/>
3.2 ¿Se le indicó en los términos y condiciones las responsabilidades de la seguridad de información?	<input type="checkbox"/>	<input type="checkbox"/>
3.3 ¿La gerencia le indicó aplicar la seguridad de la información en concordancia con las políticas establecidas?	<input type="checkbox"/>	<input type="checkbox"/>
3.4 ¿Se le brindó capacitación sobre la conciencia de la seguridad de la información?	<input type="checkbox"/>	<input type="checkbox"/>
3.5 ¿Se le comunicó los procesos disciplinarios en caso de infracción de la seguridad de información?	<input type="checkbox"/>	<input type="checkbox"/>
3.6 ¿Se le mencionó sus responsabilidades y deberes respecto a la seguridad de información al terminar su vínculo laboral o cambio de funciones?	<input type="checkbox"/>	<input type="checkbox"/>

4. Respecto a la Gestión de Activos en la LPM, marque con una "X" la opción que Ud. crea conveniente en cada una de las premisas.

	SI	NO
4.1 ¿Se realiza periódicamente un inventario de los activos de la LPM?	<input type="checkbox"/>	<input type="checkbox"/>

**Figura 55. Pág. 01 de 05 – Encuesta aplicada a personal de la LPM**

Fuente: Elaboración del autor

4.2	¿Los activos (Software, Hardware y otros) son propiedad de la LPM?		
4.3	¿Tiene conocimiento de reglas para el uso aceptable de los activos?		
4.4	¿Tiene idea de algún procedimiento de retorno de todos los activos al término del vínculo contractual?		
4.5	¿La información que se maneja en la LPM se encuentra clasificada?		
4.6	¿Existe algún procedimiento de etiquetado de información?		
4.7	¿Conoce la existencia de procedimientos para el manejo de activos?		
4.8	¿Se le ha informado de la implementación de procedimientos para la gestión de medios removibles?		
4.9	¿Se ha puesto a su disposición medios usando procedimiento formales?		
4.10	¿Existe una protección a los medios que contienen información?		

5. Respecto al Control de Acceso en la LPM, marque con una "X" la opción que Ud. crea conveniente en cada una de las premisas.

	SI	NO
5.1	¿Tiene conocimiento de políticas de control de accesos?	
5.2	¿Los accesos que Ud. tiene son los mismos a los que se autorizaron?	
5.3	¿Existe un proceso formal de registro y baja de usuarios?	
5.4	¿Existe un proceso formal de aprovisionamiento de acceso usuarios?	
5.5	¿La asignación de derechos de acceso privilegiado son de carácter restringido?	
5.6	¿Existe un proceso formal para la asignación de información de autenticación secreta?	
5.7	¿Se revisan los derechos de acceso de usuarios periódicamente?	
5.8	¿La remoción de los derechos de acceso se ejecuta de manera inmediata al término de contrato o cambio de funciones?	
5.9	¿Hay una exigencia en la aplicación de buenas prácticas en la autenticación secreta de información?	
5.10	¿Tiene conocimiento de restricciones de acceso a la información?	
5.11	¿Se le menciona la implementación de procedimientos de ingreso seguro?	
5.12	¿Se ha implementado un Sistema de gestión de contraseñas para LPM?	
5.13	¿Existe una restricción para la instalación de programas utilitarios?	
5.14	¿El código fuente del software de la LPM se encuentra restringido?	

6. Respecto a la Criptografía en la LPM, marque con una "X" la opción que Ud. crea conveniente en cada una de las premisas.

	SI	NO
6.1	¿Se le ha comunicado de alguna política sobre el uso de controles criptográficos?	
6.2	¿Existe una política de gestión de claves criptográficas?	

**Figura 56.** Pág. 02 de 05 – Encuesta aplicada a personal de la LPM

**Fuente:** Elaboración del autor



7. Respecto a la Seguridad Física y ambiental en la LPM, marque con una "X" la opción que Ud. crea conveniente en cada una de las premisas.

	SI	NO
7.1 ¿Existen perímetros de seguridad definidos en las instalaciones donde labora?		
7.2 ¿Hay controles de ingreso que permiten el acceso sólo a personal autorizado?		
7.3 ¿Las instalaciones cuentan con una adecuada seguridad física?		
7.4 ¿Se han implementado protecciones contra amenazas externas o ambientales?		
7.5 ¿Existen procedimientos definidos para el trabajo en áreas seguras?		
7.6 ¿En Las áreas de despacho se controla los puntos de acceso?		
7.7 ¿Los equipos tecnológicos con los que trabaja, se encuentran ubicados y protegidos correctamente?		
7.8 ¿Los equipos tecnológicos con los que trabaja, se encuentran protegidos contra fallas de electricidad?		
7.9 ¿Los cableados de energía y telecomunicaciones se encuentran debidamente protegidos contra interferencias o daños?		
7.10 ¿Se ha programado mantenimientos preventivos de los equipos?		
7.11 ¿Cuenta con autorización para retirar los equipos con los que trabaja de su lugar?		
7.12 ¿Se aplica seguridad para los equipos que tengan que salir de las instalaciones de LPM?		
7.13 ¿La reutilización de equipos se hace de manera correcta?		
7.14 ¿Los equipos en desuso son protegidos y asegurados en un lugar adecuado?		
7.15 ¿Existen políticas de escritorio limpio y pantalla limpia?		

8. Respecto a la Seguridad de las operaciones en la LPM, marque con una "X" la opción que Ud. crea conveniente en cada una de las premisas.

	SI	NO
8.1 ¿Existen procedimientos operativos documentados?		
8.2 ¿Hay un control de los cambios, procesos o sistemas que afecten la seguridad?		
8.3 ¿Existe un monitoreo respecto a la capacidad de los recursos?		
8.4 ¿Los entornos de desarrollo, pruebas y operaciones se encuentran separados?		
8.5 ¿Se ha implementado controles contra códigos maliciosos?		
8.6 ¿Se realizan copias de respaldo de información regularmente?		
8.7 ¿Existe una revisión regular de los registros de eventos?		
8.8 ¿Se ha implementado alguna protección para los registros y su información?		
8.9 ¿Se cuenta con un registro de las actividades del administrador?		
8.10 ¿Existe una sincronización de los relojes de los sistemas de procesamiento de información?		
8.11 ¿Se han implementado procedimientos para el control de instalación de software en sistemas operacionales?		
8.12 ¿Se informa de manera oportuna las vulnerabilidades técnicas de los sistemas de información?		

