

UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ

Facultad de Ciencias Administrativas, Contables y Comercio

Carrera de Gestión de la Información Gerencial

**TRABAJO DE UNIDAD DE INTEGRACIÓN CURRICULAR
MODALIDAD ESTUDIO DE CASO**

Previo a la obtención del título de:

Licenciada en Gestión de la Información Gerencial

TEMA

Norma de Seguridad para la Recuperación Efectiva de la Información del Sector
Público de la Universidad Laica Eloy Alfaro de Manabí de la Dirección
Administrativa de Talento Humano, Manta 2025 (Estudio de Caso)

AUTORA

Calderón Vera Karina Lorena

TUTORA

Lic. Mercy Rojas Once, Mgt.

MANTA-MANABÍ-ECUADOR

2025-1

Tema

Norma de Seguridad para la Recuperación Efectiva de la Información del Sector Público de la Universidad Laica Eloy Alfaro de Manabí de la Dirección Administrativa de Talento Humano, Manta 2025 (Estudio de Caso)

	NOMBRE DEL DOCUMENTO: CERTIFICADO DE TUTOR(A).	CÓDIGO: PAT-04-F-004
	PROCEDIMIENTO: TITULACIÓN DE ESTUDIANTES DE GRADO BAJO LA UNIDAD DE INTEGRACIÓN CURRICULAR	REVISIÓN: 1
		Página 1 de 1

CERTIFICACIÓN

En calidad de docente tutor de la Facultad de Ciencias Administrativas, Contables y Comercio de la Universidad Laica “Eloy Alfaro” de Manabí, CERTIFICO:

Haber dirigido, revisado y aprobado preliminarmente el Trabajo de Integración Curricular: Estudio de Caso bajo la autoría de la estudiante **Calderón Vera Karina Lorena**, legalmente matriculada en la carrera de Gestión de la Información Gerencial, período académico 2025-2, cumpliendo el total de 240 horas (96 horas Fase de Diseño y 144 horas Fase de Resultados e Informe), cuyo tema del proyecto es **“Recuperación Efectiva de la Información del Sector Público de la Universidad Laica Eloy Alfaro de Manabí de la Dirección Administrativa de Talento Humano, Manta 2025 (Estudio de Caso)”**.

La presente investigación ha sido desarrollada en apego al cumplimiento de los requisitos académicos exigidos por el Reglamento de Régimen Académico y en concordancia con los lineamientos internos de la opción de titulación en mención, reuniendo y cumpliendo con los méritos académicos, científicos y formales, y la originalidad del mismo, requisitos suficientes para ser sometida a la evaluación del tribunal de titulación que designe la autoridad competente.

Particular que certifico para los fines consiguientes, salvo disposición de Ley en contrario.

Manta, 27 de enero de 2026.

Lo certifico,


 Lic. Mercy Celinda Rojas Once, Mg.
 Docente Tutora

Autoría

Yo, Karina Lorena Calderón Vera, con cédula de identidad Número 1315559300, estudiante de la Carrera Gestión de la Información Gerencial, de la Facultad de Ciencias Administrativas, Contables, y Comercio de la Universidad Laica Eloy Alfaro de Manabí, declaro que el presente trabajo cuyo tema es “Norma de Seguridad para la Recuperación Efectiva de la Información del Sector Público de la Universidad Laica Eloy Alfaro de Manabí de la Dirección Administrativa de Talento Humano, Manta 2025 (Estudio de Caso).” es de mi Autoría y ha sido realizado con fines académicos,

En tal sentido, manifiesto, la originalidad del trabajo, dejando establecido que aquellos aportes intelectuales de otros autores se han referenciado debidamente en el texto del trabajo.


Karina Lorena Calderón Vera

C.I: 1315559300

Dedicatoria

Quiero agradecer principalmente a Dios por permitirme cumplir con uno de mis objetivos y por darme todas esas fuerzas que a veces sentía que ya no podía, porque cuando pensaba en rendirme él me decía que yo podía y que siempre me guio por hacer las cosas bien.

Dedico esta investigación a mi Madre Angelica Vera porque desde que inicie esta etapa fue la que más me dio su apoyo siempre me decía tú puedes y eso sinceramente era lo que más me motivaba que ella creyera en mí cuando ni yo sabía que podía lograrlo

Dedico también este esfuerzo a mi padre Cesar Calderón por qué sé que él siempre me apoyo a si no me lo dijera, a mis hermanos porque sé que siempre desearan todo lo mejor para mí

A mí pareja Deivi Holguin que siempre estuvo allí dándome animo diciéndome en cada momento que yo podía que era muy inteligente y que me admiraba mucho y a mi hijo Lahiam Holguín que fue mi inspiración para poder superarme, a mis hermanos, Grendy Calderón, Alejandro Calderón, Yandri Calderón, y por último a mi tutora, que cada día me daba sus consejos para que hiciera las cosas bien, a mis compañeros que siempre estuvieron allí ayudándome en lo que no entendía

Y por último a mis abuelos que siempre me decían ese título te va abrir caminos no lo vallas a dejar nunca porque nosotros creemos en ti, a todas estas personas que amo tanto, le estoy muy agradecida gracias, por siempre creer en mí.

Calderón Vera Karina Lorena

Agradecimientos

Expreso mi más sentido agradecimiento a la Universidad Laica Eloy Alfaro de Manabí, especialmente a la Carrera de Gestión de Información Gerencial, de la Facultad de Ciencias Administrativas, Contables y Comercio que me ha permitido ser parte de este templo de conocimiento y aprendizaje.

A la Facultad de Ciencias Administrativas, Contables y Comercio, por acogerme como estudiante para la preparación académica y por aportarme conocimientos en este hermoso campo que es Gestión de la Información Gerencial.

Agradezco a mis docentes de la Carrera mencionada desde mi corazón por cada consejo brindado hacia mi persona, por sus enseñanzas, y por todo lo compartido en el aula de clases en la cual me siento muy sentimental en este momento recordando todo lo bonito que se vivió con mis compañeros ya que cada uno tomará su rumbo y solo espero que a todos les vaya bien en el ámbito profesional.

Finalmente, un agradecimiento especial a mi tutora Lic. Mercy Rojas Once, Mgt. por acompañarme por tener dedicación y paciencia por aconsejarme en esta investigación, por el apoyo brindado que sin duda alguna si no hubiese sido por ella no hubiese podido finalizar esta investigación con éxito.

Karina Lorena Calderón Vera

ÍNDICE

Certificación	3
Autoría	4
Dedicatoria	5
Agradecimientos	6
ÍNDICE	7
Resumen.....	9
Abstract	10
INTRODUCCIÓN	11
Antecedentes Investigativos.....	13
Justificación	16
OBJETIVOS	17
Objetivo general.....	17
Objetivos Específicos.....	17
MARCO CONCEPTUAL	18
Seguridad de la Información en Entornos Administrativos Universitarios	18
<i>Principios: confidencialidad, integridad y disponibilidad</i>	<i>18</i>
<i>Normativas aplicables: ISO 27001, ISO 15489 y EGSi</i>	<i>18</i>
Amenazas Comunes en la Administración Pública y Educativa	19
Recuperación de la Información como Función Estratégica	19
<i>Tipos de recuperación: parcial, total e inmediata</i>	<i>19</i>
Protocolos de Respaldo, Copia de Seguridad y Contingencia.....	19
Factores que limitan la recuperación eficaz en instituciones públicas	20
Cultura organizacional y capacidades institucionales.....	20

<i>Rol del personal y percepción del riesgo</i>	20
<i>Capacitación técnica como pilar de la seguridad documental</i>	20
<i>Barreras organizacionales y culturales</i>	21
<i>Barreras organizacionales y culturales</i>	21
Marco Metodológico.....	22
Diseño de la investigación	22
Enfoque de investigación.....	22
Tipo de investigación	22
Métodos de investigación	22
Población y muestra.....	22
<i>Población</i>	22
<i>Muestra</i>	23
Técnicas e instrumentos de recolección de información	23
Guías de entrevista y guía de observación.....	23
Resultados Obtenidos.....	24
Análisis de Resultados	34
Conclusión	36
Referencia	39
Anexos	47
<i>Fundamentar teóricamente la seguridad de la información</i>	48
<i>Propuesta de mejora (Norma)</i>	48
Propuesta de solución	50

Resumen

La presente investigación se llevó a cabo debido a los diversos problemas existentes en relacionados a la seguridad y recuperación de la información, principalmente en el entorno administrativo de talento humano de la Universidad laica Eloy Alfaro de Manabí, donde se manejan datos esencia de todos los colaboradores qué trabajan en esta alma mater. Para tal efecto, se plantea como objetivo general, diseñar una Norma de Seguridad que permita una recuperación eficiente de la información institucional, Dónde promedio de un diseño metodológico de carácter cualitativo y descriptivo, y mediante la integración de técnicas de recopilación de datos como entrevistas semiestructuradas y una ficha de observación que permita evaluar los procesos y restauración de la información, se encontraron diversos hallazgos que permitieron identificar que no existe una norma detallada, y al mismo tiempo, tampoco el personal que trabaja en la Universidad no recibe capacitaciones constantes, generando que se usen mecanismos con enfoques informales al momento de recuperar la información, generan generando un riesgo sustancial al momento del manejo de los datos. Por lo cual, se concluye que es esencial la implementación de una norma interna que contribuye a sistematizar los procesos, disminuir riesgos y vulnerabilidades con la finalidad de impulsar una cultura de seguridad relacionada con la información, provocando que la gestión administrativa sea eficiente y segura.

