Universidad CENFOTEC

Escuela de Ciberseguridad

DISEÑO DE UNA ESTRUCTURA DE SEGURIDAD PARA EXPEDIENTES DIGITALES DEL ICAP

PROYECTO DE INVESTIGACIÓN PARA OPTAR POR EL TÍTULO DE MAESTRÍA EN CIBERSEGURIDAD

Sustentante:

Grettel Rivera Rojas

Septiembre, 2022

Declaratoria de Derechos de autor

La suscrita, Grettel Rivera Rojas, estudiante de la Universidad Cenfotec DECLARO que soy autora intelectual de la investigación titulada: Diseño de una estructura de seguridad para Expedientes Digitales del ICAP, fundamento que los capítulos del 1 al 5 tienen la literatura citada con su respectiva referencia con el fin de preservar los derechos de autor de las diferentes fuentes bibliográficas consultadas. Asimismo, autorizo la reproducción total o parcial, con fines académicos, por cualquier medio o procedimiento, incluyendo la cita bibliográfica del documento. Es todo. Firmo en San José el_05_de_noviembre_de 2022.

Grettel Rivera Rojas

Dedicatoria

Esta investigación la dedico a Gabriel Mora, la persona que más me apoyó para llegar al final de la meta, quien me mostró cómo mi resiliencia podía ayudarme a superar los momentos de frustración y desánimo. Él me brindó palabras de aliento y me escuchó en cada momento que necesité cuando estaba estudiando mi maestría. Al creer en mí antes de que yo lo hiciera, él apoyaba mi crecimiento profesional y también me incentivaba a crecer más personalmente. Por su valentía y perseverancia conmigo y en su vida, vaya este pequeño pero significativo homenaje.

Agradecimiento

Agradezco a mis papás, ya que son la razón de que siempre pensara en un mejor futuro para mí. Ellos me han guiado siempre en la labor de crecer en valores y ética.

A mi hermano que fue muy colaborativo con la estructura de la citación de fuentes y me brindó material de apoyo para crear el capítulo 3 de esta investigación.

A mi profesor tutor, el master Roy Valenciano, porque me proporcionó enlaces para la investigación, me tuvo paciencia y me acompañó durante mucho más del tiempo imaginado que tomaría hacer esta investigación.

Finalmente, agradezco a mi hermana y a mis mejores amigos y amigas pues tomaron el tiempo para demostrar su preocupación ante mis necesidades personales y me apoyaron para seguir adelante y así llegar a la meta de la conclusión de una maestría que es destacable ante muchas otras.

TRIBUNAL EXAMINADOR

Este proyecto fue aprobado por el Tribunal Examinador de la carrera: **Maestría Profesional en Ciberseguridad,** requisito para optar por el título de grado de **Maestría,** para el estudiante: **Rivera Rojas Grettel Eugenia.**

Firmado digitalmente por ROY VALENCIANO GONZALEZ (FIRMA)
Fecha: 2022.11.07 15:21:50 -06'00'

M. Sc. Roy Valenciano González
Tutor

JOSE DAVID IBARRA QUESADA (FIRMA)
Firmado digitalmente por JOSE DAVID IBARRA QUESADA (FIRMA)
Fecha: 2022.11.07 09:04:05 -06'00'

MSEG. José David Ibarra Quesada
Lector 1

IGNACIO TREJOS ZELAYA (FIRMA)
Firmado digitalmente por IGNACIO TREJOS ZELAYA (FIRMA)
Fecha: 2022.11.11 18:39:21 -06'00'

M. Sc. Ignacio Trejos Zelaya
Lector 2

Tabla de contenido

Índice de figuras

Índice de tablas

Abstract

La investigación trata acerca de todo el proceso para diseñar la estructura de seguridad de los expedientes digitales para el Instituto Centroamericano de Administración Pública (ICAP) para solventar los problemas de falta del control sobre la confidencialidad de los datos, canales inapropiados de distribución, dudas sobre la integridad de los documentos electrónicos que vayan a conformar los expedientes digitales, accedidos por usuarios del área Administrativa, Financiero y Contable y de Tecnologías de la Información.

La pesquisa trata temas como formas de almacenamiento seguro, hace referencia a bases de datos relacionales y no relacionales; asuntos de políticas de seguridad de la información, normativas de respaldo y políticas de control se seguridad física. También, trata sobre cuestiones relacionadas con la autenticación, autorización, integridad, no repudio y disponibilidad para los documentos electrónicos y a su vez para los expedientes electrónicos y otros relacionados a seguridad de la información.

Durante la investigación, se llegan a conocer aspectos relacionados con el ciclo de vida que debe seguir un expediente electrónico desde el inicio. Adicional a ello, se sugiere implementar buenas prácticas para la implementación y gestión del expediente digital.

En medio de la investigación, también se aborda otros complementos de la plataforma de Office 365 que se pueden emplear para fortalecer la estrategia de seguridad de los expedientes digitales, entre ellos las etiquetas de sensibilidad, pérdida de datos y resistencia de datos multigeográfica.

Además, se considera esta investigación como muy innovadora, pues al momento de hoy, ninguna institución en el territorio nacional de índole intergubernamental, ni otra institución dedicada a dar formación técnica, capacitación o enseñanza superior, ha hecho un diseño para sus expedientes digitales considerando la seguridad de estos. También, es innovadora porque va a proporcionar una línea base para seguridad de la información al ICAP.

Palabras clave: expedientes digitales, estructura de seguridad, indexación de documentos, información electrónica, documentos electrónicos, visualización de documentos, integridad de documentos, bitácora electrónica.

Capítulo 1. Introducción

1.1 Generalidades

El presente estudio pretende mostrar información realista y a la vez representativa de la institución en estudio; no obstante, al tratarse de una investigación aplicada y a solicitud del cliente, se han de simular datos con el fin de preservar la confidencialidad del ente en cuestión.

1.2 Antecedentes del problema

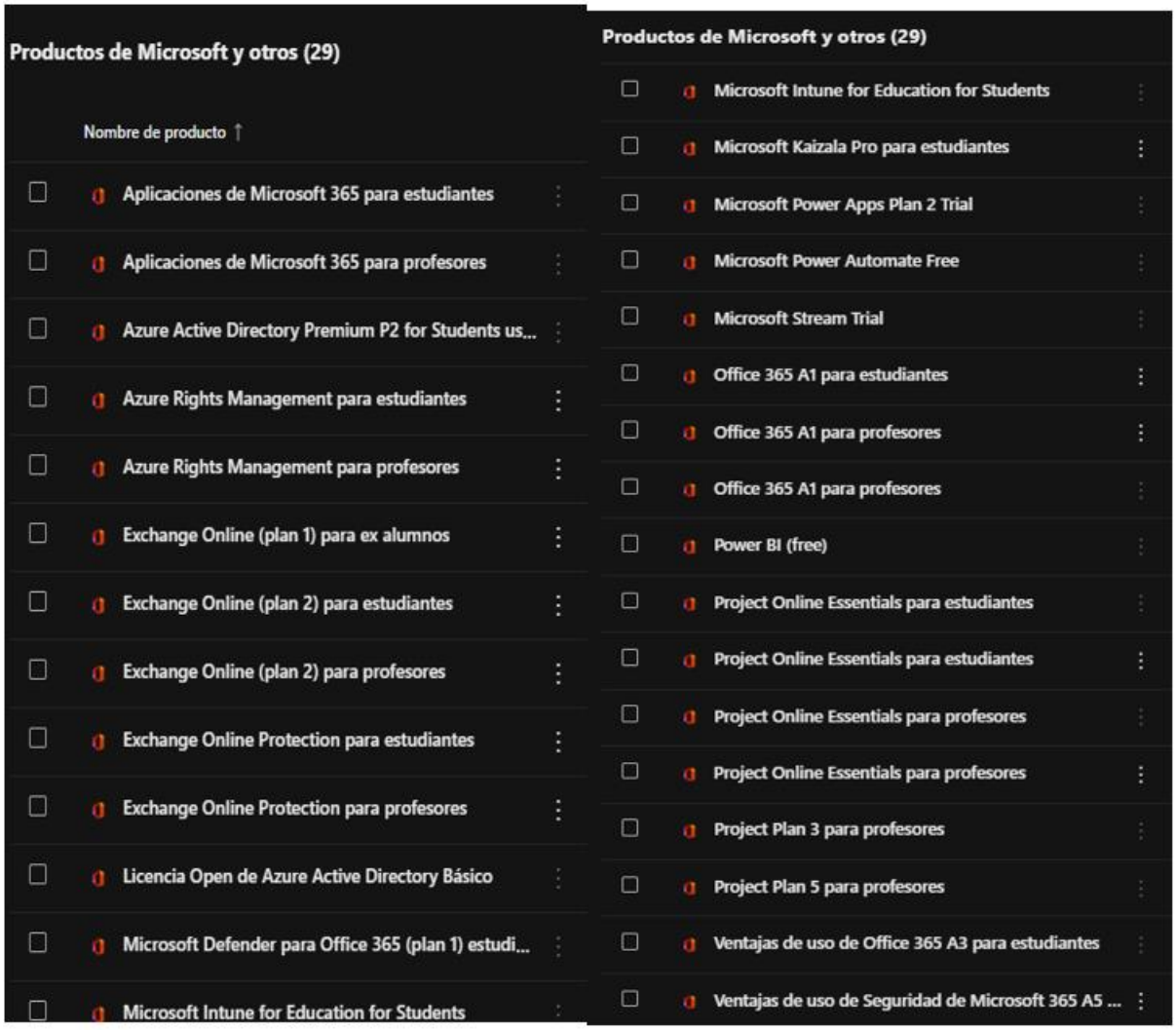
Con base en la problemática que se está por describir, cabe destacar lo siguiente: la información se accede desde la nube, muchos documentos son creados o cargados a carpetas que se pueden encontrar en páginas creadas en el *SharePoint Online* o bien en *el OneDrive*.

Además, la organización desde hace 4 años cuenta con licencias de Microsoft para trabajar en la nube, entre las plataformas que han tenido acceso está el *Active Directory*, en el cual tenían configurados todos los usuarios de la organización y algunos profesores. Poco a poco, la organización fue migrando la infraestructura de administración de usuarios y documentos a los servicios en la nube.