**Figura 57.** Pág. 03 de 05 – Encuesta aplicada a personal de la LPM

**Fuente:** Elaboración del autor



8.13 ¿Existen restricciones sobre instalación de software?		
8.14 ¿Se ha implementado controles de auditoría de sistemas de información?		

9. Respecto a la Seguridad de las comunicaciones en la LPM, marque con una "X" la opción que Ud. crea conveniente en cada una de las premisas.

	SI	NO
9.1 ¿Se ha implementado controles de red en los sistemas de información LPM?		
9.2 ¿Existen mecanismos de seguridad aplicados a los servicios de red?		
9.3 ¿Los grupos de servicios de información se encuentran segregados en redes?		
9.4 ¿Existen políticas y procedimientos formales para la transferencia de información?		
9.5 ¿Están definidos acuerdos sobre la transferencia de información?		
9.6 ¿Existe una protección a los mensajes electrónicos?		
9.7 ¿Se han establecido acuerdos de confidencialidad y no divulgación?		

10. Respecto a la Adquisición, desarrollo y mantenimiento de sistemas en la LPM, marque con una "X" la opción que Ud. crea conveniente en cada una de las premisas.

	SI	NO
10.1 ¿Se han establecido requisitos relacionados a la seguridad de la información para nuevos sistemas de información?		
10.2 ¿Existe una protección de actividad fraudulenta contra la información involucrada en los servicios de aplicaciones?		
10.3 ¿Se ha establecido una protección para las transacciones de servicios?		
10.4 ¿Existen políticas de desarrollo seguro de software?		
10.5 ¿Se han implementado procedimientos de cambios de los sistemas dentro del ciclo de vida?		
10.6 ¿Existe una revisión técnica luego de los cambios de las plataformas operativas?		
10.7 ¿Se han definido restricciones respecto a cambios en los paquetes de software?		
10.8 ¿Existe principios de ingeniería establecidos para sistemas seguros?		
10.9 ¿Se ha protegido los ambientes de desarrollo seguro?		
10.10 ¿Existe una supervisión y monitoreo de la actividad de desarrollo de sistemas?		
10.11 ¿Las pruebas de funcionalidad de los sistemas se desarrollan en la fase de desarrollo?		
10.12 ¿Se ha establecido pruebas de aceptación sobre los sistemas desarrollados?		
10.13 ¿Los datos de prueba se encuentran protegidos y controlados?		

11. Respecto a las Relaciones con los proveedores de la LPM, marque con una "X" la opción que Ud. crea conveniente en cada una de las premisas.

	SI	NO
11.1 ¿Existe alguna política de seguridad para las relaciones con los proveedores?		
11.2 ¿Se establecen todos los requisitos relevantes de seguridad en los acuerdos?		

**Figura 58.** Pág. 04 de 05 – Encuesta aplicada a personal de la LPM

**Fuente:** Elaboración del autor



11.3 ¿Se incluye requisitos para abordar riesgos de seguridad en los acuerdos?		
11.4 ¿Existe un monitoreo y revisión de los servicios de los proveedores?		
11.5 ¿Se realiza una buena gestión de cambios sobre los servicios de los proveedores?		

12. Respecto a la Gestión de incidentes de seguridad de la información de la LPM, marque con una "X" la opción que Ud. crea conveniente en cada una de las premisas.

	SI	NO
12.1 ¿Están establecidos las responsabilidades y procedimientos respecto a los incidentes de seguridad?		
12.2 ¿Existe un reporte de eventos relacionados a la seguridad de la información?		
12.3 ¿Logra reportar oportunamente algún incidente de seguridad de información advertido?		
12.4 ¿Se evalúa y se clasifican los incidentes ocurridos?		
12.5 ¿Existe una respuesta a los incidentes de seguridad de información?		
12.6 ¿Se logra un aprendizaje de la experiencia causada por alguna incidencia de seguridad de la información?		
12.7 ¿Existen procedimientos de recolección de evidencia de los incidentes de seguridad de información producidos?		

13. Respecto a la Continuidad de seguridad de la información de la LPM, marque con una "X" la opción que Ud. crea conveniente en cada una de las premisas.

	SI	NO
13.1 ¿Se ha establecido algún Plan de continuidad de seguridad de la información?		
13.2 ¿Existe procesos, procedimientos y controles para la continuidad de seguridad de la información?		
13.3 ¿La entidad verifica los controles de continuidad de seguridad de la información?		
13.4 ¿Las instalaciones de procesamiento de información se implementan con redundancia suficiente para cumplir con los objetivos?		

14. Respecto al Cumplimiento de la LPM, marque con una "X" la opción que Ud. crea conveniente en cada una de las premisas.

	SI	NO
14.1 ¿Se encuentran identificados los requisitos contractuales para cada sistema de información?		
14.2 ¿Existen procedimientos apropiados para asegurar el cumplimiento de los derechos de propiedad intelectual?		
14.3 ¿Existe una protección de los registros de seguridad de la información?		
14.4 ¿Se mantiene privado y protegido los datos personales de los acuerdos legales y contractuales?		
14.5 ¿Existen controles criptográficos usados en el cumplimiento de todos los acuerdos, legislación y regulación relevantes?		
14.6 ¿Existe una revisión independiente de la seguridad de la información?		
14.7 ¿Cumple con las políticas y normas de seguridad de la información en la LPM?		
14.8 ¿Existe una revisión regular respecto al cumplimiento de las políticas y normas?		