Palabras clave: Seguridad de la información, recuperación de la información, talento humano

Abstract

This research was conducted due to various problems related to information security and recovery, mainly in the human resources administration environment at the Eloy Alfaro University in Manabí, where essential data on all employees working at this alma mater is managed. To this end, the general objective is to design a Security Standard that allows for the efficient recovery of institutional information. Using a qualitative and descriptive methodological design and integrating data collection techniques such as semi-structured interviews and an observation form to evaluate the processes and restoration of information, various findings were made that identified that there is no detailed standard, and at the same time, the staff working at the University does not receive ongoing training, leading to the use of informal approaches when recovering information, which generates a substantial risk when handling data. Therefore, it is concluded that it is essential to implement an internal standard that contributes to systematizing processes and reducing risks and vulnerabilities in order to promote a culture of information security, resulting in efficient and secure administrative management.

Keywords: Information security, information recovery, human talent

INTRODUCCIÓN

Actualmente, las empresas que son de carácter estatal se encuentran a una presión considerable que se relaciona con un manejo eficaz y seguro del flujo de información, lo cual genera que exista un mayor peso para el entorno de talento humano, debido a que en esta área se encuentra información no solamente con enfoque personal, sino también laboral que no puede quedar a la intemperie, significando determinante implementar normas precisas y estrategias que fortalezcan la confidencialidad e integridad de información, así como también el acceso a los datos.

En este sentido, el control y la gestión de la información en las instituciones públicas no constituyen una opción eventual, sino una necesidad estratégica. Aquello tiene como finalidad salvaguardar la transparencia e impulsar un servicio eficiente sin intermitencias.

La presente investigación, titulada "Norma de Seguridad para la Recuperación Efectiva de la Información del Sector Público de la Universidad Laica Eloy Alfaro de Manabí, Dirección Administrativa de Talento Humano, Manta 2025", aquello se justifica en el entorno de exigencia para mejorar la protección de información, así como también potenciar la recuperación de datos de este departamento. De esa manera, muchas instituciones han optado por dirigirse a entornos digitales diversos con la finalidad de gestionar documentos, lo cual genera que no siempre se fortalezca la seguridad, principalmente cuando estos no han sido integrados al manejo de estándares técnicos, o en su defecto métodos que son de carácter informal que limitan el resguardo de la información.

Por esa razón, se emplea como objetivo general, establecer una norma de seguridad para la recuperación efectiva de la información en la Dirección Administrativa de Talento Humano de la ULEAM, para alcanzar este propósito, se emplea un enfoque cualitativo, basado en entrevistas semiestructuradas y revisión documental, con el fin de analizar las prácticas actuales y detectar vulnerabilidades en los sistemas de respaldo y recuperación.

El presente trabajo está estructurado conforme al modelo de integración curricular por fases. En la fase de diseño se abordarán los antecedentes, la justificación del problema, el marco conceptual y el enfoque metodológico. Primero se interpretó lo que el trabajo de campo permitió ver con claridad, a partir de aquello, se trabajó en una propuesta concreta que cumpla con los estándares de calidad que la institución requiere.

Por lo que esta investigación busca detectar los puntos donde la información está en riesgo, dejar claras las acciones para recuperarla, si algo falla y reforzar, desde dentro, una cultura que realmente valore el cuidado de los datos en el área de Talento Humano de la ULEAM.

En el ámbito universitario, robustecer las pautas de seguridad de la información protege los datos internos y, de paso, sembrar una cultura preventiva frente a riesgos tecnológicos y administrativos, debido a que las unidades que manejan información deben revisar periódicamente sus protocolos, formar al personal y adoptar herramientas que aseguren la recuperación ágil de información. Por lo cual, es de vital importancia conocer y detectar las fortalezas, debilidades y ámbitos concretos susceptibles de mejora en los procedimientos de recuperación de la Dirección Administrativa de Talento Humano (Garavito, 2022).

Antecedentes Investigativos

Los antecedentes permiten identificar investigaciones previas y situaciones reales que contextualizan el problema de estudio, evidenciando vacíos existentes en la seguridad y recuperación de información en instituciones públicas.

Un estudio realizado por García y Hervás (2020) en una universidad mexicana examinó el sistema de gestión de seguridad de la información (SGSI) bajo la norma ISO/IEC 27001, a pesar de que las políticas formales estaban implementadas, se pudo constatar que aún persistían fallas importantes en los procedimientos de respaldo y en la capacidad real de restaurar la información cuando ocurrían incidentes críticos, siendo necesario replantear las rutas de contingencia mediante la ejecución periódica de simulacros y la actualización constante del inventario digital, permitiendo con ello disminuir los tiempos de interrupción operativa y resguardar de forma efectiva la integridad de los archivos institucionales.

Asimismo, Borrero (2022), identificaron que diversas instituciones confían en tener respaldos como si eso, por sí solo, resolviera cualquier pérdida de información, pero en realidad los sistemas no se prueban ni se revisan con la frecuencia que exige una amenaza real. Su estudio combinó entrevistas con responsables técnicos y un análisis aplicado de la norma ISO 27002, y a lo largo del proceso quedó claro que el mayor riesgo no está en la ausencia de herramientas, sino en la falta de procedimientos vivos, capaces de activarse sin improvisación. La brecha entre el discurso normativo y lo que se hace en campo termina dejando a las organizaciones en un estado de vulnerabilidad disfrazado de cumplimiento. Para ellos, el problema no es solo técnico, sino cultural: sin personal entrenado y procesos que se apliquen con regularidad, ninguna norma puede garantizar que la información esté realmente segura cuando más se la necesita.

Durante los últimos años, se ha evidenciado que las entidades públicas en Ecuador enfrentan serias dificultades para implementar de forma efectiva medidas robustas de seguridad informática, y en este panorama, Armas y Taherdoos (2025) advierten que, aunque el Esquema General de Seguridad de la Información (EGSI) cuenta con respaldo normativo, su aplicación práctica se ve obstaculizada por la insuficiencia de recursos económicos y la falta de capacitación especializada entre el personal técnico que debería ejecutarlo.

Un análisis reciente de Ávila-Coello (2024), referente con lo que ocurre dentro de varias entidades públicas del país, se nota que siguen existiendo vacíos importantes en todo lo relacionado con la seguridad de la información, y eso se debe, en gran parte, a que no se han corregido ciertas fallas estructurales que ya se vienen arrastrando desde hace tiempo, como la falta de entrenamientos reales para el personal, la ausencia de ejercicios o pruebas que simulen restauraciones ante emergencias, y una manera de trabajar donde no se le da la importancia necesaria a los riesgos que puede traer una mala gestión documental. Por eso, el autor recomienda hacer talleres que ayuden al personal a poner en práctica los protocolos y que las normas no queden solo en papel.

En un estudio publicado por Core (2024), se fijó en algo que casi nadie mira, qué tan lista está una institución pública para recuperar su información cuando algo falla. Hablaron con gente de adentro y revisaron normas como la ISO 27001, y descubrieron que, aunque los sistemas aguantan problemas, no están preparados para actuar rápido, así que no sirven mucho cuando pasan caídas o ataques inesperados. Más allá de los documentos o manuales que puedan existir, el estudio dejó claro que lo urgente es contar con protocolos que eficientes, con personal capacitado para ejecutarlos y con una estructura de respaldo que no dependa de buenas intenciones, sino de prácticas sostenidas en el tiempo.

Y finalmente, un estudio ejecutado por Palacios (2022) acerca de la aplicación del sistema de conservación del archivo central de Agrocalidad, planteando como objetivo principal, medir si cada disposición de la norma se traduce en una recuperación efectiva de los expedientes institucionales, encontrando que, si bien los procedimientos oficiales habían sido plasmados sobre el papel, seguían faltando pruebas de restauración. De esa manera, al cierre del informe, se determinó que desde la perspectiva regulatoria no existe ningún tipo de respaldo de enfoque práctico, así como tampoco de vigilancia permanente, lo cual genera que los documentos no se aseguran de forma eficiente, ni tampoco la disponibilidad cuando se los necesita, obligando a sugerir reformas inmediatas de carácter técnico al personal, con la finalidad de llevar a cabo controles operativos que mejoren la sostenibilidad de la gestión documental. Así mismo, se destaca que estos antecedentes evidencian la falta de marcos normativos, y recursos tecnológicos disponibles asociados a las fallas de enfoque estructural o en su defecto, ausencia de una cultura organizacional que sigue complicando la recuperación integral de la información.

Definición del Estudio de Caso

La presente investigación se enfoca en la Dirección Administrativa de Talento Humano de la Universidad Laica Eloy Alfaro de Manabí (ULEAM), ubicada en la ciudad de Manta, debido al manejo constante de información sensible, como datos personales de los colaboradores, contratos laborales, movimientos administrativos y demás documentación inherente a la gestión del personal. Por ello, la elección de esta área no se seleccionó de forma aleatoria, sino que se justifica en la importancia que representa para la institucionalidad de esta alma máter, asociado al alcance operativo y disponibilidad al momento de otorgar acceso a cualquier tipo de información que se necesite y que sea relevante.