La licencia actual con la que cuenta la organización es Office 365 para centros educativos plan A3 que incorpora *OneDrive, SharePoint*, Teams y otros servicios. El plan A3 tiene las ventajas de que también ofrece el plan A1 para estudiantes y profesores. Además, el plan ofrece a los usuarios la posibilidad de instalar las aplicaciones de escritorio de Office 365 en hasta 5 computadoras personales (PC por sus siglas en inglés) con Sistema Operativo de Windows o en 5 computadoras Mac, 5 tabletas y 5 teléfonos (para saber más información acerca de los planes existentes de Microsoft y los productos integrados ver el Anexo 7).

Figura 1

Productos de Microsoft que puede acceder el ICAP



Nota: Adaptado de *Productos de Microsoft disponibles para el ICAP*, 2022, 4ta entrevista realizada al Gerente de UTIC del ICAP.

De este modo y conociendo el plan de la organización, se sabe que en *OneDrive* como en *SharePoint*, los usuarios pueden trabajar colaborativamente, en *SharePoint*, se han creado sitios en los cuales se han definido una serie de restricciones con los grupos de seguridad, ya sea que pueda tener visibilidad de la existencia de las carpetas o que no; también hay otros permisos de lectura y de escritura asignados a lo documentos en las carpetas. No obstante, no han existido otros mecanismos de seguridad que protejan los documentos electrónicos y nunca se ha contratado personal externo o empresa alguna para encargarse de la seguridad de la información en el ICAP.

Cabe decir que no hay una restricción a la intranet (el *SharePoint Online*) por direcciones IP o zonas geográficas, a pesar de que el acceso usualmente es

desde las oficinas en Curridabat, pero que de igual manera el acceso se hace desde cualquier lugar remoto.

1.3 Definición y descripción del problema

La problemática identificada para esta investigación trata acerca de la seguridad de la información que albergan los documentos electrónicos en el ICAP y, por tanto, aquellos que van a conformar los expedientes de los profesores. En estos, los datos personales o sensitivos tienen insuficiencia de controles aplicados de seguridad, como que no se aplican las etiquetas de datos sensibles, no se analizan los datos contra amenazas, no se firman los documentos, se comparten con usuarios fuera de la organización sin seguir restricciones de compartir o bien usando los canales no aptos para compartir, los controles de la información en estado físico no se auditan y tampoco hay suficientes lectores para tarjetas de acceso. A raíz de esto, se incrementa el riesgo de pérdidas de datos, acceso no autorizado, distribución a usuarios no autorizados y/o innecesarios, falta de validación sobre la integridad de los documentos y otros problemas.

Ahora bien, es una realidad tecnológica que estamos en la era de la transformación digital, la cual está haciendo que las empresas vayan migrando a medios electrónicos la información completada a mano, así como formularios impresos, las *curricula vitae*, las facturas y otros documentos físicos. De manera que la información puede estar más segura, centralizada y accesible desde cualquier parte. Así es como los centros de formación y/o de capacitación técnica no son una excepción a la regla y para continuar en la evolución de los procesos, también han de integrarse pasos que lleven a las acciones de transformación digital, empezando por los expedientes digitales.

Cabe mencionar que los expedientes digitales correspondientes a documentos de archivo, de acuerdo con la norma internacional ISO 15489-1 (2001):

> Los documentos de archivo contienen información que constituye un preciado recurso y un importante activo de la organización. La adopción de un criterio sistemático de la gestión de documentos de archivo resulta esencial para las organizaciones a la hora de proteger y preservar los documentos como evidencia de sus actos. Un sistema de gestión de

> documentos de archivo se convierte en una fuente de información sobre las actividades de la organización, que puede servir de apoyo a posteriores actividades y toma de decisiones; al tiempo que garantiza la asunción de responsabilidades frente a las partes interesadas presentes y futuras (p.5).

También esta norma indica que un procedimiento de gestión de documentos debería producir documentos de archivo fidedignos que reúnan las características de autenticidad, fiabilidad, integridad y disponibilidad, las cuales a la fecha no se están consiguiendo al 100%.

1.4 Justificación

Por las razones citadas anteriormente, la investigación indica que a las instituciones de formación y/o de capacitación técnica les hace falta mejorar o bien crear sistemas de gestión de documentación electrónica confiables. De modo que se plantea diseñar la estructura de seguridad necesaria para que los documentos de los expedientes electrónicos cumplan con las características de un documento de archivo y esté presente la seguridad en todo el ciclo de vida de los expedientes.

1.5 Viabilidad

1.5.1 Punto de vista técnico.

Desde el punto de vista técnico, esta investigación es viable ya que existen las herramientas tecnológicas que pueden servir de base para la creación de la estructura que se desea diseñar, así como para el cumplimiento de cada uno de los objetivos específicos de este proyecto. Se cuenta con los conocimientos técnicos requeridos a través de la formación adquirida en los cursos de Seguridad de datos almacenados, Análisis y evaluación de riesgos, Detección de vulnerabilidades, entre otros. También, está presente la capacidad para evaluar las herramientas y tecnologías actuales y para seleccionar el medio de almacenamiento más adecuado que garantice la integridad, disponibilidad y confiabilidad de los datos incluidos en cada expediente digital.

1.5.2 Punto de vista operativo.

Desde el punto de vista operativo, esta investigación es viable, ya que es de interés para la institución que el personal administrativo y el personal administrativo de TI, cuenten con una estrategia de seguridad de los expedientes digitales que permita administrarlos de manera segura, dando por sentado que la institución tendrá una estructura de expedientes digitales, la cual proporciona confidencialidad, integridad y disponibilidad de estos.

Asimismo, se cuenta con la posibilidad de obtener las licencias de los sistemas que se recomendarán y el tiempo adecuado para dar una solución al problema, así como que parte del personal de la institución llegue a involucrarse en el proyecto. También, se dispone de los recursos de información y software para poder llevar a cabo lo que se vaya requiriendo para hacer una propuesta de solución a la situación identificada.

1.5.3 Punto de vista económico.

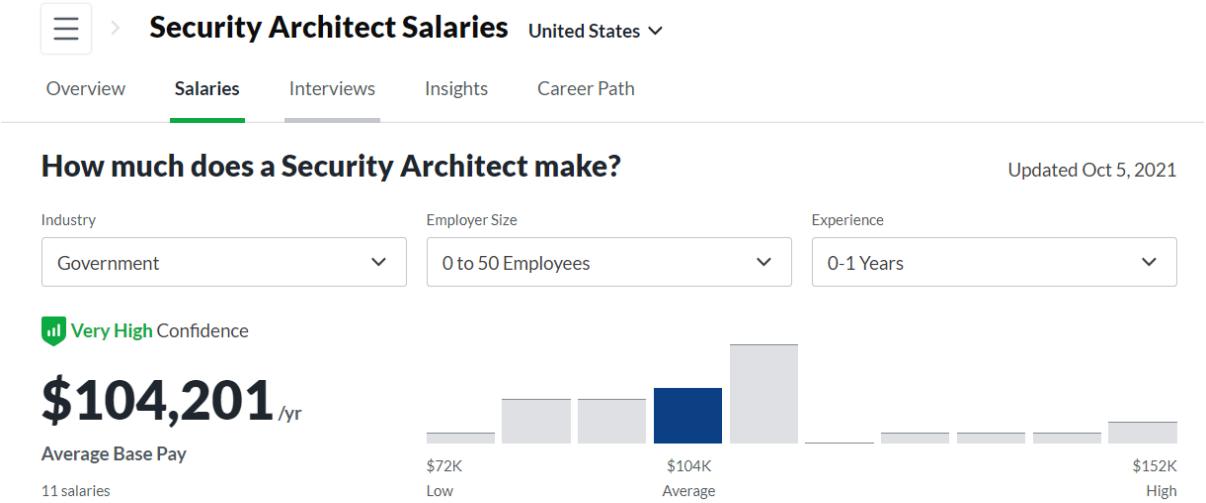
La hora de la consultora dedicada a la investigación aplicada será gratuita por lo que no se incurre en gastos económicos por el tiempo de planificación y diseño. Tampoco, se requiere inversión adicional en licencias o derechos de uso de software, pues solo se está planteando el diseño de una estructura de seguridad de la información de expedientes digitales, especializados para centros de formación superior y/o capacitación técnica.

Por otro lado, se ha de indicar un costo teórico que corresponde al cálculo de horas trabajadas, tomando en cuenta el salario promedio anual de un Arquitecto de seguridad o bien de un Arquitecto en Seguridad de la Información en una empresa pequeña con un año de experiencia.

La Figura 2 muestra el salario promedio anual de un Arquitecto de Seguridad en Estados Unidos, para Costa Rica no se encuentra disponible esta información en Glassdoor, no obstante, la mayoría de los salarios en empresas privadas llegan a hacer la tercera parte de un salario en Estados Unidos.

Figura 2

Salarios de Arquitectos de Seguridad en Estados Unidos de Glassdoor.



Nota: La imagen representa los salarios anuales de profesionales Arquitectos de Seguridad que tienen entre 0 a un año de experiencia y que laboran en empresa de hasta máximo 50 empleados. Adaptado de *Salarios de Arquitectos de Seguridad*, 2021, Glassdoor (https://www.glassdoor.com/Salaries/security-architect-salary-SRCH_KO0,18.htm).

Dada la información anterior, se puede analizar que el salario anual aproximado de un Arquitecto en Seguridad que logra llegar a tener un año de experiencia en una empresa pequeña puede ser de aproximadamente de $35000 anuales; no obstante, más fuentes de este valor deben ser requeridas para hacer un mejor análisis, porque la muestra que se tomó aún es pequeña para determinar de forma más precisa dicho aproximado.

La Figura 3 muestra un promedio del salario anual de un Arquitecto en Seguridad de la Información en Estados Unidos, tiene un mínimo de $75 500 y un máximo de $181 000. El promedio para los trabajadores en esta área teniendo entre uno y cinco años de experiencia sería de $122000 al año.