**Figura 59.** Pág. 05 de 05 – Encuesta aplicada a personal de la LPM

Fuente: Elaboración del autor





**Anexo 05. Relación de N° de pregunta de Encuesta con cláusulas del  
Anexo A de la NTP ISO/IEC 27001:2014**

*Tabla 32. Relación N° de Pregunta – Cláusula NTP ISO/IEC 27001:2014*

PREGUNTAS DE ENCUESTA		CLÁUSULAS DEL ANEXO A - NTP ISO/IEC 27001:2014		
N°	SUB N°	N°	DESCRIPCIÓN	
P1	1.1	A.5	A. 5.1.1	Políticas de seguridad de la información
	1.2		A. 5.1.2	
P2	2.1	A.6	A. 6.1.1	Organización de la seguridad de la información
	2.2		A. 6.1.2	
	2.3		A. 6.1.3	
	2.4		A. 6.1.4	
	2.5		A. 6.1.5	
	2.6		A. 6.2.1	
	2.7		A. 6.2.2	
P3	3.1	A.7	A. 7.1.1	Seguridad de los recursos humanos
	3.2		A. 7.1.2	
	3.3		A. 7.2.1	
	3.4		A. 7.2.2	
	3.5		A. 7.2.3	
	3.6		A. 7.3.1	
P4	4.1	A. 8	A. 8.1.1	Gestión de Activos
	4.2		A. 8.1.2	
	4.3		A. 8.1.3	
	4.4		A. 8.1.4	
	4.5		A. 8.2.1	
	4.6		A. 8.2.2	
	4.7		A. 8.2.3	
	4.8		A. 8.3.1	
	4.9		A. 8.3.2	
	4.10		A. 8.3.3	
P5	5.1	A. 9	A. 9.1.1	Control de acceso
	5.2		A. 9.1.2	
	5.3		A. 9.2.1	
	5.4		A. 9.2.2	
	5.5		A. 9.2.3	
	5.6		A. 9.2.4	
	5.7		A. 9.2.5	
	5.8		A. 9.2.6	
	5.9		A. 9.3.1	
	5.10		A. 9.4.1	
	5.11		A. 9.4.2	
	5.12		A. 9.4.3	
	5.13		A. 9.4.4	

	5.14		A. 9.4.5	
P6	6.1	A. 10	A. 10.1.1	Criptografía
	6.2		A. 10.1.2	
	7.1		A. 11.1.1	
	7.2		A. 11.1.2	
	7.3		A. 11.1.3	
	7.4		A. 11.1.4	
	7.5		A. 11.1.5	
	7.6		A. 11.1.6	
	7.7		A. 11.2.1	
P7	7.8	A. 11	A. 11.2.2	Seguridad física y ambiental
	7.9		A. 11.2.3	
	7.10		A. 11.2.4	
	7.11		A. 11.2.5	
	7.12		A. 11.2.6	
	7.13		A. 11.2.7	
	7.14		A. 11.2.8	
	7.15		A. 11.2.9	
	8.1		A. 12.1.1	
	8.2		A. 12.1.2	
	8.3		A. 12.1.3	
	8.4		A. 12.1.4	
	8.5		A. 12.2.1	
	8.6		A. 12.3.1	
P8	8.7	A. 12	A. 12.4.1	Seguridad de las operaciones
	8.8		A. 12.4.2	
	8.9		A. 12.4.3	
	8.10		A. 12.4.4	
	8.11		A. 12.5.1	
	8.12		A. 12.6.1	
	8.13		A. 12.6.2	
	8.14		A. 12.7.1	
	9.1		A. 13.1.1	
	9.2		A. 13.1.2	
	9.3		A. 13.1.3	
P9	9.4	A. 13	A. 13.2.1	Seguridad de las comunicaciones
	9.5		A. 13.2.2	
	9.6		A. 13.2.3	
	9.7		A. 13.2.4	
	10.1		A. 14.1.1	
	10.2		A. 14.1.2	
	10.3		A. 14.1.3	
P10	10.4	A. 14	A. 14.2.1	Adquisición, desarrollo y mantenimiento de sistemas
	10.5		A. 14.2.2	
	10.6		A. 14.2.3	
	10.7		A. 14.2.4	



	10.8		A. 14.2.5	
	10.9		A. 14.2.6	
	10.10		A. 14.2.7	
	10.11		A. 14.2.8	
	10.12		A. 14.2.9	
	10.13		A. 14.3.1	
P11	11.1	A. 15	A. 15.1.1	Relaciones con los proveedores
	11.2		A. 15.1.2	
	11.3		A. 15.1.3	
	11.4		A. 15.2.1	
	11.5		A. 15.2.2	
P12	12.1	A. 16	A. 16.1.1	Gestión de incidentes de seguridad de la información
	12.2		A. 16.1.2	
	12.3		A. 16.1.3	
	12.4		A. 16.1.4	
	12.5		A. 16.1.5	
	12.6		A. 16.1.6	
	12.7		A. 16.1.7	
P13	13.1	A. 17	A. 17.1.1	Aspectos de seguridad de la información en la gestión de continuidad del negocio
	13.2		A. 17.1.2	
	13.3		A. 17.1.3	
	13.4		A. 17.2.1	
P14	14.1	A. 18	A. 18.1.1	Cumplimiento
	14.2		A. 18.1.2	
	14.3		A. 18.1.3	
	14.4		A. 18.1.4	
	14.5		A. 18.1.5	
	14.6		A. 18.2.1	
	14.7		A. 18.2.2	
	14.8		A. 18.2.3	

**Nota.** Fuente: Elaborado por el autor



## **Anexo 06. Manual de Seguridad de la Información para la Línea de Producción de Microformas**

### **INTRODUCCIÓN**

El Manual de Seguridad de la Información de la Línea de Producción de Microformas ha sido elaborado en concordancia a la NTP ISO/IEC 27001:2014 “TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos”

En ese sentido, se han adoptado las recomendaciones de la referida norma técnica y la normativa institucional para la Línea de Producción de Microformas, a fin de proteger la información y asegurar la Certificación de Idoneidad Técnica de Producción y Almacenamiento de Microformas de la Línea de Producción de Microformas.