De esa forma, el desarrollo investigativo permitió evidenciar de forma directa como se están cuidando los respaldos asociados a la información en Área de Talento Humano, permitiendo determinar detalles que solo se observan en el interior de este departamento con la finalidad de comprender si cumplen con los estándares de preparación inmediata para recuperar la información en caso de cualquier escenario hostil.

Este trabajo intentó ver si las formas que hoy se usan para cuidar y recuperar la información realmente funcionan como deberían. Después de eso, se busca entender si esas soluciones pueden sostenerse con el tiempo y si las personas dentro del área realmente las integran como parte de su trabajo diario, no solo por obligación, sino como una práctica que protege el funcionamiento institucional.

En este sentido, se plantean las siguientes interrogantes, derivadas de la problemática

1. ¿Cuáles son las principales fuentes de vulnerabilidad y fallas en el manejo de la información del Departamento de Talento Humano, según un análisis de riesgos basado en evidencia?
2. ¿Qué nivel de eficacia tienen los procedimientos actuales de recuperación de datos en garantizar la continuidad operativa del Departamento de Talento Humano ante incidentes?
3. ¿Qué elementos clave deben incluirse en los protocolos y lineamientos para que sean efectivos en la protección de la información del Departamento de Talento Humano?

Justificación

La presente investigación surge de una necesidad concreta que no puede seguir ignorándose dentro de la Dirección Administrativa de Talento Humano de la Universidad Laica Eloy Alfaro de Manabí, pues al analizar cómo se llevan a cabo las actividades en el entorno administrativo, donde se considera que actualmente no son tan eficientes al momento de guardar la información ante cualquier problema que se presente, reflejando un riesgo para los archivos y documentos. Aunque existen ciertos protocolos, su aplicación resulta débil y poco efectiva en momentos donde más se los necesita, lo cual revela que el problema no está solo en lo que falta, sino en cómo se ha venido sosteniendo un sistema que no responde a las exigencias del entorno.

La importancia del estudio radica en que esta unidad administrativa resguarda información sensible como contratos, movimientos laborales y datos personales del personal universitario, por ello, impulsar los estándares que son de carácter documental no solo ayuda a proteger todo el contenido, sino que también impulsa la capacidad inmediata de carácter institucional ante demandas internas y externas, dinamizando que la gestión documental se realice por medio de principios básicos, como la justicia, transparencia o en su defecto la agilidad.

Desde la perspectiva de los beneficios, este trabajo no solo se enfoca en identificar las fallas desde la perspectiva administrativa, sino que construye propuestas reales y viables, pensadas para traducirse en políticas institucionales que eleven el nivel técnico de los procesos internos y reduzcan la exposición al riesgo tecnológico y humano, lo cual no solo permitirá una recuperación de información más eficaz, sino que también promoverá una cultura de prevención permanente que abarque desde la capacitación del personal hasta el uso inteligente de los recursos disponibles.

Finalmente, el alcance de este estudio trasciende lo local, ya que sus resultados pueden ser útiles como referencia para otras instituciones públicas que enfrentan problemáticas similares, de esta manera, la investigación aporta conocimiento aplicable y validado, que contribuye a una mejora continua de los sistemas de información que sostienen el funcionamiento diario del aparato estatal.

OBJETIVOS

Objetivo general

- Analizar la Norma de Seguridad de la Información que garantice la recuperación rápida, segura y eficiente de la información gestionado por el Departamento Administrativo de Talento Humano de la Universidad Laica Eloy Alfaro de Manabí 2025

Objetivos Específicos

- Identificar los riesgos, vulnerables y fallas o fuentes conocidas al manejo y lineamiento de la información del Departamento de Talento Humano.
- Evaluar los procedimientos y mecanismos existentes para la recuperación de datos y la continuidad operativa.
- Diseñar los protocolos y lineamientos que conformarán la norma de seguridad de la información.

MARCO CONCEPTUAL

Seguridad de la Información en Entornos Administrativos Universitarios

Principios: confidencialidad, integridad y disponibilidad

En el entorno universitario, la información acompaña cada decisión, trámite y vínculo que se construye entre personas e instituciones, por eso resguardarla no es un asunto secundario ni exclusivo de lo técnico. Lo importante es que se mantenga segura, sin accesos indebidos, sin cambios fuera de control y disponible justo cuando hace falta. Todo eso crea una base sólida para trabajar con confianza. Como recuerda (Solís, 2023), cuando estos principios se viven en serio dentro de la institución, se reducen los riesgos y los procesos mantienen su credibilidad.

Cuando no hay conocimiento claro o se baja la guardia, la información queda expuesta (Mora J. P., 2020). No basta con tener normas, hace falta que todo el equipo esté comprometido y reciba formación constante, porque cuidar los datos es una tarea que le toca a todos.

Normativas aplicables: ISO 27001, ISO 15489 y EGSÍ

Cumplir con las normativas de seguridad de la información en universidades no es solo una obligación técnica sino una necesidad real para sostener procesos administrativos que manejen datos sensibles con orden y respaldo confiable donde tres marcos son esenciales en ese propósito como la ISO 27001 que regula los sistemas de seguridad la ISO 15489 que orienta la gestión documental y el Esquema Gubernamental de Seguridad de la Información (EGSI) que adapta estos principios al funcionamiento del sector público ecuatoriano y establece controles claros para mantener protegida la información institucional de forma continua. Estas normativas permiten que las instituciones consoliden procesos formales y alineados con estándares internacionales sin perder su marco legal nacional (Mora J. y., 2020).

Cada una de estas normas tiene un rol complementario que va más allá del cumplimiento formal porque juntas permiten construir una estructura funcional donde se integran responsabilidades técnicas administrativas y legales en torno a la seguridad documental donde la ISO 27001 aporta directrices sobre riesgos la ISO 15489 establece el ciclo documental y el EGSÍ obliga a aplicar estos marcos dentro del ecosistema estatal ecuatoriano y eso exige que cada unidad incorpore los principios no como una carga sino como una garantía de orden público. Cantos

(2023), menciona que el valor real de estas normas está en que permiten trabajar con menos riesgos, con más orden y de forma clara, lo que al final hace que todo se entienda y se maneje con más transparencia.

Amenazas Comunes en la Administración Pública y Educativa

Cuando no hay sistemas firmes ni pasos claros para actuar, la información queda expuesta, y eso pasa seguido en instituciones públicas y educativas. Ahí es donde empiezan los problemas: datos que se pierden, que se filtran o que terminan donde no deberían. Ávila (2024) comenta que muchas organizaciones siguen usando prácticas empíricas, y eso hace que sus sistemas sean más frágiles y propensos a fallar.

Zambrano y Mendoza (2023) señalan que las amenazas no solo vienen de fallas técnicas, sino también de hábitos inseguros y poca cultura preventiva, por lo que la prevención debe integrarse en toda la organización.

Recuperación de la Información como Función Estratégica

Tipos de recuperación: parcial, total e inmediata

La recuperación de información no siempre se da de la misma forma, todo depende del daño y de qué tan urgente sea resolverlo:

- **Si es parcial**, se restauran solo algunos archivos o bases puntuales.
- **Si es total**, hay que levantar todo el sistema desde cero.
- **Si es inmediata**, se busca acceder rápido a lo más crítico, sin pausas ni bloqueos.

Como explica Carrión (2021), aplicar bien cada tipo ayuda a que la institución aguante mejor los problemas y no pierda tiempo valioso. Escoger cuál usar depende de qué tan grave fue el impacto y qué herramientas se tienen a mano.

Protocolos de Respaldo, Copia de Seguridad y Contingencia

Tener copias guardadas y saber cómo reaccionar marca la diferencia cuando se trata de seguir trabajando sin contratiempos. Como mencionan Haro y Silva (2022), cuando todo eso se piensa con anticipación, los errores y los fallos técnicos se resuelven sin mayores complicaciones.

Un plan de contingencia solo sirve si hay preparación real, si cada persona sabe qué hacer y si todo se ha puesto en práctica antes. (Borrero J. M., 2024), cuando eso se cumple, no solo se logra seguir funcionando, también se protege lo más valioso: la información.

Factores que limitan la recuperación eficaz en instituciones públicas

Recuperar la información se vuelve un problema cuando no hay la tecnología necesaria, el personal no sabe bien qué hacer y no existen reglas claras para actuar rápido. Trujillo (2025) señala que todo eso hace que sea difícil reaccionar cuando ocurre un problema, y entonces se pone en riesgo tanto el trabajo como los datos importantes.

Además, hay cosas que complican aún más las cosas, como los trámites interminables, la resistencia a cambiar lo que ya está y que las diferentes áreas no se entiendan ni trabajen juntas. (Saleh M. O., 2021) menciona que mientras no se arreglen esas dificultades, difícilmente se podrá tener un sistema que funcione bien y dure en el tiempo.

Cultura organizacional y capacidades institucionales

Rol del personal y percepción del riesgo

El personal administrativo es fundamental para proteger la información, pero no basta con que sepan que hay riesgos; ese sentido se va formando con charlas, capacitación y comunicación constante. Delgado (2024) , expresa que la actitud que tenga cada persona hace la diferencia para que los controles realmente funcionen.

Por otro lado, Ávila (2024) determina que cuando quienes trabajan en la institución entienden bien qué papel juegan y cómo afectan sus acciones, se crea una cultura que previene problemas y fortalece la seguridad de todos.