Figura 3

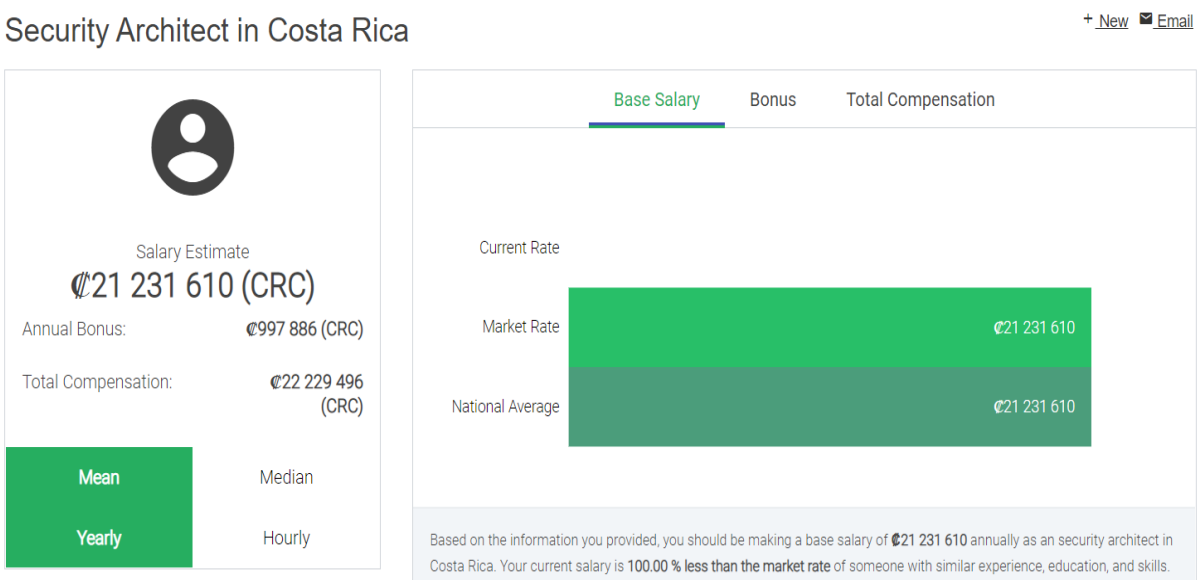
Salarios de Arquitectos en Seguridad de la Información en Estados Unidos de LinkedIn

Nota: La imagen representa los salarios anuales de profesionales Arquitectos en Seguridad de la Información con una media en el valor total de la compensación por $122000 anuales. Adaptado de *Salarios Anuales de Arquitectos en Seguridad*, 2021, LinkedIn (https://www.linkedin.com/salary/search?countryCode=xx&geoId=103644278&keywords=Information%20Security%20Architect).

La Figura 4 muestra el salario promedio anual de un Arquitecto de Seguridad en Costa Rica de acuerdo con datos del Instituto de Investigación Económica.

Figura 4

Salarios de Arquitectos de Seguridad en Costa Rica



Nota: La imagen muestra las compensaciones totales anuales como de bonus anuales de profesionales Arquitectos de Seguridad en Costa Rica. Adaptado de *Salarios de Arquitectos en Seguridad en Costa Rica*, por Instituto de Investigación económica, 2021, Erieri (https://www.erieri.com/salaryreport/report).

Figura 5

Compensación total del Arquitecto de Seguridad en Costa Rica basado en la Experiencia

Nota: La imagen muestra las compensaciones totales anuales según un Nivel Entrante, un Nivel Promedio y un Nivel Senior de Arquitectos de Seguridad en Costa Rica. Adaptado de *Nivel de Compensaciones para Arquitectos de Seguridad,* por Instituto de Investigación económica, 2021, Erieri (https://www.erieri.com/salaryreport/report).

Es así como, considerando que las tres fuentes anteriores tienen valores bastante cercanos entre sí, el salario en Costa Rica puede ser aproximadamente una tercera parte de una remuneración en Estados Unidos.

De modo que, la Tabla 1 muestra un desglose del salario de un profesional en el área mencionada en salario mensual y por hora, tomando como base la Figura 5.

Tabla 1

Desglose de Salarios de un profesional en Arquitectura de Seguridad con salario anual, mensual y por hora.

Salario Anual	Salario Mensual	Salario por hora
21 231 610	**1 769 301**	**11 058,13**

Nota: Elaboración propia.

Así que, para el costo teórico se tendría calculado un costo estimado/ horas consultor (Tabla 2) de aproximadamente **4 976 159 06** colones tomando en cuenta un salario por hora de **11 058 13** colones.

Tabla 2

Costo estimado/ horas de la consultora para la investigación aplicada en un cuatrimestre.

Horas de investigación	Horas semanales	Duración del TFG en Meses	Duración del TFG en horas	Costo estimado/Horas Consultor
Grettel Rivera	30	4	450	4.976.159,06

Nota: Elaboración propia.

1.6 Objetivos

Se usa la taxonomía de Bloom (la revisada del año 2000) debido a que existe extensa documentación al respecto, a su estructuración jerárquica y a la adaptación que mejor refleja los objetivos de la presente investigación.

1.6.1 Objetivo general.

Diseñar una estructura de seguridad de la información de los expedientes digitales especializados para el ICAP como parte del proceso de transformación digital.

1.6.2 Objetivos específicos.

- Analizar la seguridad actual desde el inicio del ciclo de vida de los expedientes electrónicos para encontrar vulnerabilidades y amenazas en la seguridad.
- Aplicar las acciones adecuadas de control y correctivas que proporcionen integridad, disponibilidad y confiabilidad a los expedientes mediante una línea base de seguridad de la información.
- Evaluar las necesidades de los usuarios que acceden a los expedientes digitales para seleccionar el medio de almacenamiento más adecuadamente seguro.
- Describir un método de control digital de la integridad de la información a través de una indexación en los expedientes digitales.
- Explicar la estructura de seguridad de la información que garantice la integridad, disponibilidad y confiabilidad de los datos incluidos en cada expediente digital mediante una representación gráfica.

1.7 Alcances y limitaciones

1.7.1 Alcances.

La investigación se centrará en el diseño de la estructura de seguridad para los expedientes digitales de los profesores de centros de formación superior (diplomados, maestrías) y/o de capacitación técnica, tal y como es el Instituto Centroamericano de Administración Pública (ICAP).

Para llevar a cabo por completo el alcance, se realizará una tabla comparativa de al menos 3 aplicaciones de gestión documental que compare las especificaciones que permitan cumplir con la Normativa Técnica de Interoperabilidad de Documentos y Expedientes electrónicos y seguir las pautas que se definan para la estructura de seguridad. Además, se analizarán las actuales tecnologías de las que dispone el centro y se realizarán las respectivas recomendaciones basadas en mejores prácticas.

También, el alcance cubrirá las políticas que formarán parte de una línea base para la seguridad de la información y las políticas que integrarán la Política de Gestión de documentos electrónicos.

El alcance de la investigación incluirá identificar las brechas que puedan afectar la seguridad de los expedientes digitales a lo largo de su ciclo de vida para así establecer los lineamientos clave para el diseño de la estructura de seguridad de éstos.

Finalmente, todo el alcance de la propuesta de solución (la tabla comparativa, los lineamientos clave para la estructura de seguridad de los expedientes, los lineamientos básicos para la línea de seguridad y el esquema de seguridad) se estará explicando de manera detallada a la Institución al final y durante la investigación para obtener retroalimentación y mejorar la solución.

1.7.2 Limitaciones.

Como limitaciones de esta investigación, se tiene que no se entregará ninguna solución desarrollada, sino más bien, la propuesta de diseño de la estructura de seguridad de la información de expedientes digitales especializados para centros de formación superior y/o de capacitación técnica. Además, no se pretenderá crear toda una política para el resguardo de la seguridad física. Así tampoco se entregará ningún desarrollo de software,

prototipo de software o análisis FODA de aplicaciones para administrar expedientes digitales. No se hará un análisis de ventajas y desventajas de los diferentes proveedores que puedan usar para las para la autenticación y autorización del acceso a los medios de almacenamiento. El trabajo se centrará en el diseño de la estructura de seguridad de la información electrónica.

1.8 Marco de referencia organizacional y socioeconómico

1.8.1 Historia

El ICAP es un organismo internacional regional que se constituye en la segunda mitad del siglo XX, más específicamente el 16 de octubre de 1953 con el nombre de ESAPAC. La institución surge como necesidad de cubrir la asistencia técnica en administración pública del Istmo Centroamericano y también porque estaba retomando la idea de la creación de una escuela Superior de Administración de Educación Pública para Centroamérica que venía como Idea de la División de Administración de Asistencia Técnica de las Naciones Unidas, NN.UU.

> Aun cuando la institución inició labores desde 1954, no fue sino hasta el 12 de diciembre de 1956, durante la Tercera Reunión Ordinaria de la Junta General de la ESAPAC, en San José, que los representantes de los Gobiernos de Costa Rica, El Salvador, Guatemala, Honduras y Nicaragua aprobaron el Convenio para el establecimiento de la Escuela Superior de Administración Pública América Central, ESAPAC, sobre bases internacionales regionales (Regidor-Barbosa, 2010, párrafo 5).
>
> Posteriormente, el incremento de actividades en el marco de ESAPAC, llevó a que la Junta Directiva reconsiderara sus alcances. Así, durante la Reunión Ordinaria del 30 de octubre de 1964, se iniciaron las gestiones para convertir a la ESAPAC en lo que hoy es el Instituto Centroamericano de Administración Pública, ICAP, siendo que, en la Reunión Ordinaria del 20 de noviembre de 1965, se presentó la propuesta para que el Fondo Especial de las Naciones Unidas, financiara junto a otras instancias gubernamentales y cooperantes internacionales, el proceso de transformación. De tal forma, en la Reunión Ordinaria del 17 de febrero de

> 1967, la Junta General aprobó dicho proyecto y firmó el “Plan de Operaciones”, que se encuentra respaldado jurídicamente por convenios básicos firmados entre los Gobiernos de la Región y el PNUD, conocido como el documento que da origen al ICAP en su forma actual. (Regidor-Barbosa, 2010, párrafo 8)

Al llevar a cabo dicha transformación, no adulteró la filosofía constitutiva original, al contrario, fortaleció la necesidad de continuar presentando los servicios ya dispuestos al recurso humano de la administración pública centroamericana.