### **1. GENERALIDADES**

#### **1.1 Objetivo**

Establecer el procedimiento de seguridad de la información para asegurar la confidencialidad, integridad y disponibilidad de la información que se procesa en la Línea de Producción de Microformas.

#### **1.2 Finalidad**

Desarrollar un marco regulador para preservar la información que se procesa en la Línea de Producción de Microformas, asimismo, asegurar la Certificación de Idoneidad Técnica de Producción y Almacenamiento de Microformas de la Contraloría General de la República.

#### **1.3 Alcance**

Es de observancia y cumplimiento obligatorio para todos los trabajadores del Dpto. de Gestión Documentaria y de las sedes regionales que laboran en la Línea de Producción de Microformas, incluyendo los trabajadores con contratos administrativos de servicios y servicios por tercero, así como los trabajadores de empresas que mantienen una relación contractual con la institución, en tanto y en cuanto ejecuten sus actividades en la Línea de Producción de Microformas.

Asimismo, a los trabajadores de la Contraloría General de la República, que tengan contacto con los recursos e información de la Línea de Producción de Microformas.

#### **1.4 Documentos de Referencia**

NTP ISO/IEC 27001:2014. “TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos”

NTP ISO/IEC 17799:2007. EDI. Tecnología de la Información. Código de Buenas prácticas para la Gestión de la Seguridad de la Información, aprobado por Resolución Ministerial N° 246-2007-PCM

NTP 392.030-2 2005 MICROFORMAS. Requisitos para las organizaciones que operan Sistemas de Producción de Microformas Parte 2: Medios de Archivos Electrónicos

## **2. POLITICAS DE SEGURIDAD ASOCIADO AL SISTEMA DE PRODUCCIÓN DE MICROFORMAS**

### **2.1 Políticas de Seguridad de la Línea de Producción de Microformas**

El Departamento de Gestión Documentaria de la Contraloría General de la República es el órgano encargado de la producción de microformas; por lo consiguiente, debe resguardar la información que maneja, por lo que se establece las siguientes políticas de seguridad de la información en la Línea de Producción de Microformas.

- a. Implementar medidas para resguardar la información que se maneja en la Línea de Producción de Microformas.
- b. Asegurar la continuidad del funcionamiento de la Línea de Producción de Microformas.
- c. Mejorar de manera continua los procesos referentes a la Seguridad de la información de la Línea de Producción de Microformas.
- d. Promover la concientización de la seguridad de la información a los trabajadores que laboran en la Línea de Producción de Microformas.
- e. Capacitar continuamente a los trabajadores, respecto a la seguridad de la información relacionada a la Línea de Producción de Microformas.



## **2.2 Revisión y Evaluación**

- a. Las políticas de Seguridad de la Información de la Línea de Producción de Microformas, se debe actualizar cada tres años, cuando vence la vigencia del manual o cuando se detecten o presenten riesgos potenciales que puedan afectar la seguridad de la información, como resultado de una evaluación continua
- b. Se debe designar un coordinador técnico, encargado de la revisión y actualización de las Políticas de Seguridad de la Información de la Línea de Producción de Microformas.

## **3. ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD**

### **3.1 Organización para la seguridad de la Información**

#### **a. Organización**

El Dpto. de Gestión Documentaria, es el responsable de administrar las operaciones, recursos tecnológicos y humanos, así como, la seguridad de la información en la Línea de Producción de Microformas.

Los encargados de proponer y aprobar las políticas y medidas de seguridad de la información de la Línea de Producción de Microformas, está integrado por las siguientes personas:

- Gerente de Gestión Documentaria
- Coordinador Técnico
- Supervisor de la Línea de Producción de Microformas.
- Monitor de la Línea de Producción de Microformas.
- Responsable de Soporte Informático.

#### **b. Asignación de Responsabilidades sobre Seguridad de la Información**

El Departamento de Gestión Documentaria, es el responsable de la información y del sistema de información que da soporte informático a sus actividades.

El Departamento de Tecnologías de la Información y el Departamento de Logística respectivamente, son las únicas unidades orgánicas autorizadas para instalar, cambiar, revisar, reparar, manipular los equipos de cómputo,

escáneres de producción, impresoras, entre otros equipos. Asimismo, instalar y configurar el software de digitalización e indexación entre otros, así como realizar el análisis de vulnerabilidades a fin de detectar y neutralizar probables manipulaciones en los activos.

### **c. Revisión Independiente de la Seguridad de la Información**

La revisión de la seguridad de la información de la Línea de Producción de Microformas debe ser llevada a cabo por las Unidades Orgánicas competentes.

El Departamento de Seguridad Integral, es responsable de efectuar el seguimiento y monitoreo de la seguridad integral de la institución.

Asimismo, realiza la evaluación de la seguridad personal de la Alta Dirección y de los trabajadores, cuando sea necesario; con el propósito de determinar si la actividad que viene realizando, significa algún riesgo para su integridad física.

El Departamento de Tecnologías de la Información, es responsable de efectuar en forma periódica la verificación sobre el correcto uso de los equipos de telefonía, computo, correos electrónicos, etc.

El Departamento de Logística, efectuará en forma periódica verificaciones físicas de la ubicación y estado de los activos de la institución, como medida de seguridad de los mismos y proponer medidas correctivas que consideren convenientes.

## **3.2 Seguridad en los Accesos a Terceras Personas**

### **a. Identificación de los Riesgos por Accesos a Terceros**

El Dpto. de Gestión Documentaria, es el responsable de autorizar el acceso a las instalaciones, estaciones de trabajo, documentación en soporte de papel y electrónica que se encuentren en la Línea de Producción de Microformas.

El Dpto. de Tecnologías de la Información, será el responsable de administrar los accesos a Laserfiche, computadores, servidores de datos y equipos de comunicación (centrales telefónicas, routers, switches, etc) y protegerlos contra daños y hurtos

El Dpto. de Seguridad Integral, se encargará del control de accesos del personal a la sede central y administrar el acceso biométrico a las instalaciones del Dpto. de Gestión Documentaria. Asimismo, administrar el control de acceso de

personal a las instalaciones de las sedes regional de control, donde se ubica la Línea de Producción de Microformas.