Capacitación técnica como pilar de la seguridad documental

Pacotaípe y Rondón (2024) remarcan que cuando el personal se capacita seguido, trabaja con más confianza y comete menos errores por desconocimiento. Cedeño (2024) añade que una formación constante y bien hecha hace que el equipo se comprometa más y que la seguridad en la institución sea mejor.

Barreras organizacionales y culturales

Trujillo (2025) muestra que la resistencia que viene desde dentro, la falta de información clara y las costumbres que se mantienen por hábito son los mayores obstáculos para que los sistemas de seguridad documental realmente funcionen. Saleh et al. (2021) apuntan que para que una política de seguridad tenga éxito, es clave encontrar un balance entre la tecnología, las personas y la cultura que se vive en la institución.

Barreras organizacionales y culturales

Muchas veces el problema no está en la falta de recursos, sino en una cultura interna que frena cualquier intento de cambio, porque cuando no hay una guía clara ni se comunica con transparencia, la gente desconfía, se resiste y deja de comprometerse, y eso termina afectando los procesos que deberían proteger la información y asegurar que todo siga funcionando, por eso no se trata solo de hacer ajustes técnicos, sino de cambiar la forma en que se entiende el trabajo desde adentro. Trujillo (2025), estas barreras limitan la aplicación efectiva de sistemas y procedimientos a pesar de contar con recursos técnicos adecuados.

Estos retos no solo se ven en la estructura organizativa, sino que se viven en la cultura diaria donde predominan costumbres informales, falta de conciencia real sobre lo que implica la gestión documental y poca formación, lo que hace que el personal no asuma su responsabilidad en la seguridad de la información y por eso es necesario apostar por estrategias que combinen capacitación constante, liderazgo claro y políticas firmes para construir una cultura basada en la responsabilidad compartida. El éxito en la gestión documental depende del equilibrio entre tecnología, personas y cultura organizacional (Saleh et al., 2021).

Marco Metodológico

Diseño de la investigación

Esta investigación se basa en observar cómo funcionan las cosas en la institución sin alterar nada, simplemente viendo lo que ocurre en su ambiente normal. Este enfoque es ideal para entender cómo están hoy los protocolos de seguridad y recuperación de información en la Dirección Administrativa de Talento Humano de la Universidad Laica Eloy Alfaro de Manabí. Según lo que se encontró en la revisión de documentos y el diagnóstico inicial, los procesos con la documentación se hacen sin reglas claras, lo que hace que este análisis técnico y organizacional sea aún más necesario.

Enfoque de investigación

Este estudio adopta un enfoque cualitativo para acercarse a lo que el personal realmente vive cuando aplica medidas de seguridad y recuperación de datos, poniendo atención en cómo entienden y enfrentan esos procesos más allá de lo que dicen los protocolos. Al revisar con detenimiento sus relatos, se revelan fallas, contradicciones y vacíos que permiten mirar el problema con más claridad y pensar en respuestas que sí se ajusten a la realidad.

Tipo de investigación

Esta investigación, de carácter descriptivo y propósitivo, busca detallar cómo funcionan hoy los mecanismos para recuperar la información, y al mismo tiempo, plantear una propuesta técnica que se adapte a las necesidades reales sin alterar la dinámica habitual. No se trata solo de señalar fallas, sino de ofrecer soluciones prácticas y duraderas que realmente fortalezcan la seguridad documental dentro de la institución.

Métodos de investigación

Se empleo la metodología inductivo -deductivo y sintético-analítico bibliográfico.

Población y muestra

Población

Este estudio se enfocó en el personal administrativo de la Dirección de Talento Humano de la Universidad Laica Eloy Alfaro de Manabí, especialmente en quienes se encargan del archivo, la

gestión, el cuidado y la digitalización de la información laboral. Son quienes más contacto tienen con los sistemas institucionales, por lo que conocen bien cómo se maneja la seguridad y la recuperación de datos en el día a día.

Muestra

La muestra fue intencional y se eligió pensando en quienes cuentan con experiencia, están involucrados en procesos importantes y trabajan directamente con el manejo de Información Pública. Solo se incluyó a funcionarios que realmente manejan archivos e información institucional, para asegurar que el análisis tenga sentido y los resultados sean útiles, en este caso fueron 3 entrevistados de los cuales 1 directora y 2 funcionarios.

Técnicas e instrumentos de recolección de información

Guías de entrevista y guía de observación

Resultados Obtenidos

Los resultados que se obtuvieron a raíz de las aplicaciones técnicas que hacen referencia a la observación directa, así como a la entrevista, fueron de gran importancia debido a que contribuyeron a la recopilación y análisis de la información, tanto desde una perspectiva de carácter teórica, y al mismo tiempo práctica. Aquello contribuyó a evaluar el entorno actual del Departamento de Talento Humano de la Universidad Laica Eloy Alfaro de Manabí.

En relación la Universidad Laica Eloy Alfaro de Manabí, no tiene una norma única y específica para la recuperación de Información de Talento Humano, sino que se rige por políticas y reglamentos generales de la Universidad. En la cual establece medidas generales para proteger la información Institucional ya que cuenta con un reglamento de Gestión Documental y archivo que establece con responsabilidad mantener un archivo digital y el proceso de recepción y tener registrados los documentos y, por otra parte, a nivel de seguridad integral, aplica el Reglamento de Seguridad, Higiene y Salud del Trabajo (ULEAM, 2016), en el cual se le asigna responsabilidades de los funcionarios en caso de emergencia.

Políticas y Normativas aplicables

Políticas de Seguridad de la Información

Establece la implementación de medidas de seguridad para proteger la información en todas sus fases garantizando confidencialidad, Integridad y disponibilidad.

Reglamentos de Gestión Documental y Archivo

Establece la responsabilidad de cada dependencia de la Universidad Incluyendo a Talento Humano de mantener un archivo digital de la Información documental relevante que tenga en su cargo (ULEAM, 2023).

Asimismo, al examinar los resultados con mayor detenimiento, se advierte que el Departamento de Talento Humano actúa bajo lineamientos institucionales amplios; no obstante, carece de una directriz específica que ordene el proceso de recuperación de la información ante una eventual contingencia. En este escenario, la actuación frente a fallos técnicos o pérdidas de datos depende, más bien, de la experiencia práctica del personal que de un procedimiento formal previamente definido. Por ello, aunque existe una intención clara de proteger la documentación, la ausencia de una norma detallada deja espacios de interpretación que podrían generar respuestas distintas ante una misma situación crítica.

Ahora bien, en relación con los mecanismos de respaldo, se observa que la información se almacena en sistemas digitales institucionales; sin embargo, no se evidencia una práctica constante de verificación que permita comprobar si esas copias pueden restituirse con rapidez y sin errores. Dicho de otro modo, conservar archivos en la nube representa un paso importante, aunque no suficiente, para garantizar una recuperación eficaz. Además, cuando no se realizan pruebas reales de restauración, el riesgo permanece oculto, ya que solo se detecta la verdadera capacidad de respuesta cuando ocurre un incidente concreto.

Por otra parte, también resulta relevante señalar que la capacitación formal en torno a los principios de confidencialidad, integridad y disponibilidad no ha sido sistemática. En efecto, cuando estos fundamentos no se refuerzan mediante espacios de formación continua, su aplicación se vuelve desigual entre los miembros del equipo. Así, mientras algunos funcionarios comprenden la importancia de resguardar datos sensibles, otros pueden limitarse a cumplir tareas operativas sin dimensionar plenamente el impacto de una gestión inadecuada. Esta realidad adquiere mayor peso si se considera que el área administra información laboral y datos personales que requieren especial cuidado dentro del contexto universitario.

Finalmente, al integrar todos los hallazgos, se puede afirmar que la institución dispone de bases normativas que orientan la gestión documental, donde todavía hace falta consolidar un instrumento interno que precise responsabilidades, establezca tiempos estimados de recuperación y determine mecanismos de control periódico. De esta forma, la recuperación de la información dejaría de depender de acciones aisladas y pasaría a formar parte de un sistema organizado y verificable. En ese contexto, fortalecer este aspecto no solo mejoraría la protección de los datos, sino que también aportaría mayor estabilidad y confianza en la gestión administrativa del Departamento de Talento Humano.

Por otra parte, al analizar la forma en que se aplican las políticas institucionales dentro del área, se puede observar que la normativa existente orienta el cuidado general de la información, aunque no profundiza en la recuperación específica de los datos gestionados por Talento Humano. En este sentido, los reglamentos vigentes establecen responsabilidades amplias relacionadas con el archivo digital y la protección documental; sin embargo, no desarrollan con claridad procedimientos operativos adaptados a las dinámicas propias del departamento. Así, el manejo de la recuperación queda integrado de manera implícita dentro de disposiciones generales, lo cual limita la precisión técnica con la que deberían abordarse posibles incidentes.