“Considerando sus orígenes y proceso participativo, el ICAP se ha integrado como una institución parte del Sistema de Integración Centroamericana, SICA” (Regidor-Barbosa, 2010, párrafo 9).

1.8.2 Tipo de negocio y mercado meta.

El ICAP está especializado en Administración Pública, de carácter intergubernamental, orientado al desarrollo del talento humano y la modernización de la institucionalidad pública centroamericana.

Las áreas de especialización son:

Formación académica: desde sus inicios, el ICAP ha ejecutado exitosamente más de cincuenta promociones de programas a nivel de Maestría, Posgrados, Pasantías y Diplomados, tanto a nivel nacional como regional. Por ser el tratado constitutivo, uno de carácter internacional, el ICAP cuenta con el reconocimiento de pleno derecho de los títulos que otorgue por parte de sus países miembros.

Capacitación: la institución ha logrado desarrollar habilidades y experiencia específica en programas de capacitación en áreas y temas necesarios y vinculantes para el cotidiano quehacer de la Administración Pública. Los programas están dirigidos a fortalecer las capacidades, cualidades, aptitudes y actitudes de los funcionarios públicos de la región.

Información y difusión: el programa editorial del ICAP, destaca obras de carácter técnico y científico, sobre temas relevantes para la administración pública. De igual manera, la institución ha desarrollado vigorosamente un

> Centro de Recursos de Información y Aprendizaje, CRIA, cuya labor se ha extendido desde aspectos fundamentales como la tenencia de una colección amplia de material bibliográfico y acceso a bases de datos con información especializada vía página web, hasta convertirse en un importante referente de documentación especializada en materia de administración pública en la región.
>
> **Consultoría y asistencia técnica:** por requerimiento de los Estados Miembros, el ICAP ha realizado consultorías específicas y ha brindado programas de asistencia técnica en todos los países de la región. Ha colaborado en la implementación de proyectos de carácter regional y nacional coordinadamente con instancias gubernamentales. Los programas se orientan al logro de la eficiencia, eficacia y efectividad de la gestión institucional en la administración pública, promoviendo la cooperación horizontal y el intercambio de experiencias entre países miembros.
>
> **Investigación:** como parte de su aporte a la investigación y formación del pensamiento centroamericano, ha contribuido en la realización de numerosas investigaciones académicas y científico-sociales, sin contar, con la gran producción anual de proyectos y trabajos finales de graduación enfocados al mejoramiento de las capacidades de las instituciones en que laboran sus estudiantes. (Regidor-Barbosa, 2010, párrafo 15).

El principal objetivo de la organización fue dirigido, desde sus inicios, a toda aquella institución de administración pública de todo el Istmo Centroamericano, cuyo mercado meta serían las instituciones públicas, instituciones de gobiernos y gobiernos locales; adicionalmente, se extiende a funcionarios y a funcionarias de la administración pública centroamericana para facilitarles la organización e implementación de programas de formación académica y capacitación.

1.8.3 Misión, visión y valores.

Misión: se enfoca en fortalecer las competencias del recurso humano, la reforma y modernización de las entidades públicas y el apoyo para la integración centroamericana.

Visión: ser la institución del Sistema de la Integración Centroamericana especializada en la gestión del conocimiento para la innovación de las organizaciones y el mejoramiento de las capacidades de gerencia de las políticas públicas a nivel local, nacional y regional.

Valores.

Integridad: obrar con rectitud y probidad, que incluye comunicar en forma abierta y directa sus intenciones, ideas y sentimientos.

Excelencia: capacidad y actitud de exceder las expectativas en su gestión diaria, buscando siempre brindar un valor agregado, basándose en una constante actualización y búsqueda permanente de retroalimentación.

Respeto: mostrar tolerancia hacia la diversidad de ideas, opiniones, y personalidades, en sus interacciones cotidianas. Uso correcto del vocabulario verbal o simbólico y trato con los demás. Respeto al acatamiento de las normativas, cumplir con lo prometido o establecido y manejar con prudencia la información de la Institución.

Compromiso: sentir como propios los objetivos de la organización. Responsabilidad en el cumplimiento de obligaciones o deberes contraídos o a la palabra dada, o la actitud de comprometerse consigo mismo de hacer las cosas de manera óptima y correcta.

Trabajo en equipo: capacidad de integrarse, comunicarse y comprometerse con un equipo de trabajo, aportando sugerencias, ideas y esfuerzos con el fin de alcanzar eficaz y eficientemente los objetivos y metas comunes.

1.8.4 Políticas institucionales.

Actualmente, desde el CATIC existen una serie de lineamientos que se trabajan para la gestión del equipo informático, políticas aplicadas al software en la nube y *firewalls*, así como de conexión de dispositivos, préstamos de los equipos y otros. Sin embargo, no hay políticas relacionadas con la

confidencialidad, integridad y disponibilidad de la información de manera específica, la institución se encuentra trabajando en ello.

1.9 Estado de la cuestión

1.9.1 Planificación de la revisión.

Teniendo en cuenta que el tema por investigar es de una estructura de seguridad de expedientes digitales para el ICAP, se decide empezar por buscar primero en fuentes de origen extranjero, ya que el tema en este país es muy reciente y no existe una normativa específica para expedientes digitales.

Para esta investigación, se realizó una búsqueda por separado de cada uno de los temas que conforman una estructura de seguridad, al conocer que la información que se busca no se encuentra en un consolidado. Esta búsqueda se realiza en dos tipos de fuentes de información: la primera, en libros, revistas y normativas que estandaricen los procedimientos asociados al manejo de expedientes electrónicos y/o sus componentes (por ejemplo, documentos electrónicos); en segundo lugar, fuentes como reglamentos, artículos, tesis relacionadas y otros repositorios. Cabe decir, que la mayoría de la información no se encuentra en idioma español, sino en inglés, por lo cual muchos de los textos requerían traducirse.

1.9.1.1 Formulación de la pregunta.

En esta sección, los objetivos de la investigación ya están claramente definidos y con ayuda de estos se buscan respuestas, por ejemplo, sobre cómo garantizar la integridad, disponibilidad y confiabilidad de los datos incluidos en los expedientes digitales. Dichas respuestas han de demostrar la importancia de este trabajo, en cuanto a la aplicación práctica en el ICAP.

1.9.1.2 Enfoque de la pregunta.

Se requiere para la presente investigación enfocarse en documentos técnicos que expliquen sobre las prácticas de seguridad que están detrás de una arquitectura que involucra documentos electrónicos y expedientes digitales. Además, tiene que estar enfocada en encontrar la documentación de las especificaciones técnicas de diferentes software y técnicas que brinden

confidencialidad, disponibilidad e integridad a los datos que contienen los expedientes digitales.

1.9.1.3 Calidad y amplitud de la pregunta.

1. **Problema**

El objetivo de la revisión sistemática es proporcionar a la investigación la manera en que los arquitectos de seguridad de la información implementen buenas prácticas y tecnologías acordes con la necesidad y estrategia de la organización, para solventar problemas como falta de control sobre la confidencialidad, dudas sobre la integridad, inapropiada disponibilidad y otros problemas que afectan directamente la estructura de seguridad de los expedientes digitales.

2. **Pregunta**

A través de la revisión sistemática se pretende responder a, ¿cuáles medidas se han tomado por diferentes organizaciones en el campo de la educación y la administración pública, para tener seguridad en todos los aspectos relacionados con la información contenida en expedientes digitales?

3. **Palabras clave y sinónimos**

Se hace un listado de palabras clave que se van a utilizar para la búsqueda e
identificación de documentos y trabajos relacionados con esta investigación. Algunos términos están en el idioma inglés. A continuación, el listado:

- Seguridad de la información
- Expedientes digitales
- Expediente electrónico
- Bases de datos
- *Documental databases*
- Documentos electrónicos
- Documentos de archivo
- Encriptación
- *Authentication*
- Indexación de documentos electrónicos
- Administración electrónica

- Gestión de documentos electrónicos
- Lineamientos de expedientes
- Firma digital
- CSV
- *SharePoint*

4. Intervención

Lo que se va a observar en el contexto de esta revisión sistemática planificada es cómo mediante el conocimiento se puede hacer la selección de medios de almacenamiento seguro, el establecimiento de procedimientos de indexación en los expedientes digitales y la aplicación de medidas de control y correctivas que brinden confidencialidad, integridad y disponibilidad; todo con el fin de diseñar una estructura de seguridad para expedientes digitales.

5. Control

Al iniciar la investigación, se toma como base dos tesis presentadas en los años 2019 y 2020: una se titula, *Diseño de una estructura de seguridad de la información de expedientes digitales especializados para Centros Médicos*, de Minor Agüero Marín y la otra es *BlockChain como solución para la Administración de Expedientes Digital*, de Eduardo Vindas Córdoba.

Adicionalmente, la base de esta investigación fueron las palabras claves definidas anteriormente en este documento.

6. Efecto

Los resultados esperados al final de la revisión sistemática es tener suficiente documentación técnica que brinde conocimiento sobre las medidas, softwares utilizados, normativas empleadas de referencia y maneras de administración de la información electrónica que fueron tomadas por diferentes organizaciones tanto a nivel nacional como internacional para tener una estructura segura para los expedientes digitales.

7. Medida de resultado

Para la documentación encontrada, se realiza una revisión de la calidad de esta, indicada en los mismos sitios web, tomando en cuenta la puntuación dada por los investigadores y la cantidad de veces que fueran citadas las fuentes de investigación.

8. **Población**

El grupo de personas que será observado corresponde a los usuarios de los expedientes digitales, así como las personas de tecnología que contribuyen con la estructura de los sistemas en la organización.

9. **Aplicación**

Los que se beneficiaran de los resultados de la revisión sistemática son los profesionales en el área de ciberseguridad informática en roles como arquitectura de seguridad, análisis de riesgos y asesor de cumplimiento. También se beneficiarán los ingenieros informáticos que ocupen el rol de analistas de la información y arquitectura de sistemas. Eventualmente, para un analista de negocio podrían ser útiles dichos resultados de la revisión sistemática.