#### **b. Requisitos de Seguridad en Contratos por Terceros**

El proveedor que brinda servicio en la Línea de Producción de Microformas y maneja información, debe firmar la Declaración Jurada “Personal Externo que labora en la Línea de Producción de Microformas”.

El supervisor de la Línea de Producción de Microformas, debe oficializar la entrega de la normativa institucional sobre la seguridad de la información para los trabajadores que cumplen funciones, antes del inicio de sus servicios en la Línea de Producción de Microformas que son los siguientes:

- 1) Reglamento de Seguridad de la Contraloría General de la República.
- 2) Directiva para la Conducta y Desempeño del Personal de la Contraloría General de la República y de los Órganos de Control Institucional.
- 3) El Dpto. de Tecnologías de la Información, debe supervisar los trabajos de configuración e instalación de software y hardware realizado por los proveedores de la Línea de Producción de Microformas

#### **c. Outsourcing (Subcontratación de Empresas especializadas)**

El Dpto. de Gestión Documentaria, es la unidad orgánica encargada de dirigir procesos técnicos de la Línea de Producción de Microformas en la institución, responsable del buen uso, conservación y custodia de la información en la Línea de Producción de Microformas, en consecuencia, no autoriza los contratos de outsourcing referentes a la producción de microformas.

### **4. CLASIFICACIÓN Y CONTROL DE ACTIVOS**

#### **4.1 Responsabilidad sobre los Activos**

El supervisor de la línea de Producción de Microformas, es el encargado de elaborar, actualizar y conservar el inventario de activos de la línea de producción de microformas

#### **4.2 Inventario de Activos**

El sistema de Producción de Microformas, debe contar con un inventario de activos de información, lo cual se detallan a continuación:

##### **Activos de información:**

Expedientes.

Cargos de oficio.

Informes de control emitidos por las unidades orgánicas.

Microformas.

Manual del sistema de producción de microformas.

Manual de producción de microformas.

Procedimientos del sistema de producción de microformas.

Manual de seguridad de la información del sistema de producción de microformas.

**Activos software:**

Laserfiche Server.

Laserfiche Audit Trail Advanced.

Laserfiche Web Access.

Laserfiche Email.

Laserfiche Snapshot.

Laserfiche Workflow.

Laserfiche ScanConnect.

Laserfiche Toolkit.

Laserfiche User Full Named.

Laserfiche CD Plus.

Laserfiche Quick Fields.

Cosingn For Laserfiche.

**Activos Físicos:**

Equipos de Cómputo.

Escáneres de Alta Producción.

Escáneres de Producción Departamental.

Escáner de Planos.

Escáner de documentos empastados.

Impresora de Producción.

Impresora de Discos.

Lectoras de código de Barras.

**Servicios:**

Servicio de Mantenimiento de los escáneres de Producción.

Servicio de soporte y mantenimiento del Laserfiche.

Servicio de fedatario Juramentado con especialización de informática.



Servicio de custodia de Microarchivo.

**Personal:**

Gerente de Gestión Documentaria.

Coordinador técnico.

Supervisor de la Línea de Producción de Microformas.

Fedatario Juramentado.

Monitor de la Línea de Producción de Microformas.

Responsable de Preparación de Documentos.

Responsable de Digitalización e Indexación.

Responsable de Control de Calidad 01.

Responsable de Calidad 02.

Responsable de Calidad 03.

Responsable de Grabación y Rotulado.

Analista de Trámite Documentario.

Responsable de Armado de Documentos.

Responsable de Reprocesamiento.

#### **4.3 Clasificación de la Información**

La información debe ser clasificada de acuerdo al valor del activo, requisitos legales, sensibilidad y criticidad para la Línea de Producción de Microformas. La clasificación y valoración de los activos de información debe ser elaborada por el Coordinador Técnico y el Supervisor de la Línea de Producción de Microformas. Para la clasificación y valoración de los activos de información, deben emplearse los criterios establecidos.

### **5. SEGURIDAD LIGADA AL PERSONAL**

#### **5.1 Inclusión de la seguridad en las responsabilidades laborales.**

- a. El Supervisor de la Línea de Producción de Microformas, debe brindar al trabajador que ingrese por primera vez a la Línea de Producción de Microformas, la orientación sobre la normativa institucional vigente en la entidad, así como la indicación de sus derechos, obligaciones y funciones.
- b. Todos los trabajadores de la Línea de Producción de Microformas, incluyendo los trabajadores que laboran, bajo cualquier forma o modalidad contractual, que presta servicios a la referida línea, deben conocer y cumplir lo siguiente:





- 1) Presentar una Declaración Jurada de Confidencialidad o Integridad, conforme al Manual del Sistema de Producción de Microformas.
  - 2) Usar su computadora, correo electrónico e información de la Línea de Producción de Microformas solo para fines del cumplimiento de sus trabajos asignados, siendo estos únicamente de carácter institucional.
- c. Todos los trabajadores de la Línea de Producción de Microformas, incluyendo los trabajadores que laboran, bajo cualquier forma o modalidad contractual, que presta servicios la referida línea se encuentran prohibidos de:
- i. Usar, revelar, o entregar información, incluyendo la contenida en medios magnéticos, bajo cualquier modalidad, a la que hayan accedido con ocasión del ejercicio de sus funciones o cargo desempeñado, con el objeto de ser utilizada para fines distintos o a la producción de microformas, o con el fin de obtener una ventaja indebida para sí, o para terceros.
  - ii. Divulgar, difundir o transmitir total o parcialmente a terceros ajenos al ámbito funcional de la Línea de Producción de Microformas, cualquier contenido de información, documentos o material de trabajo de la Contraloría General de la República.
  - iii. Pegar stickers en las computadoras.
  - iv. Ingerir alimentos sobre las computadoras o documentos, así como colocar y/o manipular líquidos en su cercanía.
  - v. Rociar directamente sobre las computadoras líquidos de ambiente.
  - vi. Colocar y/o apilar documentos u otros objetos sobre las computadoras, y en ubicaciones que obstruyan o impidan su adecuada ventilación y uso.
  - vii. Ubicar la unidad central de proceso en una posición distinta a su diseño original (horizontal o vertical).
  - viii. Dejar las computadoras y sus accesorios, en lugares inseguros.
  - ix. Conectar artefactos eléctricos sobre la línea eléctrica de uso exclusivo para las computadoras, o sobre estabilizadores de corriente.
  - x. Trasladar las computadoras a otra área, sin la autorización expresa del Gerente de Gestión Documentaria y del Dpto. de Logística.