Tabla 1*Matriz de triangulación de la información*

Pregunta	P1	P2	P3	Cita	Análisis
1. ¿Qué entiende por “seguridad de la información” aplicada al sector público universitario?	Hoy en día la seguridad de la Información es lo más importante que se debe aplicar en una institución de educación superior como es la nuestra en la cual estamos aquí en entornos laborales al ser un área de Talento Humano nosotros debemos entender que se debe preservar la información incluso se deben aplicar formatos de confidencialidad al personal, se deben entregar convenios de confidencialidad o acuerdos para que el personal entienda que aquí la información no puede verse afectada.	Son procesos, políticas o herramientas en la cual se ayuda a proteger la información que se maneja dentro de una institución ya sea pública o privada en el cual solo los accesos del personal autorizado tienen el acceso a esta información para que no allá alteraciones en la institución.	Exigir lo que debe tener la información del personal institucional o de las diferentes gestiones que se hacen tanto para usuarios internos como externos.	Se entiende como un conjunto de acciones que cuida la información institucional, y además garantiza un acceso seguro, mantiene los datos correctos y permite que estén disponibles para apoyar las actividades académicas y administrativas sin generar problemas (Menendez y Moreira Sánchez, 2025).	En base a la opinión de los participantes se destaca que se debe exigir el uso de herramientas para resguardar la información del Personal.
2. ¿Qué diferencia existe entre confidencialidad, integridad y	Se entiende que confiabilidad de datos solo las personas autorizadas pueden acceder a la Información, es decir no	Confidencialidad se enfoca que solo puede ser accesible la información por personas autorizadas,	La integridad es que la información sea la misma se maneje constantemente	La confidencialidad señala quién puede acceder a los datos, y además la integridad revisa que se mantengan sin	Los participantes mencionan que la confidencialidad se enfoca

disponibilidad de los datos?	compartir datos personales con terceros, a tener un cifrado de información que cada usuario debe tener su contraseña para ingresar al sistema, Integridad de datos que deben ser estos correctos, completos que sean claros que no se puedan modificar sin ninguna autorización y así se va a evitar que alguien cambie o edite información que no deba y disponibilidad de datos es que deben estar accesibles para cumplir con la ley de transparencia.	integridad se enfoca en que la información tiene que ser exacta, completa y sin alteraciones y disponibilidad es que la información debe ser accesible para todo el personal que está autorizado.	nte, la confidencialidad es que no se divulgue y disponibilidad que este siempre que se necesite a la mano para poder utilizar.	cambios, mientras que la disponibilidad garantiza que puedan utilizarse cuando se los necesita dentro de las actividades institucionales (Segura y Jorge Wilson, 2025).	en información real y que la integridad tiene que ser información exacta y disponibilidad que siempre que se necesite la información puedan utilizarla de acuerdo a la necesidad.
3. ¿Ha recibido capacitación formal sobre estos tres principios? ¿En qué consistió?	Claro que si la Constitución indica que como servidores públicos bueno no es necesario ser capacitados es importante entender la ley e interpretarla la constitución indica claramente en unos de sus principios en unos de sus artículos que nosotros debemos precautelar la información de terceros ser íntegros y sobre todo	Capacitación como tal indico que no porque yo soy nueva en el puesto de trabajo formal no pero capacitación por parte de la directora en cuanto a la información, la seguridad y la integridad si.	Capacitación formal en base a este tema no hemos recibido.	Ha recibido una capacitación formal sobre confidencialidad, integridad y disponibilidad, y además consistió en aprender con ejemplos prácticos, revisar procedimientos esenciales y practicar acciones sencillas que permiten proteger la información dentro de las actividades institucionales (Vega et al., 2025)	

	que la información también sea transparente y clara para los organismos de control.				
4. ¿Qué sistema o herramienta utiliza para almacenar los expedientes del personal?	Nosotros utilizamos sheron también tenemos un sistema de Gestión de Talento Humano institucional para allí precautelar por ejemplo la información que tiene que ver con licencia de estudio, licencia por enfermedad todo un sinnumero de información recabada en la nube que también nos colabora con el acceso directo cuando necesitamos una información escaniamos el documento y eso se sube a la nube y es una carpeta compartida solo para personal autorizado.	Aquí en Talento Humano yo almaceno la información tanto físico como digitales, en los digitales utilizamos el Poe, el drive, también tenemos un punto físico que es archivo con todos los expedientes todas las carpetas de los funcionarios que eso lo maneja nuestros compañeros de archivo nadie puede ingresar sin autorización de la Directora.		Utiliza un sistema digital de la institución para guardar los expedientes del personal, y además emplea herramientas básicas de archivo que permiten ordenarlos, mantenerlos protegidos y facilitar su consulta cuando se los necesita en las actividades administrativas (Angarita y Prieto Taborda, 2025).	En el Departamento de Talento Humano los Participantes mencionan que utilizan para almacenar los expedientes del personal es la herramienta OneDrive.
5. ¿Con qué frecuencia se respalda la base de datos de empleados y dónde se guarda esa copia?	Tenemos una base de datos denominada plantilla y distributivo institucional esa base de datos esta respaldada solo por el ingeniero de sistema de talento humano el es quien precautela la información solamente el la puede editar ya que	Como le indico en el Área de archivo o por medios de OneDrive y solo personas autorizadas tienen el acceso.	No manejo yo es información.	El respaldo se inicia con el cuidado de los datos de empleados, y además se debe realizar cada día o cada semana según la actividad, guardándose en un servidor seguro o en un dispositivo externo que	Se menciona que respaldan la información por medio de OneDrive.

	esos ingresos son los que se realizan al ministerio de finanzas para pagos de roles entonces es el quien precautela esa información yo como directora tengo el acceso a visualizar mas no de ingresar ni hacer ningún movimiento y es almacenada en la nube también y en el sistema de gestión de Talento Humano.			permita mantener la información protegida (Uceda et al., 2024).	
6. ¿Ha vivido pérdida, daño o extravío de información en el último año? ¿Cómo se resolvió?.	No	En el mes que llevo aquí laborando no ósea la información si es un poco complicada talvez encontrarla porque manejamos mucha información de toda la Institución pero como tal siempre se encuentran la información.	No a pasado.	Las pérdidas de información pueden presentarse en el año, y además se solucionan mediante copias de respaldo, revisión de archivos afectados y recuperación de los datos necesarios para que las actividades institucionales continúen sin generar mayores inconvenientes (Valiente et al., 2023)	Se menciona que en este año no hubo perdida o extravío de Información.
7. ¿Existe un procedimiento escrito que indique paso a paso cómo recuperar	Están los manuales de procedimientos, el proceso que debe seguir de cada proceso corresponde a cada área específica ya entonces	Considero qué si porque aquí tenemos técnicos e ingenieros en sistemas que nos ayudan en cuanto a	No manejo esa parte	Existe un procedimiento escrito que explica paso a paso cómo recuperar información después de un fallo, y además	La Mayoría de los participantes dicen que no existe

información tras un fallo?	para manuales de fallo si existe y se encuentra en una parte que está ubicado en la parte de aseguramiento de calidad.	lo que es repartir archivos, tanto digitales como físicos.		indica quién participa, qué acciones se aplican y cómo usar las copias de respaldo para que los datos vuelvan a estar disponibles (Caicedo et al., 2024).	
8. ¿En cuánto tiempo estima que podrían restablecerse todos los datos si el servidor principal fallara hoy?	Eso depende de la gravedad de la información es decir si un equipo se llega a dañar tienes la posibilidad de 24 horas de recuperar la información.	Yo creo que nuestros compañeros de ingeniería en sistemas lo sepan manejar en reestablecer datos en dos horas más o menos.	Normalment e cuando regresa el internet se puede pero las personas que manejan los datos son dos compañeros.	El restablecimiento total podría tomar unas horas o un día, y además depende del volumen de los datos, la rapidez del respaldo y la coordinación del personal técnico que realiza la recuperación para que el sistema vuelva a operar con normalidad (Zambrano y Moreno Tamayo, 2024)	Se menciona que se puede restablecer enseguida.
9. ¿Se realizan auditorías internas de seguridad de la información? ¿Con qué periodicidad?	No	Ahora ultimo tuvimos un auditoria de parte de contraloría del ministerio de trabajo entonces creo que dos veces al año.	Es constante.	Se realizan auditorías internas de seguridad de la información, y además suelen efectuarse cada año o cada semestre para revisar los controles, identificar riesgos y asegurar que los procedimientos se mantengan correctos dentro de las actividades institucionales (Torres	Algunos Participantes mencionan que si se realizan las auditorias por o menos dos veces al año.

				y Reyes Cárdenas, 2025).	
10. ¿Qué beneficios percibiría si se implantara una Norma interna de seguridad y recuperación?	Si se mejorara sería dejar bien establecidos los puntos es decir tener documentos recuperables aunque no todo documento es recuperable ya que siempre abra información que sea más prioritaria o más tiempo tenerla que otra información que solo se emane en determinado año.	Sería de buena ayuda para la dirección pues como le indico si hay cosas que fortalecer dentro de lo que es el sistema.	Si hubiera otra sería de mucha ayuda para el departamento de Talento Humano.	Percibiría beneficios como un manejo más organizado de la información, y además contaría con pasos claros para atender fallos, disminuir riesgos y asegurar que los datos puedan recuperarse con rapidez dentro de las actividades institucionales (Pilamunga y Camero Berrones, 2025).	Los participantes mencionan que sería de mucha ayuda ya que la dirección de Talento Humano necesita fortalecer el sistema.
11. ¿Qué recursos (tecnológicos, económicos o humanos) faltarían para poner en marcha dicha Norma?	Mas scaner	Mas scaner .	Mas scaner .	Faltarían recursos como equipos tecnológicos actualizados, y además se requerirían fondos para su mantenimiento y personal capacitado que permita aplicar la Norma y mantener su funcionamiento dentro de las actividades institucionales (Coello, 2024)	Los Participantes mencionan que en los recursos hacen falta son scaner

12. ¿Está dispuesto a participar en simulacros de restauración de datos al menos una vez al año?	Si se llega a dar sería excelente de que las máquinas todas estén entrelazadas entonces una sola persona controlarlas para que se apague y todo es casi como usuario pero no se ve eso.	si	si	Es importante participar en simulacros de restauración de datos una vez al año, y además estas prácticas ayudan a tener mejor respuesta ante fallos y permiten cuidar la información dentro de las actividades de la institución (Ali et al., 2024).	Los participantes mencionan que si están dispuestos a participar en simulacros.
---	---	----	----	--	---

Elaborado por: Karina Lorena Calderón Vera

Análisis de Resultados

En relación con la entrevista realizada en el Departamento de Talento Humano de la Universidad Laica Eloy Alfaro de Manabí, la cual fue dirigida a la Directora, a la secretaria, al coordinador general, es importante destacar que:

Los entrevistados dieron a conocer que en los procesos que se llevan a cabo en el departamento de Talento Humano surge la necesidad de implementar una norma que ayude a recuperar la información sin embargo, mediante la realización de la entrevista se pudo conocer que no han recibido ningún tipo de capacitación sobre los principios de Confidencialidad, Integridad, y disponibilidad por parte de la Dirección de Talento Humano, siendo evidente que existe desconocimiento sobre el tema, incluso cuando este conocimiento forma parte de algo muy común en sus procesos encargados.