10. **Diseño experimental**

En el proceso del diseño experimental se hace un análisis y clasificación de los estudios obtenidos tomando en cuenta su relevancia para la investigación y desde luego la calidad de la fuente. De modo que se garantice mayor confianza para la investigación y se evite tener un rango demasiado amplio de estudios que pudieran generar resultados no deseados.

1.9.1.2 Selección de fuentes.

1.9.1.2.1 Definición del criterio de la selección de las fuentes.

Los criterios que se definieron para seleccionar efectivamente las fuentes de investigación son:

- ✓ Popularidad entre investigadores.
- ✓ Respaldo académico.
- ✓ Respaldo de investigadores destacados.
- ✓ Cantidad de menciones en trabajos de investigación.
- ✓ Grado confianza en relación con la palabra clave utilizada.
- ✓ Seguridad para la consulta de la fuente.

1.9.1.2.2 Métodos de búsqueda de fuentes.

Los motores de búsqueda y repositorios virtuales usados fueron *Google Academics*, *Springer eBooks*, EBSCO y elibro.net. Todos estos proporcionan acceso a más de un millón de documentos de investigación y libros. Se consideran las principales fuentes de recursos para todos los investigadores, profesores y estudiantes; y en general, son plataformas sencillas de manejar e intuitivas, lo que facilita la localización de contenidos.

Los métodos de búsqueda de fuentes de investigación usados son: búsqueda estructural, *backward snowboling y skiming lecture*.

1.9.1.2.3 Cadena de búsqueda.

Las cadenas de búsqueda utilizadas tienen combinación de “OR” y “AND”. (“documentos electrónicos” AND “políticas”) AND (("expedientes digitales" OR "expedientes electrónicos") AND (“seguridad de la información” OR “*information security*”)) AND (("*hash*" OR “firma digital") AND (“documentos de archivos” AND “normativas”) AND (("seguridad" AND "expediente digital" OR “expediente electrónico”) AND (“*authentication methods*” OR “métodos de autenticación”)).

1.9.1.3.4 Lista de fuentes.

Las fuentes usadas fueron: *Google Academics*, *SpringerLink*, eLibro.net, ACM Digital Library, Science Direct, Repositorio UTN, EBSCO, Librarika, PAe, INTECO, MINTIC, Atlasian, Zoho y Microsoft Docs.

1.9.1.2.5 Selección de fuentes después de la evaluación.

Las fuentes que se encuentren en los repositorios y motores de búsqueda indicados en el punto anterior deben evaluarse según los puntos indicados en la selección de criterios de selección de fuentes para determinarse si van a utilizar en la investigación o no.

Algunas de las fuentes ya descartadas se encuentran: Revista Ulatina y Repositorio UTN.

1.9.1.2.6 Comprobación de referencias.

En este momento no se cuenta con un criterio experto para la selección de las fuentes; por lo cual, se emplean los criterios de selección de fuentes para hacerlo. Se espera más adelante contar con un criterio experto para depurar la lista o agregar más, según sea necesario.

1.9.1.3 Selección de los estudios de la revisión.

A continuación, se presenta el proceso de selección llevado a cabo para las
diferentes fuentes.

1.9.1.3.1 Definición del criterio de inclusión y exclusión de estudios.

Se utilizan los criterios detallados en la Tabla 3, para incluir o excluir un estudio.

Tabla 3

Criterios de inclusión y exclusión

Pregunta de Investigación	Término principal para criterio de inclusión	Criterios de exclusión
¿Cuáles medidas se han tomado por diferentes organizaciones en el campo de la educación y la administración pública, para tener seguridad en todos los aspectos relacionados con la información contenida en expedientes digitales?	Seguridad de la información Expedientes digitales Expediente electrónico Bases de datos *Documental databases* Documentos electrónicos Documentos de archivo	- Guías, normativas y lineamientos con un periodo de actualización de más de 10 años. - La relación con la palabra clave es ambigua o poco clara. - Tiene edición abierta al público en general. - Carece de autor.

	Encriptación *Authentication* Indexación de documentos electrónicos Administración electrónica Gestión de documentos electrónicos Lineamientos de expedientes Seguridad en expedientes digitales.	- Tienen menos de dos menciones en trabajos de investigación. - No aparece en ninguno de los motores de búsqueda académico.

1.9.3.2 Definición de tipos de estudio.

Los tipos de estudio primario que son seleccionados se basan en los criterios indicados en la Tabla 4.

Tabla 4

Criterios para tipos de estudio primario

Pregunta de investigación	¿Qué?	¿Cómo?	¿Dónde?
¿Cuáles medidas se han tomado por diferentes organizaciones en el campo de la educación y la administración pública, para tener seguridad en todos los aspectos relacionados con la información contenida en expedientes digitales?	Medidas para la Seguridad en expedientes digitales.	Prevención Reacción	Organizaciones intergubernamentales. Organizaciones intergubernamentales. Instituciones de capacitación.

			Instituciones de forma técnica. Instituciones de formación superior.

Nota: Elaboración propia

1.9.1.3.3 Procedimiento para la selección de los estudios.

Se realizó el siguiente proceso iterativo por cada fuente encontrada para la selección de los estudios:

- Utilizar la opción de búsqueda avanzada o búsqueda general disponible en las fuentes seleccionadas.
- Emplear las cadenas de búsqueda aplicables en el repositorio o motor de búsqueda para obtener resultados considerados de interés.
- Aplicar filtros o cadenas adicionales para disminuir la lista de resultados, por
  ejemplo, fechas de publicación y autor.
- Hacer *skiming lecture* que incluya el resumen o *abstract*, si el documento tiene uno, para identificar la relación con lo que se desea encontrar.
- Evaluar los resultados obtenidos y aplicar los criterios de exclusión.
- Seleccionar los resultados considerados relevantes para la fuente consultada y repetir el proceso con las demás fuentes disponibles.

Capítulo 2. Marco Conceptual

2.1 Conceptos

2.1.1 Expedientes electrónicos.

De acuerdo con la Norma Técnica Nacional de Lineamientos para la conformación de Expedientes Administrativos, se define como expediente digital:

> A la agregación de objetos creados en ambientes electrónicos, ordenados cronológicamente, que se gestionan dentro de un sistema de gestión de documentos electrónicos de archivo y que se preservan en un repositorio digital, los cuales responden a un trámite administrativo. La creación de estos expedientes debe estar regulada por las políticas de gestión de documentos electrónicos propias de cada institución (Archivo Nacional, 2020, p.26).

El expediente electrónico tiene los siguientes componentes:

1. Documentos electrónicos.

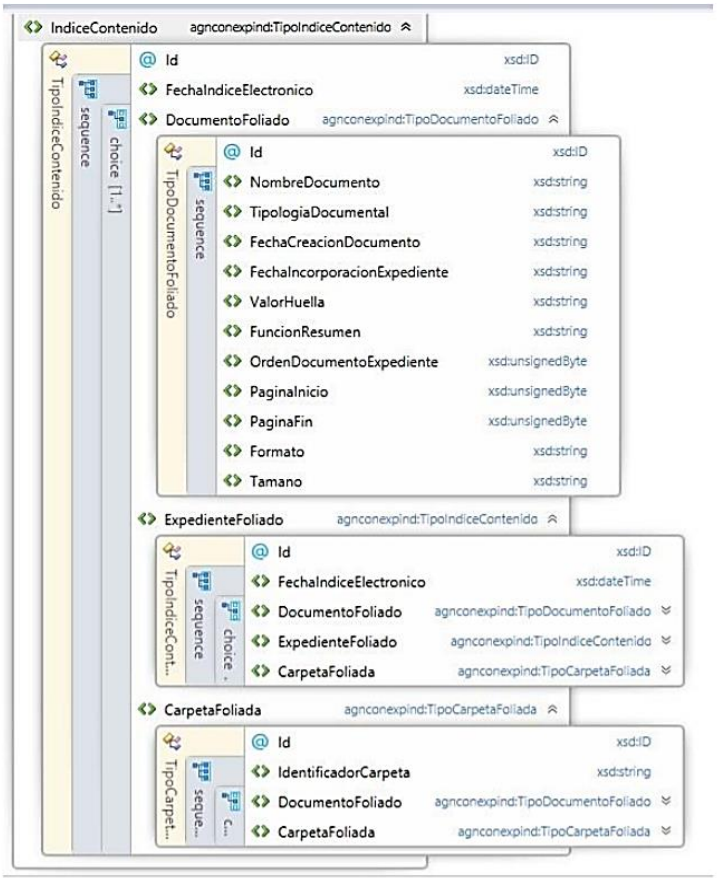
   Los documentos electrónicos podrán incluirse en un expediente electrónico bien directamente como elementos independientes, bien dentro de una carpeta, entendida ésta como una agrupación de documentos electrónicos creada por un motivo funcional, o bien como parte de otro expediente, anidado en el primero (Ministerio de Hacienda Pública y Administraciones Pública de España, 2016b, p.13).
2. Índice electrónico generado automáticamente: garantizará la integridad del expediente electrónico y permitirá su recuperación siempre que sea preciso. “El índice electrónico recogerá el conjunto de documentos electrónicos asociados al expediente en un momento dado y, si es el caso, su disposición en carpetas o expedientes” (Ministerio de Hacienda Pública y Administraciones Pública de España, 2016b, p.13).
3. Firma digital del índice electrónico: será para garantizar la integridad y autenticidad del contenido del índice y por extensión, la de los documentos electrónicos que conforman el expediente electrónico. Los sistemas de firma electrónica por parte de la organización que pueden ser utilizados son: Firma electrónica basada en certificados y Firma de Código

Seguro de Verificación (CVC); más adelante explicado en esta investigación.

4. Metadatos del expediente electrónico: “constituyen un conjunto de datos que proporciona contexto al contenido, estructura y firma de un documento, contribuyendo al valor probatorio y fiabilidad de éste a lo largo del tiempo como evidencia electrónica de las actividades y procedimientos” (Ministerio de Hacienda y Administración Pública de España, 2016a, p.14).