- xi. Utilizar protectores de pantalla para los monitores de las computadoras con fotos de artistas modelos, deportistas, dibujos animados, o cualquier otra imagen que pueda resultar poco seria u ofensiva.
- xii. Instalar programas informáticos en las computadoras.
- xiii. Modificar los parámetros o configuración de las computadoras de la institución, así como el software y/o sistema informático instalado.
- xiv. Abrir las computadoras, así como extraer o cambiar componentes.
- xv. Acceder a información contenida en unidades de almacenamiento (medios magnéticos u ópticos) o en los discos de las computadoras personales que no les han sido asignadas.
- xvi. Hacer uso de software ajeno a la institución con el fin de acceder a información no autorizada.
- xvii. Alterar, modificar, falsificar, ocultar o destruir documentos de trabajo, así como extraer documentos de la Contraloría General de la República.

## **5.2 Compromiso de Confidencialidad.**

- a. Todos los trabajadores de la Línea de Producción de Microformas, que tengan acceso a información, deben firmar cláusulas de protección de la confidencialidad de dicha información, durante y después de la relación contractual.
- b. El Supervisor de la Línea de Producción de Microformas, debe asegurar que todos los trabajadores que laboran en la Línea de Producción de Microformas, presenten su Declaración Jurada de Confidencialidad, asimismo, debe custodiar dicha documentación.
- c. Todos los activos de información existentes en el Dpto. de Gestión Documentaria, pertenecen a la Contraloría General de la República y su divulgación debe contar con la autorización del Gerente de Gestión Documentaria.
- d. Los trabajadores de la Línea de Producción de Microformas, están prohibidos de alterar, modificar, falsificar, ocultar, extraer o destruir documentos oficiales de la Contraloría General de la República, inclusive aquellos que no tengan clasificación.



### 5.3 Términos y Condiciones de la Relación Laboral.

Los trabajadores de la Línea de Producción de Microformas, están en la obligación de cumplir con las siguientes acciones:

- a. Desempeñar su labor con eficiencia y eficacia, cumpliendo sus funciones de acuerdo a su naturaleza y en concordancia a los objetivos y metas del Dpto. de Gestión Documentaria.
- b. Desempeñar las funciones y realizar las tareas asignadas, observando una conducta proba y honesta durante su labor cotidiana, cumpliendo con las órdenes y directivas que se impartan.
- c. Acatar la función directriz de la institución manteniendo el principio de autoridad, así como el respeto a los superiores y demás trabajadores de la Contraloría General de la República.
- d. Conservar y hacer buen uso de los equipos, útiles y materiales que se proporcionen para el desempeño de sus funciones.
- e. Cooperar con el orden e informar oportunamente a quien corresponda, sobre situaciones o acciones que puedan poner en grave peligro la seguridad del personal u ocasionar daños a los muebles, equipos e instalaciones de la Línea de Producción de Microformas; o sobre riesgos que se presenten.
- f. Observar las obligaciones y prohibiciones dispuestas en las normas reglamentarias sobre transparencia en la conducta y/o desempeño que dicte la Contraloría General de la República.
- g. Conservar los documentos o bienes en general que utilicen en el desarrollo de sus actividades, cuya titularidad, posesión o custodia estén a cargo del Departamento de Gestión Documentaria.

### 5.4 Cumplimiento de las Políticas de Seguridad de la Información.

Cualquier incidente de seguridad de la información en la Línea de Producción de Microformas originado por incumplimiento del presente Manual, podrá dar lugar a una acción disciplinaria.

Son consideradas faltas disciplinarias de los trabajadores de la Línea de Producción de Microformas y sujetas a sanción las siguientes:

- a. El incumplimiento de lo normado en las leyes laborales, reglamentos, normas y directivas que emanen de la Alta Dirección.

- b. El incumplimiento injustificado de sus obligaciones de trabajo y la negligencia en el ejercicio de las funciones que le correspondan en el cargo asignado.
- c. La reiterada resistencia al cumplimiento de las órdenes de sus superiores inmediatos.
- d. Operar equipos de cómputo que no le hayan sido asignado o para el cual no tuviese autorización.
- e. Dar a conocer a terceros el contenido de documentos.
- f. No cumplir con las disposiciones de control de vigilancia y seguridad de la Contraloría General de la República, así como las que indiquen el personal de seguridad que presta servicios para la institución.

### **5.5 Capacitación de Usuarios.**

- a. El supervisor de la Línea de Producción de Microformas, está en la obligación de cumplir con las siguientes acciones:  
Brindar una capacitación en las funciones y en seguridad de la información como parte del proceso de inducción a los nuevos trabajadores de la Línea de Producción de Microformas.  
Oficializar programas de concientización para el personal de la Línea de Producción de Microformas, en temas de seguridad de la información sobre amenazas existentes y las medidas de seguridad apropiadas.
- b. Los trabajadores de la Línea de Producción de Microformas, están en la obligación de capacitarse de manera obligatoria y actualizada en sus funciones y en seguridad de la información.

### **5.6 Terminación de Relación Laboral o Cambio de Empleo.**

El trabajador saliente de la Línea de Producción de Microformas debe cumplir lo siguiente:

- a. Presentar una carta al Dpto. de Personal o Dpto. de Logística con los vistos buenos del Supervisor de la Línea de Producción de Microformas y del Gerente de Gestión Documentaria.
- b. Efectuar la entrega de su carnet de identificación, los bienes asignados para el desempeño de sus funciones, el informe del estado de labores que tiene bajo su responsabilidad.