Además, se pudo indagar que su principal fuente de información que le permite el cumplimiento de sus labores diarias, es la información archivada o llegada en físico, y por otro lado también existe el uso de una herramienta que es utilizada en el departamento, de la cual algunos de los servidores cuentan con un acceso solo de visualización, dependiendo de su rol como servidor público.

Una de las preguntas que se realizó a los entrevistados fue como llevaban a cabo la seguridad de la información y qué tipo de seguridad utilizaban dentro del departamento de Talento Humano para respaldar los documentos, en la cual los entrevistados explicaron que su seguridad se basa en almacenar la información en la nube y que este proceso solo está encargado en dos servidores, para que de este modo la información no sufra ediciones no deseadas. Mientras que el resto de servidores públicos solo tienen acceso a esta como observador.

En una de las preguntas que se les formula se mencionan que no cuentan con capacitaciones y principalmente tienen desconocimiento de los principios fundamentales de la norma, como la Confiabilidad, Integridad, y disponibilidad de la Información. El diseño de esta norma requiere superar estas limitaciones mediante estrategias de capacitación integral, procesos claros y recursos que fortalezcan la seguridad de la información en la organización, alineando las percepciones y acciones del personal con los estándares establecidos.

Por ende, una organización o empresa debe tener conciencia que la información es un activo importante en la continuidad de los procesos. Por lo cual deberá establecer medidas que apoyen a garantizar su integridad, disponibilidad y confiabilidad ya que son principios muy importantes a tener en cuenta.

En el entorno universitario, la información acompaña cada decisión, trámite y vínculo que se construye entre personas e instituciones, por eso resguardarla no es un asunto secundario ni exclusivo de lo técnico. Lo importante es que se mantenga segura, sin accesos indebidos, sin cambios fuera de control y disponible justo cuando hace falta. Todo eso crea una base sólida para trabajar con confianza. Como recuerda (Solís, 2023), cuando estos principios se viven en serio dentro de la institución, se reducen los riesgos y los procesos mantienen su credibilidad.

En este sentido de acuerdo a lo señalado por (Solís, 2023) la información debe considerarse un activo muy importante para la continuidad del negocio, lo cual implica la necesidad de garantizar su integridad, disponibilidad y confidencialidad mediante un enfoque integral de seguridad de la información. Este enfoque supera los límites que tienen muchas organizaciones, que suelen centrarse únicamente en medidas de seguridad física, dejando al lado aspectos críticos relacionados con la protección de la información.

Conclusión

Se concluye que analizar una Norma de Seguridad para la Recuperación de la Información es necesaria para el Departamento de Talento Humano, debido a que esta guía ayuda a ordenar mejor las tareas, así como también, proteger los datos y organizar el trabajo de manera clara, permitiendo que el personal siga pasos simples y seguros en sus actividades diarias y evitando confusiones que afecten las labores del área, lo cual fortalece el manejo de la información y apoya una gestión más estable dentro de la institución.

OB.ESP.1. El diagnóstico evidenció debilidades en la gestión y recuperación de la información dentro del Departamento de Talento Humano, particularmente en la ausencia de procedimientos específicos y en la aplicación no uniforme de controles internos. Este hallazgo permitió identificar que la organización actual del manejo de datos no garantiza una respuesta estructurada ante posibles incidentes, lo que afecta la estabilidad operativa y la coordinación interna del área.

OBJ.ESP.2. La revisión técnica y normativa permitió constatar que, aunque existen reglamentos institucionales relacionados con la gestión documental y la seguridad, no se dispone de una norma específica que regule la recuperación de la información en el departamento. Esta situación demuestra una brecha entre el marco normativo general y la práctica operativa concreta del área, limitando la consolidación de un sistema formal de recuperación de datos.

OBJ.ESP.3. La investigación permitió diseñar una estructura documental que organiza los protocolos de prueba y restauración necesarios para el Departamento de Talento Humano, estableciendo lineamientos claros sobre responsabilidades, tiempos de actuación y mecanismos básicos de control. Con ello, se consolidó una base técnica que integra la recuperación de la información dentro de un esquema normativo específico para el área.

Recomendación

Se recomienda continuar con la validación de la Norma de Seguridad, con la finalidad de socializar la utilidad de su contenido al personal, lo cual es esencial para que entiendan cada paso y puedan aplicarlo sin dificultad, permitiendo organizar mejor las tareas diarias y creando hábitos sencillos que ayuden a proteger la información, lo cual también refuerza la responsabilidad del equipo y facilita que el departamento mantenga un orden claro y estable en sus actividades logrando una ejecución más segura del trabajo.

Se recomienda fortalecer los controles y mejorar los procesos de manejo de datos, y además es importante capacitar al personal en acciones simples que reduzcan riesgos y mejoren la respuesta ante fallos, permitiendo que el área mantenga sus actividades sin interrupciones y apoyando un trabajo más seguro cuando aparece algún problema en la información, lo cual también contribuye a que el personal actúe con más confianza y mantenga un ritmo estable en las tareas logrando una gestión más segura.

Se recomienda usar los criterios técnicos encontrados para formar un plan de trabajo claro, y además es conveniente escoger herramientas fáciles que apoyen el buen cuidado de la información, permitiendo que el personal adopte hábitos más seguros, estableciendo que el manejo de los datos sea más ordenado y confiable dentro de la institución, lo cual también favorece que las actividades se realicen con menos errores y que el equipo tenga una guía clara para su trabajo logrando un uso más responsable de la información.

Se recomienda aplicar los protocolos de prueba y restauración establecidos; además es útil realizar simulacros frecuentes que permitan revisar los resultados y mejorar la preparación del personal, permitiendo respuestas más rápidas ante fallos y ayudando a mantener un control

constante sobre la información institucional, lo cual también refuerza la seguridad del área y facilita que se actúe con más precisión logrando una recuperación más efectiva de los datos.

Referencia

- Ali, T., Al-Khalidi, M., & Al-Zaidi, R. (2024). Métodos de evaluación de riesgos de seguridad de la información en la computación en la nube: revisión exhaustiva. *Revista de sistemas de información informática*, 1(1), 13-25. <https://doi.org/10.1080/08874417.2024.2329985>
- Angarita, L. B., & Prieto Taborda, M. (2025). Desarrollo de un sistema de gestión de la información de la investigación basado en repositorios de conocimiento caso: Dirección de Investigación y Extensión de la Universidad Nacional de Colombia - Sede Manizales. *Revista Rcta*, 1(45), 8-14. <https://doi.org/10.24054/rcta.v1i45.3129>
- Armas, R., & Taherdoost, H. (2025). Construyendo una cultura de ciberseguridad en la educación superior: Proponiendo un paradigma de concientización sobre ciberseguridad. *Revista de Seguridad de la Información, Preservación de Datos e Informática Forense*, 16(5), 32-45. <https://doi.org/10.3390/info16050336>
- Ávila, A. (2024). Seguridad de la información en instituciones públicas: desafíos y buenas prácticas en el contexto ecuatoriano. *Journal of Economic and Social Science Research*, 4(2), 140-156. <https://doi.org/10.55813/gaea/jessr/v4/n2/96>
- Bonal, J., & Ortego, M. (2020). Los procesos de gestión de documentos en la Ley General de Archivos de México: análisis de contenido desde una perspectiva cuantitativa. *Investigación bibliotecológica*, 34(85), 9-12. <https://doi.org/10.22201/iibi.24488321xe.2020.85.58232>
- Borrero, J. M. (2024). *Planes de contingencia en la administración pública: fundamentos y prácticas efectivas*. Instituto Nacional de Gestión Pública.