Figura 6

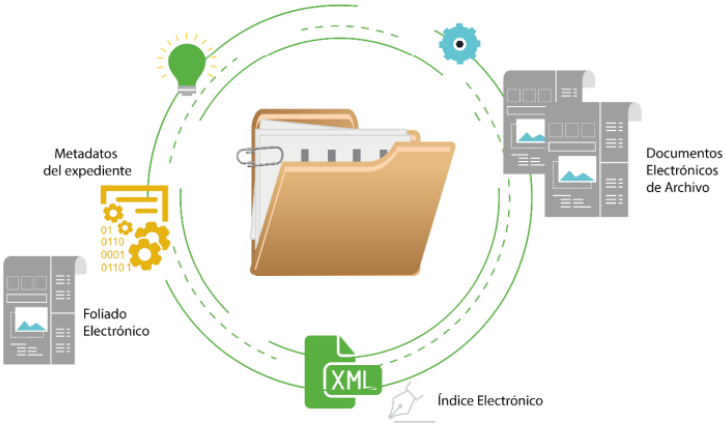
Ejemplo de Metadatos



Nota: Ejemplo de los metadatos usado en el expediente digital. Adaptado de *Guía para la gestión de documentos y expedientes electrónicos del Gobierno de Colombia* (p.12), por Rangel y Merchán, 2019, Dirección de Gobierno Digital de Colombia.

Figura 7

Componentes del expediente electrónico.



Nota: Componentes del expediente electrónico. Adaptado de *Guía para la Gestión de documentos y expedientes electrónicos* (p.66), por Rangel, 2019, Dirección de Gobierno Digital de Colombia

Es importante mencionar que el diseño e implementación de cada componente del expediente electrónico sea conforme a las necesidades y política específica de cada organización.

2.1.2 Políticas de gestión de documentos electrónicos.

De acuerdo con la Guía de aplicación de la Norma Técnica de Interoperabilidad de Expediente electrónico del Gobierno de España, Ministerio de Hacienda Pública y Administraciones Pública de España (2016); se define como Orientaciones o directrices que define una organización para la creación y gestión de documentos auténticos, fiables y disponibles a lo largo del tiempo, de acuerdo con las funciones y actividades que le son propias. La política se aprueba al más alto nivel dentro de la organización, y asigna responsabilidades en cuanto a la coordinación, aplicación, supervisión y gestión del programa de tratamiento de los documentos a través de su ciclo de vida.

2.1.3 Autenticidad.

Un documento de archivo auténtico es aquél del que se puede probar:

a) que es lo que afirma ser;
b) que ha sido creado o enviado por la persona que se afirma que lo ha creado o enviado; y
c) que ha sido creado o enviado en el momento que se afirma. (ISO 15489, 2001, p.10).

Para garantizar la autenticidad de los documentos, las organizaciones tendrían que implantar y documentar políticas y procedimientos para el control de la creación, recepción, transmisión, mantenimiento y disposición de los documentos de archivo.

2.1.4 Confiabilidad

Consiste en:

Propiedad o característica que indica que su contenido puede ser considerado una representación completa y precisa de las actuaciones, las actividades o los hechos de los que da testimonio y al que se puede recurrir en el curso de posteriores actuaciones o actividades (Ministerio de Hacienda Pública y Administraciones Pública de España, 2016a, p.13).

2.1.5 Integridad.

La integridad de un documento de archivo hace referencia a su carácter completo e inalterado.

Es necesario que un documento esté protegido contra modificaciones no autorizadas.

Las políticas y los procedimientos de gestión de documentos deberían especificar qué adiciones pueden realizarse en un documento después de su creación, en qué circunstancias pueden autorizarse dichas adiciones o anotaciones y quién está autorizado para llevarlas a cabo (ISO 15489, 2001, p.10).

2.1.6 Disponibilidad.

Un documento de archivo disponible es aquel que puede ser localizado, recuperado, presentado e interpretado. Su presentación debería mostrar la actividad u operación que lo produjo. Las indicaciones sobre el contexto de los documentos de archivo deberían contener la información necesaria para la comprensión de las operaciones que los crearon y usaron. “Debería ser posible identificar un documento en el contexto amplio de las actividades y las funciones de la organización. Se debería mantener los vínculos existentes entre los documentos de archivo que reflejan una secuencia de actividades” (ISO 15489, 2001, p.11).

2.1.7 Trazabilidad.

"Se define para los documentos de archivo, como la creación, incorporación y conservación de información sobre el movimiento y el uso de documentos de archivo" (ISO 15489, 2001, p.5). Por tanto, la trazabilidad se logra mediante un control desde su creación hasta su destrucción, que evidencie como mínimo el nombre del funcionario, la fecha y el destino físico del expediente.

2.2 Expedientes electrónicos

2.2.1 Estructura de seguridad.

Una estructura de seguridad es esencial para la implementación de un expediente electrónico, por lo que su diseño requiere la utilización de procedimientos y herramientas que le den suficiente protección a la información que aseguren en lo máximo los principios fundamentales de seguridad de la información: confidencialidad, la integridad y disponibilidad.

Se puede apuntar que una estructura de seguridad es un conjunto de procesos definidos estratégicamente, para minimizar las vulnerabilidades y el riesgo de un ataque a los datos. Por tanto, se puede ver la estructura como una estrategia, ésta tiene que fijar políticas, controles de seguridad y procedimientos de detección y control de amenazas. El principal objetivo de la estructura de seguridad es fortalecer la confianza sobre la información que resguarda dicha estructura.

Las estructuras de seguridad de la información también hacen uso de las estrategias del negocio para establecer sus procesos estratégicos, de modo que se obtiene una alineación entre la estrategia del negocio y la estrategia de seguridad de la información implementada por Tecnologías de la Información (TI).

2.2.2 Ciclo de vida del expediente electrónico.

El ciclo de vida del expediente tiene 3 fases: la de apertura (creación del expediente con su respectivo índice), la de tramitación y la fase de conservación y selección. Las siguientes las fases que se describen de acuerdo

con la Normativa Técnica de Interoperabilidad de Expedientes electrónicos y en la Normativa Técnica Nacional.

2.2.2.1 Fase de apertura

- Creación del expediente electrónico: se compone de un índice, los documentos electrónicos que sean incorporados al expediente y de los metadatos asociados al expediente.
- Creación del índice electrónico: es un documento electrónico que contiene la identificación sustancial que compone el expediente debidamente ordenado para reflejar la disposición de los documentos, así como otros datos con el fin de preservar la integridad y permitir su recuperación.
- Inclusión en el índice de cada uno de los documentos electrónicos que conforman el expediente, al momento de su apertura, y los que se irán agregando, de acuerdo con su progresiva captura y registro en el sistema de gestión de documentos y su incorporación al expediente.
- Asignación de metadatos mínimos obligatorios del expediente electrónico:
  - Código de referencia
  - Identificador normalizado del expediente.
  - Nombre del productor: Identificador normalizado de la administración responsable de la tramitación del procedimiento (según Norma Nacional de Descripción Archivística).
  - Fecha de apertura.
  - Estado – Estado del expediente.
  - Restricciones de acceso.
  - Fecha de resolución.
  - Título
  - Nombre del expediente (Archivo Nacional, 2020, p.24).

2.2.2.2 Fase de tramitación.

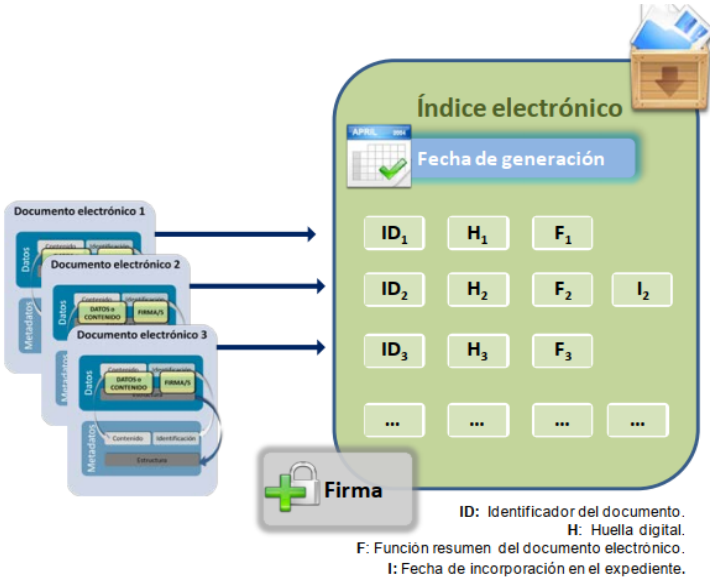
- Inclusión de los nuevos documentos: según el trámite administrativo, se incorporarán documentos al expediente, los cuales se deben reflejar en el índice electrónico.
- Cambio de estado o de características particulares: consiste en la posibilidad que durante la fase administrativa se incluyan o modifiquen

metadatos de acuerdo con las necesidades de la administración, la normativa vigente o las necesidades de información de los ciudadanos, tales como vigencia administrativa, accesos, entre otros.

- Foliado del expediente: consiste en hacer el foliado mediante el índice electrónico en el que se relacionan todos los documentos que lo componen. Dicho índice se construye con la incorporación de cada nuevo documento que se agregue al expediente y es firmado por la persona con la competencia legal, o a través de un sello electrónico (firma digital de persona jurídica) al momento del cierre del expediente. Para este tipo de trámite se debe seguir la legislación pertinente, que garantice así la integridad del expediente. El índice electrónico para documentos oficiales de archivo debe contemplar al menos los siguientes elementos:
  - Identificadores
  - El fondo y el subfondo al que pertenece el expediente.
  - Número de asiento.
  - Cada documento tendrá su propio identificador único.
  - Resumen *hash.*
  - Resultado único de la aplicación de una función *hash* a cada documento, para aseguramiento y verificación de su integridad.
  - Fecha de incorporación del documento electrónico al expediente.
  - Firma digital / sello electrónico del índice electrónico.
  - Fecha y hora de cierre del expediente.
  - Bitácora de índices anteriores (Archivo Nacional, 2020, p.24).