La referida entrega de cargo y de bienes inventariados debe remitirse al Supervisor de la Línea de Producción de Microformas

## **6. SEGURIDAD FÍSICA Y DEL ENTORNO**

### **6.1 Perímetro de Seguridad Física**

- a. El Departamento de Seguridad Integral, debe ser el responsable de la seguridad en las instalaciones de la Contraloría General de la República, tanto en la sede central como las sedes regionales.
- b. El Departamento de Seguridad Integral, debe realizar el control de acceso a las instalaciones de la sede central de la Contraloría General de la República apoyado por la empresa que brinda servicio de vigilancia.
- c. La empresa que brinda el servicio de vigilancia, debe realizar el control de acceso a las instalaciones de la sede regional de la Contraloría General de la República, supervisado por el Dpto. de Seguridad Integral.
- d. El Departamento de Gestión Documentaria, debe custodiar el equipamiento tecnológico, recursos humanos, documentación y mobiliario de la Línea de Producción de Microformas, por lo consiguiente, debe contar con un control de acceso biométrico para el ingreso de personal autorizado.
- e. Es obligación de la sede regional de la Contraloría General de la República, custodiar el equipamiento tecnológico, recursos humanos, documentación, mobiliario, entre otros bienes de la Línea de Producción de Microformas.
- f. El Dpto. de Tecnologías de la Información, deberá custodiar los servidores de datos, la base de datos y el Laserfiche, por lo consiguiente, deberá contar con un control de acceso para el ingreso de personal autorizado.

### **6.2 Controles Físicos de Ingresos**

- a. El Gerente de Gestión Documentaria, deberá autorizar el acceso de los trabajadores y proveedores que brindan servicios en la Línea de Producción de Microformas.
- b. El Supervisor de la Línea de Producción de Microformas, debe controlar el ingreso y salida de los trabajadores que brindan servicios en la Línea de Producción de Microformas y reportar al Gerente de Gestión Documentaria, en caso de presentarse incidentes.



- c. Los trabajadores de la Línea de Producción de Microformas deben realizar las siguientes acciones:
- Presentar su carnet de identificación para registrar sus ingresos y salidas a la sede central o sede regional de la Contraloría General de la República. Su uso es personal, intransferible y obligatorio.
  - Pasar su debido índice en la lectora instalada en la puerta de acceso del Dpto. de Gestión Documentaria, para ingresar a la Línea de Producción de Microformas.
  - Comunicar al Supervisor de la Línea de Producción de Microformas, el deterioro por uso, extravío o sustracción del carnet de identificación.

### 6.3 Seguridad de los Equipos

- a. El Departamento de Logística, es responsable de llevar los registros de los bienes de la institución a nivel nacional, tales como altas y bajas, adquisiciones, asignaciones, registro de inventario, ubicación física y cualquier otro acto que permita conocer el estado situacional de los activos de la Contraloría General de la República.
- b. El Dpto. de Tecnologías de la Información, es responsable de instalar los servidores de red y equipos de comunicación, en lugares apropiados y protegidos contra daños o hurtos; restringiendo el ingreso de estos lugares solo a personal autorizado.
- c. El Supervisor de la Línea de Producción de Microformas, debe elaborar el Inventario de Equipos de Cómputo de la Línea de Producción de Microformas.
- d. Los trabajadores de la Línea de Producción de Microformas, deben realizar las siguientes acciones:

Conservar y velar por el buen uso y funcionamiento del equipo de cómputo, escáner de producción, token, entre otros, que se le proporciona para el desempeño de sus funciones.

Utilizar los equipos puestos a su disposición, siguiendo las instrucciones del fabricante y/o los protocolos dictados del caso; con el propósito de evitar accidentes personales, deterioro de los equipos, incendios o cualquier siniestro que afecte los bienes y las instalaciones.

## **7. GESTIÓN DE COMUNICACIONES Y OPERACIONES**

### **7.1 Documentación de Procedimiento de Operación**

El supervisor de la Línea de Producción de Microformas, debe custodiar el Manual de Seguridad de la Información, Manual de Producción de Microformas, Procedimientos del Sistema de Producción de Microformas, el manual de usuario de los escáneres de producción y el Laserfiche, y facilitar su disponibilidad al personal autorizado por el Gerente de Gestión Documentaria.

### **7.2 Medidas y Controles contra Software Malicioso**

- a. El Departamento de Tecnologías de la Información, debe realizar medidas contra software malicioso y verificar el correcto uso de los equipos de cómputo, software, correos electrónicos, entre otros equipos, identificando las vulnerabilidades que pudieran existir en la Línea de Producción de Microformas.
- b. Los trabajadores de la Línea de Producción de Microformas, deben eliminar los archivos electrónicos recibidos de remitentes desconocidos, sin ser abiertos.
- c. El Dpto. de Gestión Documentaria, debe prohibir el acceso a internet en las estaciones de trabajo de los procesos de Preparación de Documentos, Digitalización e Indexación, Control de Calidad y Verificación de Imágenes / Firma digital y Grabación y Rotulado.

Asimismo, prohíbe la instalación de software no autorizado en los equipos de cómputo de la Línea de Producción de Microformas, tales como protectores de pantalla, software demostrativo, manejadores de música, video, mensajería instantánea, etc.

### **7.3 Gestión Interna de Respaldo y Recuperación**

#### **a. Diarios de Operación**

El Supervisor de la Línea de Producción de Microformas, debe solicitar al Responsable de Soporte Informático, la revisión periódica (Cada 15 días) de los registros operacionales respecto a los accesos y modificaciones a la información almacenada en las estaciones de trabajo de la Línea de Producción de Microformas y de existir discrepancias, deben ser informadas al Gerente de Gestión Documentaria.

**b. Registro de Fallas**

El Supervisor de la Línea de Producción de Microformas, deberá registrar las fallas (incluyendo años) de los equipos de cómputo de la Línea de Producción de Microformas.