- Borrero, J., Quintero, Y., & Álvarez, N. (2024). La seguridad de la información a través de la creación y restauración de las copias. *Journal TechInnovation*, 3(1), 71-85. <https://doi.org/10.47230/Journal.TechInnovation.v3.n1.2024.67-77>
- Cabrera, E., Zambrano, L., Mendoza, M., & Palma, G. (2020). El rol de la gestion documental y su impacto en la gestión de las instituciones educativas del Cantón Portoviejo. *Polo del Conocimiento*, 5(10), 515-538. <https://doi.org/10.23857/pc.v5i10.1830>
- Caicedo, N. L., Sánchez Quezada, J., & Chalá Cuadros, J. (2024). Gestión documental en el proceso de autoevaluación del Instituto Superior Tecnológico Tsa'chila, 2024. *Reincisol*, 3(6), 1505-1527. [https://doi.org/10.59282/reincisol.V3\(6\)1505-1527](https://doi.org/10.59282/reincisol.V3(6)1505-1527)
- Carrión, D. (2021). Instituciones resilientes para una recuperación transformadora pospandemia en América Latina y el Caribe: aportes para la discusión. *Revista de Información Documental*, 8(4), 13-19.
- Cedeño, S. (2024). Gestión documental en el criterio de docencia del Instituto Superior Tecnológico Tsachila. *Revista Reinacasol*, 3(6), 111-130. [https://doi.org/10.59282/reincisol.V3\(6\)1711-1730](https://doi.org/10.59282/reincisol.V3(6)1711-1730)
- Coello, A. A. (2024). Seguridad de la información en instituciones públicas: desafíos y buenas prácticas en el contexto ecuatoriano. *Innovación Social y Respuestas Económicas*, 4(2), 18-25. <https://doi.org/10.55813/gaea/jessr/v4/n2/96>
- Core, L. (2024). Seguridad de archivos en el proceso de autoevaluación del Instituto Superior Tecnológico Tsáchila, 2024. *Reincasol*, 9(3), 7-13. [https://doi.org/10.59282/reincisol.V3\(6\)1505-1527](https://doi.org/10.59282/reincisol.V3(6)1505-1527)

- Cuenca, B., Barona, M., & Sánchez, V. (2024). Estudio sobre cómo la transparencia en los procesos de contratación pública puede mejorar la eficiencia y reducir la corrupción. *Ciencia Latina Sociales y Humanas*, 8(4), 13-21. https://doi.org/10.37811/cl_rcm.v8i4.13144
- Delgado, J. (2024). Entorno seguro documental en entidades públicas: buenas prácticas en los departamentos públicos. *Desarrollo Documental*, 4(2), 140-156.
- Domínguez, R., Flores, O., & López, J. (2023). Evaluación de un sistema de gestión de seguridad de la información en una institución de educación superior mexicana. *Arxiv*, 3(1), 3-6. <https://doi.org/10.48550/arXiv.2306.11050>
- Estacio, C. (2024). La gestión documental: automatización y comunicación efectiva como factores clave. *Aula Virtual*, 5(12), 5-9. <https://doi.org/10.5281/zenodo.14834090>
- Garavito, Y. y. (2022). Cultura organizacional y cultura de seguridad: una revisión de la literatura. *Revista Colombiana de Salud Ocupacional*, 12(2), 1-11. <https://doi.org/10.18041/2322-634X/rcso.2.2022.8622>
- García, C., & Hervás, M. (2020). Los sistemas de evaluación de la Educación Superior en México y España. Un estudio comparativo. *Revista de la educación superior*, 49(194), 31-47. <https://doi.org/10.36857/resu.2020.194.1127>
- Haro, E., & Silva, J. (2022). Backups inmutables orientado a la implementación en servidores no virtualizados críticos de la Dirección de Tecnologías de Información y Comunicación de la Unach. *Revista de Sistema Documental*, 7(3), 31-47.
- Javier Cantos. (2023). Guía para la Implementación del EGSI. *Ministerio de Telecomunicaciones y de la Sociedad de la Información de Ecuador*, 8(1), 31-48.

- Mendoza, A. (2022). Anaálisis de seguridad y recuperación documental en universidades públicas. *Revista Iberoamericana de Documentación*, 14(2), 55-70.
- Menendez, C. Q., & Moreira Sánchez, W. (2025). Seguridad y privacidad de los datos en la era de la información en el Ecuador. *Ingeniería aplicada a problemas de la sociedad actual*, 7(2), 28-45. <https://doi.org/10.53358/ideas.v7i2.1287>
- Mora, J. P. (2020). Gestión de la seguridad de la información en entornos organizacionales. Editorial Académica.
- Mora, J. y. (2020). El sistema de gestión de seguridad de la información bajo la norma NTE ISO/IEC 27001 en instituciones de Educación Superior (Ecuador). *Roca - Revista Científico - Educaciones de la provincia de Granma*, 16(1), 546-559.
- Pacotaípe, R., & Rondon, O. (2024). Experiencias del Servicio Digital en Gestión Documentaria de las Instituciones Educativas Públicas del Perú. *Revista Docentes 2.0*, 17(2), 258–267. <https://doi.org/10.37843/rtd.v17i2.506>
- Palacios, L. (2022). Gestión documental basada en la norma ISO 15489 en procesos de autoevaluación institucional. *Revista Científica CienciAmérica*, 11(2), 142–155.
- Pilamunga, X. E., & Camero Berrones, R. (2025). Políticas de seguridad de la información según la norma iso 27001 para el municipio de Guaranda, Bolívar, Ecuador. *593 Digital Publisher CEIT*, 10(3), 340-351. <https://doi.org/10.33386/593dp.2025.3.3134>
- Saleh, M. O. (2021). *Barreras organizacionales en la recuperación de información institucional*. Fondo Editorial Público.

- Saleh, S., Nakshabandi, O., Zeebaree, M., & Aqel, M. (2021). Barreras organizacionales que enfrentan la implementación del gobierno electrónico: el marco de implementación del gobierno electrónico. *Government Information Quarterly*, 39(7), 8-18. <https://doi.org/10.25115/eea.v39i7.5231>
- Sánchez, A. (2022). Estado actual de las tecnologías de la información y comunicación en las Instituciones de Educación Superior en México: estudio 2022. *Revista de Gestión Documental*, 2(1), 7-13.
- Segura, V. T., & Jorge Wilson, T. (2025). Ciberseguridad y protección de datos. *Revista Científica Arbitrada de Investigación en Comunicación, Marketing y Empresa*, 8(16), 7-19. <https://doi.org/10.46296/rc.v8i16.0381>
- Solís, M. R. (2023). Seguridad de la información en instituciones universitarias: fundamentos y desafíos emergentes. *Retos Pendientes*, 2(2), 113-142.
- Tapia, R. (2024). Mejora de gestión documental - Revisión sistemática. *Revista Electrónica Multidisciplinaria de Ciencias Básicas*, 6(11), 8-14. <https://doi.org/10.35381/i.p.v6i11.4076>
- Timal, S. (2023). La construcción de archivos públicos base de la transparencia: los retos de la gestión pública. *Vinculatégica EFAN*, 9(5), 69–85. <https://doi.org/10.29105/vtga9.5-422>
- Torres, J. P., & Reyes Cárdenas, N. (2025). El impacto de la auditoría interna en la mejora de procesos contables en empresas manufactureras. *Revista Multidisciplinaria Perspectivas Investigativas*, 5, 597–608. <https://doi.org/10.62574/rmpi.v5ieconomica.429>

- Trujillo, P. (2025). Factores críticos de éxito en la gestión de proyectos tecnológicos en instituciones públicas y privadas. *Revista Científica Multidisciplinar*, 2(3), 58-75. <https://doi.org/10.63969/9z9h0k82>
- Uceda, M. A., Varas Zurita, P., & Mendoza De Los Santos, A. (2024). Análisis de Seguridad de Bases de Datos: Estrategias para la Protección de Datos. *Ingeniería: Ciencia, tecnología E innovación*, 11(1), 9-18. <https://doi.org/10.26495/kz3kyz70>
- Valiente, M. J., Hermes Castillo Sarmiento, J., & Mendoza De Los Santos, A. (2023). Seguridad de la información en la prevención de pérdida de datos: una revisión sistemática. *Innovación y software*, 4(2), 182-200. <https://doi.org/10.48168/innosoft.s12.a92>
- Vega, D. D., Burgos Ramírez, K., Loja Mora, N., & Loján Alvarado, H. (2025). Gestión de riesgos para el tratamiento de datos personales sensibles en el movimiento de mujeres de El Oro. *Revista Científica Arbitrada Multidisciplinaria*, 7(3), 9-18. <https://doi.org/10.59169/pentaciencias.v7i3.1505>
- Zaki, H., & Robbins, S. (2024). La influencia de la ciberseguridad en las prácticas legales y los estándares éticos de recursos humanos. *Revista de Gestión de Información*, 2(1), 4-8. <https://doi.org/10.13140/RG.2.2.12047.60321>
- Zambrano, C., & Mendoza, A. (2023). Propuesta metodológica para la evaluación de la seguridad de información en software de gestión académica. *Publicaciones Uleam*, 7(2), 18-25. <https://doi.org/10.56124/encriptar.v8i15.002>
- Zambrano, H. R., & Moreno Tamayo, C. (2024). Seguridad de la información y ciberseguridad: su importancia para los Estados, empresas y las personas, una revisión sistemática. *Estudios*

Y Perspectivas Revista Científica Y Académica, 4(1), 11-25.

<https://doi.org/10.61384/r.c.a..v4i1.90>

Anexo # 1 Evidencias fotográficas de la entrevista realizada en la dirección de Talento Humano de la Universidad Laica Eloy Alfaro de Manabí.

Ilustración 1.

Evidencia de la Entrevista a la directora del Dirección Talento Humano de la ULEAM.