Figura 8

Ejemplo de un indexado básico para un expediente electrónico



Nota: Representación del indexado básico de un expediente electrónico. Adaptado de *Guía de aplicación de la Norma Técnica de Interoperabilidad de Expediente electrónicos* (p.21), por Ministerio de Hacienda Pública y Administraciones Pública de España, 2016, Gobierno de España.

2.2.2.3 Fase de conservación y selección.

A cada institución le compete elaborar un plan de preservación, que garantice la accesibilidad, autenticidad, disponibilidad, integridad, seguridad y legalidad de los documentos electrónicos a lo largo de su ciclo de vida. Dicho plan tendría que incluir estrategias de preservación y recuperación específicas para este tipo de soporte. En cuanto a la selección y eliminación de expedientes electrónicos administrativos, se hace un cumplimiento de las regulaciones estipuladas por la Ley del Sistema Nacional de Archivos N°7202, su Reglamento Ejecutivo dado por Decreto N°40554-C y las resoluciones de la Comisión Nacional de Selección y Eliminación de Documentos (CNSED). Asimismo, la fase de conservación y selección revisa la sección: “1.8 Valoración selección y disposición final” de la Norma Técnica de Gestión de Documentos Electrónicos en el Sistema Nacional de Archivos.

Figura 9

Resumen del ciclo de vida de un expediente electrónico

Nota: Resumen del ciclo de vida de un expediente electrónico. Adaptado de *Guía de aplicación de la Norma Técnica de Interoperabilidad de Expediente electrónicos* (p.18), por el Ministerio de Hacienda Pública y Administraciones Pública de España, 2016, Gobierno de España.

2.2.3 Servicios de remisión y puesta a disposición.

Para el proceso de remisión y puesta a disposición, la consulta o puesta a disposición mediante la solicitud de la remisión o envío del expediente es realizada por los interesados. Para cuando se producen solicitudes de remisión o puesta a disposición de expedientes entre distintas organizaciones o por parte de civiles externos a la organización se siguen unas pautas comunes, para el intercambio de expedientes electrónicos, que pretenden favorecer la interoperabilidad. Sin embargo, cuando el intercambio de expedientes se produce a nivel interno, se rige por lo establecido en la política interna.

El intercambio de expedientes electrónicos se realiza mediante el envío de un canal que sea señalado por la organización (pudiendo ser que la estructura esté basándose en alguna normativa del país). Excepcionalmente, se podrían aplicar otras estructuras para el intercambio de expedientes electrónicos, cuando exista acuerdo previo entre las partes. En cualquier caso, si debe enviarse a un tercero, la estructura utilizada debe ser convertida por el emisor. Tras el envío de dicha estructura, se hace también el envío de cada uno de los documentos electrónicos que componen el expediente, en el orden indicado en el índice.

En caso de intercambio de expedientes electrónicos entre Administraciones públicas que supone una transferencia de custodia o traspaso

de responsabilidad de gestión de expedientes que deben conservarse permanentemente, el órgano o entidad transferidora verifica la autenticidad e integridad del expediente en el momento de dicho intercambio.

Cabría contemplar que los datos de los servicios de intercambio y consulta de expedientes se registren a través de metadatos del expediente, pues ello permite la trazabilidad de las distintas operaciones.

2.2.4 Consideraciones para la implementación y la gestión del expediente electrónico.

Para implementación y gestión de expediente electrónico no hay consideraciones específicas puesto que su gestión debe ser provista como parte de sección de las políticas de gestión de documentos electrónicos que también constituyen la gestión documental o de archivos dispuesta por la organización.

2.2.4.1 Estándares y buenas prácticas.

Además de lo mencionado anteriormente, se toman como buenas prácticas para la gestión de expedientes y documentos electrónicos las siguientes:

- Gestionar los documentos electrónicos como los documentos de archivo (en estado vivos o finalizado).
- Tener un repositorio digital, es decir un punto de acceso general electrónico de la administración o a una sede electrónica.
- Tener definido cuando se pueden eliminar los documentos electrónicos y un procedimiento bien definido para proceder a hacerlo.
- Brindar la debida clasificación documental acorde con la estructura orgánica – funcional.
- Efectuar el registro y almacenamiento de los metadatos asociados al expediente.
- Tener disponibilidad de mecanismos para el aseguramiento de su autenticidad, integridad y disponibilidad.
- Si es requerido, los mismos expedientes pueden tener un número de Folio o indezado al cierre del expediente.

- Poseer controles que dejen constancia de las solicitudes recibidas, atendidas respecto a la remisión y puesta a disposición de los expedientes electrónicos.

Figura 10

Ejemplo de Arquitectura de sistema de gestión de información electrónica

Nota: Elaboración propia.

2.2.4.2 Metadatos para la gestión de documentos electrónicos.

Tal y como se mencionó anteriormente en este documento, los metadatos corresponden a un componente del expediente electrónico, que facilitan la gestión, creación y uso de estos a lo largo del tiempo.

Los metadatos pueden ser mínimos obligatorios, estos:

> …constituyen un conjunto mínimo de información definido con el fin de facilitar el conocimiento inmediato y automatizable de las características básicas del expediente electrónico que permitan su contextualización en el marco de la organización y procedimiento administrativo al que corresponda (Archivo Nacional, 2020, p.24).

Por otro lado, están los metadatos complementarios, que de acuerdo con el Archivo Nacional (2020) son “para atender a necesidades de descripción

específicas, significa que varían según las necesidades que tiene la organización para el expediente que se está conformando" (p.24).

Para poder hacer una gestión eficiente de los metadatos, las relaciones entre los expedientes electrónicos y estos deben ser permanentes. Es importante indicar que la manera de implementación de los metadatos va acorde con las necesidades y nivel interno de la organización. Es decir, es libre siempre y cuando se busque garantizar la disponibilidad e integridad de los metadatos de sus documentos electrónicos y de sus expedientes electrónicos.

2.2.4.3 Política de gestión de documentos electrónicos.

La política se podrá aplicar en el desarrollo de políticas de gestión de documentos en entornos híbridos en que convivan documentos en soporte papel y documentos electrónicos.

Esta se deberá integrar con el marco general de gestión de documentos y con el contexto organizacional para el desempeño correcto de cada actividad. La política deberá aplicar estándares y buenas prácticas nacionales e internacionales aplicables para la gestión documental, ejemplo de éstas son: *General International Standard Archival Description*, ISO 27001, ISO 15489 e ISO 23081 Información y documentación Procesos de gestión de documentos.

La política de gestión de documentos electrónicos es un documento que debe incluir:

- Definición del alcance y ámbito de aplicación.
- Roles de los actores involucrados: Las personas de interés en la política de gestión de documentos electrónicos vendrían siendo directivos y otros responsables de la aprobación de políticas de gestión de documentos, responsables de sedes electrónicas, responsables y desarrolladores de creación, producción, gestión, conservación y uso de documentos electrónicos. Además, debe incluir los deberes y responsabilidades de los cargos de interés, así como el procedimiento para la designación y renovación.
- Directrices para la estructuración y desarrollo de los procedimientos de gestión documental.
- Actuaciones de supervisión y auditoría de los procesos de gestión de documentos.

- Proceso de revisión del contenido de la política con el fin de garantizar su adecuación a la evolución de las necesidades de la gestión de documentos.

2.3 Bases de datos

En la actualidad hay variedad de bases de datos, estas se clasifican de acuerdo la utilidad, contexto y estructura; no obstante, este documento solo se enfocará en dos modelos de bases de datos: relacionales y las no relacionales y sobre qué es y las ventajas de un Sistema Gestor de Base de datos (SGBD).

Un SGBD le permite al usuario el acceso a un medio para mantener y gestionar variedad de conjuntos de datos.

Ventajas de los SGBD:

- Se puede tener un acceso y una recuperación de datos de manera eficiente.
- Se puede proveer mayor integridad y seguridad en los datos, mediante restricción de visualización, reglas de negocio que prevengan que por ejemplo un precio de producto sea inferior a su valor en costos.
- Se brinda concurrencia de acceso de datos y recuperación de fallos.
- Se tiene menos tiempo en la creación de aplicaciones ya que tienen menos complejidades, es probable que las aplicaciones SGBD sean más robustas que las aplicaciones independientes similares, ya que el SGBD maneja muchas tareas importantes.

Los SGBD permiten a los usuarios definir los datos que van a almacenar en términos de un modelo. La mayor parte de los sistemas actuales de gestión de bases de datos se basan en el modelo relacional. Entre los modelos relacionales más conocidos y utilizados está el modelo entidad-relación (ER) “permite denotar de manera gráfica las entidades y las relaciones existentes entre ellas” (Ramakrishnan, 2007, p.10).

En el modelo relacional lo más importante son las relaciones que pueden considerar como un conjunto de registros y por otro lado están los esquemas de las relaciones, que especifican nombre, el nombre de cada campo y el tipo de cada campo – el esquema puede considerarse como una plantilla para la descripción de la tabla Alumnos.

Figura 11

Ejemplo de una tabla con modelo relacional

ide	*nombre*	*usuario*	*edad*	*nota*
53666	Jiménez	jimenez@inf	18	6,8
53688	Sánchez	sanchez@ii	18	6,4
53650	Sánchez	sanchez@mat	19	7,6
53831	Martínez	martinez@musica	11	3,6
53832	García	garcia@musica	12	4,0

Nota: Adaptado de *Sistemas de Gestión de bases de datos* (p.20), por Ramakrishnan, 2007, McGraw-Hill

Los modelos de las bases de datos **no relacionales o NoSQL** surgen para cubrir varias de las limitaciones que poseen los modelos relacionales como recarga del modelo semántico, bajo rendimiento para colas de consulta recursivas, tipos de datos restringidos y otras deficiencias.

> Históricamente, el término “NoSQL” se aplicaba a los sistemas de bases de datos que ofrecían lenguajes de consulta y métodos de acceso distintos al SQL estándar. Más recientemente, "NOSQL" ha llegado a significar "No sólo SQL"; NOSQL es básicamente un término general que cubre los sistemas de bases de datos que, tienen modelos de datos distintos de las tablas relacionales convencionales, admiten acceso programático al sistema de base de datos o lenguajes de consulta distintos de SQL (pero también pueden admitir SQL), pueden hacer frente a la evolución del esquema o puede manejar datos sin esquema, soportar la distribución de datos en una red de servidores por diseño o no adherirse estrictamente a las propiedades ACID (en particular en términos de consistencia) de los RDBMS convencionales (Wiese, 2015, p.15).