**c. Recuperación de la Información**

El Dpto. de Tecnologías de la Información, deberá realizar copias de seguridad de los datos y programas de la Línea de Producción de Microformas, las que serán guardadas en un lugar seguro y distinto.

Los trabajadores de la Línea de Producción de Microformas, son responsables de proteger los datos almacenados en sus computadoras, contra pérdidas o daños, debiendo elaborar sus copias de respaldo.

**8. CONTROL DE ACCESOS****8.1 Gestión de Acceso a Usuarios**

- a. El Gerente de Gestión Documentaria, autoriza el acceso a la estación de trabajo en el Laserfiche RIO
- b. El Departamento de Tecnologías de la Información, administra los usuarios de las estaciones de trabajo y los usuarios de Laserfiche.
- c. El Supervisor de la Línea de Producción de Microformas, utiliza el Audit Trail para identificar los inicios y cierres de sesión en el Laserfiche.

**8.2 Registro de Usuarios y Gestión de Privilegios**

- a. El Supervisor de la Línea de Producción de Microformas, debe elaborar, actualizar y custodiar el Inventario de Usuarios y Permisos del Laserfiche.
- b. Los trabajadores de la Línea de Producción de Microformas, de acuerdo a sus funciones y actividades se les asigna privilegios de usuarios en el Laserfiche, autorizado por el Gerente de Gestión Documentaria, mediante memorando dirigido al Dpto. de Tecnologías de la Información.

**8.3 Responsabilidades de los Usuarios**

- a. El Supervisor de la Línea de Producción de Microformas, debe oficializar el bloqueo de la contraseña de la estación de trabajo y el Laserfiche, cuando un trabajador se ausente por motivo de vacaciones, enfermedad o permiso por un periodo mayor a 5 días, el Dpto. de Gestión Documentaria, debe comunicar al

Dpto. de Tecnologías de la Información, dentro de las 24 horas siguientes de ocurrido el hecho, vía memorando para realizar el bloqueo de su contraseña, la que será restituida a su retorno.

- b. El Dpto. de Gestión Documentaria, debe comunicar al Dpto. de Tecnologías de la Información, dentro de las 24 horas siguientes, vía memorando con la finalidad de desactivar o activar un usuario, para el cese o ingreso de un nuevo trabajador a la Línea de Producción de Microformas.
- c. Los trabajadores de la Línea de Producción de Microformas, deben realizar las siguientes acciones:

Mantener en secreto su clave de acceso a la estación de trabajo y Laserfiche; todas las transacciones registradas con su clave de acceso serán de su exclusiva responsabilidad.

Evitar abandonar su estación de trabajo dejando activa su cuenta de usuario.

#### **8.4 Equipo de Cómputo de Usuario Desatendido**

Los trabajadores de la Línea de Producción de Microformas, deben asegurar que la pantalla de su equipo de cómputo quede protegida y no muestre información cuando esté desatendida.

#### **8.5 Control de Acceso al Sistema Operativo**

Los trabajadores de la Línea de Producción de Microformas, tienen restringido el acceso a las cuentas de administrador del sistema operativo de la estación de trabajo, solo el personal del Dpto. de Tecnologías de Información, tiene acceso a dichas cuentas de administrador.

### **9. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN**

- a. Los trabajadores de la Línea de Producción de Microformas, deben anotar y reportar inmediatamente los eventos o incidentes al Supervisor de la Línea de Producción de Microformas, los eventos o incidentes que deben reportar se detallan a continuación:

Pérdida de servicio de internet o equipos de cómputo.

Mal funcionamiento del software o hardware

Acceso no autorizado en la estación de trabajo y Laserfiche

Incumplimiento de las normativas y mecanismos de seguridad.

- b. El Supervisor de la Línea de Producción de Microformas, deberá registrar los detalles importantes del evento o incidente y comunicar al Dpto. de Tecnologías de la Información para su verificación.
- c. El Dpto. de Tecnologías de Información, en caso de comprobar la vulnerabilidad de la seguridad de información, comunicará al Dpto. de Gestión Documentaria.
- d. El Supervisor de la Línea de Producción de Microformas, el Coordinador Técnico y el Responsable de Soporte Informático, son los encargados de proponer y ejecutar las medidas correctivas para reforzar las medidas de seguridad vulneradas.
- e. El Supervisor de la Línea de Producción de Microformas, es el encargado de hacer el seguimiento y registro de las medidas correctivas y documentar todos los incidentes y acciones a ejecutar.

## **10. GESTIÓN DE CONTINUIDAD DEL NEGOCIO**

- a. El Supervisor de la Línea de Producción de Microformas y el Coordinador Técnico, son responsables de elaborar y actualizar el Plan de Continuidad de la Línea de Producción de Microformas.
- b. El Supervisor de la Línea de Producción de Microformas y el Monitor de la Línea de Producción de Microformas, deben ejecutar lo establecido en el Plan de Continuidad del Sistema de Producción de Microformas.

## **11. CUMPLIMIENTO**

### **11.1 Identificación de la Legislación Aplicable.**

El incumplimiento de lo señalado en el presente Manual, dará inicio al proceso administrativo – disciplinario, a cargo del Dpto. de Recursos Humanos; quien podrá solicitar la colaboración del Dpto. de Seguridad Integral en la Indagación de los hechos.

De acuerdo al capítulo XI del Reglamento Interno de Trabajo se aplicará al régimen disciplinario correspondiente tomando en cuenta la gravedad de la falta, reiteración, jerarquía, antecedentes o la causal incurrida por la cual resulte irrazonable la continuidad del vínculo laboral, sin perjuicio del inicio de acciones penales o civiles ante las autoridades competencias



### 11.2 Derechos de Propiedad Intelectual

El Laserfiche RIO está amparado en la licencia perpetuidad con la finalidad de cumplir con las leyes y asegurar el soporte continuo por parte de los proveedores.

## Anexo 07. Resultados de Urkund



### Urkund Analysis Result

Analysed Document:	Tesis - Romero Mas.docx (D41624311)
Submitted:	9/20/2018 3:37:00 PM
Submitted By:	jbruno@crece.uss.edu.pe
Significance:	10 %