Nota: En la ilustración se muestra evidencias fotográficas y documentos del proceso de entrevista realizada al personal de la dirección de Talento Humano de la Universidad Laica Eloy Alfaro de Manabí como muestra de recolectar Información para el presente estudio.

Elaboración propia

Ilustración 2.

Evidencias de la entrevista a la Secretaría de la Dirección de Talento Humano de la ULEAM.



Nota: En la Ilustración se observa claramente el proceso de la entrevista y su propósito al personal de la dirección de Talento Humano de la Universidad Laica Eloy Alfaro de Manabí.

Elaboración propia.

Anexos

Anexo #2 Evidencia de la Guía de Observación

Tema: Seguridad y Recuperación de la Información en la Dirección de Talento

Humano – ULEAM

Observador: Karina Lorena Calderón Vera

Fecha: ____ / ____ / 2025

Lugar: Dirección Administrativa de Talento Humano – ULEAM – Manta

Categoría: Seguridad y Recuperación de la Información

Nº	Pregunta de Observación	Sí / No		Observaciones
1	¿Existe un inventario actualizado que identifique la información crítica (eg, nóminas, contratos, expedientes) que debe ser objeto de recuperación?	☐ Sí	☐ No	
2	¿La información crítica (física y digital) está clasificada, etiquetada y protegida según su nivel de sensibilidad (pública, interna, confidencial)?	☐ Sí	☐ No	
3	¿Existen controles físicos o digitales que limitan el acceso a la información crítica y a los medios de resguardo solo al personal autorizado?	☐ Sí	☐ No	
4	¿Está documentado y difundido el procedimiento estándar para realizar las copias de respaldo (backup), incluyendo la frecuencia y el tipo de respaldo (completo, incremental diferencial)?	☐ Sí	☐ No	
5	¿Se realiza el respaldo de la información crítica con la frecuencia definida como necesaria para el departamento (eg. diario)?	☐ Sí	☐ No	
6	¿Se utilizan medios de almacenamiento idóneos (ej. nube, NAS, discos externos) y se almacena una copia de los respaldos en una ubicación externa o segura, alejada del sitio principal (política 3-2-1)?	☐ Sí	☐ No	
Categoría seguridad del respaldo				
Nº	Pregunta de Observación	Sí / No		Observaciones
7	¿Los medios de resguardo están protegidos contra el acceso no autorizado, daño físico o malware ¿cifrado, aislamiento físico)?	☐ Sí	☐ No	
8	¿Existe un protocolo de restauración claramente documentado que especifique los pasos a seguir para recuperar la información tras un incidente?	☐ Sí	☐ No	
9	¿Se realizan pruebas de restauración de manera periódica y documentada, y se registra la evidencia del éxito en la recuperación de los datos (validación de la confiabilidad)?	☐ Sí	☐ No	
10	¿Están definidos los responsables técnicos y administrativos que deben ejecutar el procedimiento de recuperación y quién autoriza la restauración de los datos?	☐ Sí	☐ No	
11	¿Se tiene un conocimiento empírico o estimado sobre el tiempo que tarda la restauración completa de la información más crítica del Departamento?	☐ Sí	☐ No	

Anexo #3 Evidencias de la entrevista realizada en la dirección de Talento Humano de la Universidad Laica Eloy Alfaro de Manabí.

Tema: Seguridad y Recuperación de la Información en la Dirección de Talento Humano – ULEAM.

Entrevistador: Karina Lorena Calderón Vera

Fecha: ____ / ____ / 2025

Lugar: Dirección Administrativa de Talento Humano – ULEAM – Manta

Categoría: Seguridad y Recuperación de la Información

Preguntas para la entrevista	✓ Fundamentar teóricamente la seguridad de la información
-------------------------------------	--

1. ¿Qué entiende por “seguridad de la información” aplicada al sector público universitario?

.....

2. ¿Qué diferencia existe entre confidencialidad, integridad y disponibilidad de los datos?

.....

3. ¿Ha recibido capacitación formal sobre estos tres principios? ¿En qué consistió?

.....

Estado actual de la seguridad y recuperación

4. ¿Qué sistema o herramienta utiliza para almacenar los expedientes del personal?

.....

5. ¿Con qué frecuencia se respalda la base de datos de empleados y dónde se guarda esa copia?

.....

6. ¿Ha vivido pérdida, daño o extravío de información en el último año? Cómo se resolvió.

.....

7. ¿Existe un procedimiento escrito que indique paso a paso cómo recuperar información tras un fallo?

.....

8. ¿En cuánto tiempo estima que podrían restablecerse todos los datos si el servidor principal fallara hoy?

.....

9. ¿Se realizan auditorías internas de seguridad de la información? ¿Con qué periodicidad?

.....

Propuesta de mejora (Norma)

10. ¿Qué beneficios percibiría si se implantara una Norma interna de seguridad y recuperación?

.....

11. ¿Qué recursos (tecnológicos, económicos o humanos) faltarían para poner en marcha dicha Norma?

.....

12. ¿Está dispuesto a participar en simulacros de restauración de datos al menos una vez al año?

.....

Propuesta de solución

Guía para el fortaleciendo de las aplicaciones de las políticas de seguridad para la recuperación de la información en la Dirección Administrativa de Talento Humano de la Universidad Laica Eloy Alfaro de Manabí, Manta 2025.

Esta propuesta de solución se plantea como un apoyo para ordenar y dar mayor claridad a la aplicación de las políticas institucionales relacionadas con la seguridad y recuperación de la información en la Dirección Administrativa de Talento Humano de la Universidad Laica Eloy Alfaro de Manabí, dado que permite orientar al personal sobre cómo actuar frente a situaciones que puedan afectar los datos y, a su vez, unificar criterios para el respaldo y la recuperación de la información, de manera que las actividades diarias se desarrollen con mayor organización y coherencia, mientras se refuerza la responsabilidad en el manejo de los archivos y, al mismo tiempo, se mantiene coherencia con la normativa vigente y el funcionamiento institucional.

Tema:

Fortalecimiento de la aplicación de las políticas institucionales de seguridad para la recuperación de la información en la Dirección Administrativa de Talento Humano de la Universidad Laica Eloy Alfaro de Manabí, Manta 2025.

Objetivo general

Fortalecer la aplicación de las políticas institucionales de seguridad y recuperación de la información en la Dirección Administrativa de Talento Humano, mediante lineamientos operativos claros.

Objetivos específicos

Identificar la forma en que se aplican las políticas de seguridad y recuperación de la información en el área de Talento Humano.

Establecer lineamientos básicos para el respaldo y la recuperación de la información.

Definir responsabilidades generales del personal en el manejo de la información.

Descripción de la propuesta

La propuesta se presenta como una guía interna para ordenar cómo se aplican las políticas institucionales de seguridad y recuperación de la información en la Dirección Administrativa de Talento Humano, puesto que en el trabajo diario se requiere saber con claridad cómo actuar cuando surgen fallos o riesgos en los datos y, además, contar con criterios compartidos que faciliten el respaldo y la recuperación de la información, de manera que se unifiquen las formas de trabajo, se aclaren responsabilidades y se mantenga la continuidad de los procesos, mientras se respeta la normativa vigente y se promueve un manejo más cuidadoso de la información institucional.

Para lo cual se sugieren las siguientes estrategias en función de cada objetivo planteado en la propuesta.

Objetivo específico 1:

Identificar la forma en que se aplican las políticas de seguridad y recuperación de la información en el área de Talento Humano.

Planificación de la propuesta de una guía interna

OBJETIVO	ACTIVIDAD	DESCRIPCIÓN	TIEMPO	RESPONSABLE	META
Identificar la forma en que se aplican las políticas de seguridad y recuperación de la información en el área de Talento Humano	Revisión de políticas institucionales	Revisar las políticas institucionales relacionadas con la seguridad y recuperación de la información, para conocer cómo se aplican en el área de Talento Humano y, además, reconocer qué lineamientos se utilizan en el trabajo diario.	1 mes	Dirección de Talento Humano	Conocer las políticas que se aplican en el área.
	Observación de los procesos documentales	Observar cómo se maneja la información en las actividades diarias y, a la vez, identificar de qué forma se realizan el respaldo y la recuperación de los documentos.	1 mes	Personal administrativo	Identificar la forma real en que se aplican las políticas.
Establecer lineamientos básicos para el respaldo y la recuperación de la información	Definición de lineamientos operativos	Definir lineamientos sencillos que orienten el respaldo y la recuperación de la información, tomando en cuenta las políticas institucionales y, además, las actividades que realiza el área.	2 meses	Analista de Gestión Documental	Contar con lineamientos claros para el área.
	Socialización de lineamientos	Dar a conocer los lineamientos al personal del área, de manera que sepan cómo actuar cuando se presenten problemas con la información.	1 mes	Dirección de Talento Humano	Personal informado sobre los lineamientos.
Definir responsabilidades generales del personal en el manejo de la información	Identificación de roles del personal	Identificar las funciones que cumple el personal en relación con el manejo, respaldo y recuperación de la información, considerando las tareas que realiza cada servidor.	1 mes	Dirección de Talento Humano	Roles identificados dentro del área.
	Asignación de responsabilidades	Asignar responsabilidades generales al personal, para que cada servidor conozca su papel en el cuidado y recuperación de la información institucional.	1 mes	Dirección de Talento Humano	Responsabilidades claras y comunicadas.