2.4 Control digital para la indexación

En los expedientes, la indexación de nuevos documentos es un proceso continuo que se repite cada vez que se requiere hacer cambios por actualización de datos. Por tal razón, encontrar una herramienta para crear un control de transacciones digitales para la indexación de nuevos documentos al expediente digital, es de suma importancia para mantener la confiabilidad de la información.

Una opción para este control son las bitácoras digitales, que corresponden al registro de la información importante y las acciones que se lleven a cabo en las actividades seleccionadas. Para crear el adecuado control para los requerimientos de esta investigación, se analizan las herramientas que se apeguen mejor a lo exigido por este trabajo.

2.4.1 Bitácoras en SGBD.

Normalmente en los sistemas de información tradicionales se utilizan las bases de datos para generar tablas de auditoría que muestran las transacciones realizadas con la data resguardada.

En el ámbito de la auditoría de datos, las bitácoras, también conocidas como *logs*, son estructuras generalmente usadas para registrar las modificaciones que se dan en la base de datos. Una bitácora es una herramienta para registrar, analizar, detectar y notificar eventos que suceden en cualquier sistema de información, es una herramienta ampliamente usada para grabar las modificaciones de la BD.

2.4.2 Análisis de uso de un sitio o página.

Normalmente las plataformas web ofrecen el análisis de varios elementos, a estos se les denomina foros, blogs o en el caso de SharePoint, simplemente sitios. Estos son una segmentación que suelen usar en las organizaciones para los diferentes departamentos o áreas (como contabilidad, recursos humanos, ventas, entre otros). Los administradores, propietarios, miembros y visitantes del sitio pueden ver los datos de uso de este, pero cada uno con restricciones específicas según su rol; por ejemplo, los visitantes no pueden ver datos históricos con más de 90 días. De modo que, en esta especie de bitácora que usan los foros, sitios y blogs se puede ver cuántas veces los han visitado, quiénes han accedido a ellos y la información sobre cómo interactúan los usuarios (si los comparten, los visualizan, los cambian de ruta o los editan), la ubicación usada para hacer la visita e inclusive se podría obtener toda la información para ser organizada a manera de tendencias.

Además, en cada uno de los casos mencionados, los propietarios pueden exportar y descargar el informe de uso en formatos como CSV, xml, xlsx y pdf y

combinarlos con programas de análisis masivo de datos y programas de auditoría de eventos.

2.5 Herramientas para la autenticación de documentos electrónicos

2.5.1 Certificados digitales.

> Los certificados digitales se conocen como una parte de la información que se asocia a perteneciente a un autor (autenticación), verificar que no ha sido manipulado ni modificado (integridad), al igual que impide que el autor niegue su autoría (no repudio) mediante validación de la clave pública del autor, quedando de esta manera vinculado al documento de la firma (Rangel, 2019, p. 25).

El certificado digital, de llave pública o de usuario, es un documento electrónico, identificado por un número de serie único y con un periodo de validez, el ente emisor, la versión y el algoritmo de firma del certificado. Este es emitido por una entidad de confianza, denominada Autoridad Certificadora (CA por sus siglas en inglés) y vinculado a su propietario con una clave pública. Dicha CA, también hace revocación de los certificados digitales, es decir, con ellas se establece la vigencia del certificado digital, la cual es difundida luego mediante el *Certificate Revocation List (CRL)*, la cual es leída por el sistema del cliente.

2.5.2 Firma electrónica.

Pueden ser códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permiten identificar a una persona, en relación con un archivo de datos, la firma puede darse dentro de la captura de los documentos electrónicos.

2.5.3 Firma digital basada en certificado.

La firma digital se basa en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma o ente certificador. Que en el caso de Costa Rica lo hace el ente certificador que, según el MICIT (2022) es la persona jurídica pública o privada, nacional o extranjera, prestadora del servicio de creación, emisión y operación de certificados digitales. Este certificador realiza

el proceso de certificación que, “es el proceso de creación de un certificado de llave pública para un suscriptor” (BCCR, 2019).

Además, “la firma digital es el conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permita verificar su integridad e identificar en forma unívoca y vincular jurídicamente al autor con el documento” (MICIT, 2022).

La firma digital permite a una entidad receptora probar la autenticidad del origen y la integridad de los datos recibidos; es decir, con ella se representa la autenticidad, integridad y no repudio. La principal diferencia que tiene con una firma electrónica es que la firma digital se tiene que probar (verificar) antes de determinar que se trata de un mecanismo confiable.

Después de la creación del certificado digital y su respectiva firma digital, se tiene la herramienta para autenticar los documentos digitales que, de acuerdo con el MICIT (2022), tendrán un valor igual al firmado manualmente con el puño y letra.

2.5.4 Código seguro de verificación (CSV).

> Las copias realizadas en soporte papel de documentos públicos administrativos emitidos por medios electrónicos y firmados electrónicamente pueden tener la consideración de copias auténticas siempre que incluyan la impresión de un código generado electrónicamente u otros sistemas de verificación que permitan contrastar su autenticidad mediante el acceso a los archivos electrónicos de la Administración Pública, órgano o entidad emisora (Rangel, 2019, p. 25).

2.6 Estándares de administración de información electrónica

2.6.1 BSI BS 10008.

Es un estándar británico creado en el 2008 y recientemente revisado en el 2020, que describe las mejores prácticas para la implementación y operación de sistemas de gestión de información electrónica, incluyendo almacenamiento y transferencia de la información. Está diseñado para evitar las trampas legales del almacenamiento de información. También, describe las mejores prácticas para transferir información electrónica entre sistemas y migrar registros en papel

a archivos digitales. Además, brinda pautas para administrar la disponibilidad y accesibilidad de cualquier registro que pueda ser requerido como prueba legal.

Capítulo 3. Marco Metodológico

3.1 Tipo de Investigación

El tipo de investigación del caso en estudio es aplicada debido a que esta, “se caracteriza porque, busca la aplicación o utilización de conocimientos adquiridos, a la vez que se adquieren otros" […] la cual “usa el conocimiento y los resultados de la investigación como una forma rigurosa, organizada y sistemática de conocer la realidad” (Vargas, 2009, p.6).

3.2 Alcance investigativo

Dado el contexto de la presente investigación se consideran los siguientes tipos:

3.2.1. Exploratoria.

Se entiende que este tipo de pesquisa “atiende aspectos poco conocidos, se propone ofrecer claridad sobre temas que no son comunes” (Hernández, 2014, p.91). En este caso, no hay investigaciones que hagan referencia a la estructura de seguridad detrás del acceso, eliminación, edición y comunicación de expedientes digitales asociados a perfiles profesionales en la administración pública, especialmente si se habla de esfuerzos relacionados en el área de seguridad y más aún a nivel de una institución intergubernamental. Esta arista relacionada a los expedientes digitales no ha sido suficientemente explorada, es relativamente desconocida.

3.2.2. Descriptiva.

Por otro lado, esta investigación se puede tomar como descriptiva. Esta: “busca especificar propiedades importantes de personas, grupos, comunidades o cualquier otro fenómeno que se someta a un análisis" (Hernández, 2014, p.92). En cuyo caso, este trabajo considera el estudio y análisis de los expedientes digitales, sus propiedades, así como las características de las personas que los

comparten y los usan y en general de los medios que albergan los expedientes digitales, entre otros puntos. El trabajo de investigación pretende analizar el grado de seguridad que poseen los expedientes digitales y los documentos electrónicos que estos contienen.

3.3 Enfoque

Se propone un enfoque cualitativo, ya que lo que se intenta en la investigación es adentrarse en la realidad, tampoco se conoce de la subjetividad que se genera a nivel social en la organización estudio. Además, todos los conceptos se vuelven parte del proceso de investigación.

Asimismo, el enfoque pretende tener un método inductivo (de lo específico a lo general) que incluye la técnica de entrevista estructurada.

3.4 Diseño

Mediante el diseño se pretende visualizar de una manera más práctica las respuestas a las preguntas de esta investigación y poder cumplir con los objetivos previstos. “El término diseño se refiere al plan o estrategia concebida para obtener la información que se desea con el fin de responder al planteamiento del problema” (Hernández, 2014, p.128).

De acuerdo con los diseños establecidos por Hernández (2014) se tienen diseños para la investigación experimental y no experimental. De tal manera que el presente estudio se trata de uno no experimental, porque se enfoca principalmente en diagnosticar una situación presente en el ICAP a la fecha y de esa manera proponer una solución para el diseño de una arquitectura de seguridad para sus expedientes digitales; se podría decir que el diseño más apropiado tendría que seguir las características de un diseño transversal exploratorio, con este se puede “comenzar a conocer una variable o un conjunto de variables, una comunidad, un contexto, un evento, una situación. Se trata de una exploración inicial en un momento específico. Por lo general, se aplican a problemas de investigación nuevos o poco conocidos” (Hernández, 2014, p.155).

3.5 Población y muestreo

La población meta es de cualquier género (hombre, mujer, intersexual, transexual) con un rango de edad que varía de entre los 30 a los 60 años.

Adicionalmente son personas que van desde el área Administrativa, Contables, Financiera hasta la Gerencia Técnica y de Tecnologías de la Información (TI). También, esta población tiene una antigüedad laboral de entre los 2 a los 10 años. Además, la investigación se enfoca en un escenario en el cual el sector más impactado sea el de TI.

3.6 Instrumentos para la recolección de datos

Entiéndase como la recolección de datos a la forma en que se reúne la información que se empleará. Es importante considerar que todos los datos sean útiles para alcanzar los objetivos propuestos en la investigación, para lo cual se debe proceder de la siguiente manera:

Selección de las situaciones e individuos que se observarán y/o entrevistarán. O bien la selección de otras posibles fuentes de información haciendo uso de instrumentos como entrevistas, conversación informal y observación.

- Aplicación de los instrumentos de recolección de datos
- Análisis de los datos obtenidos con los instrumentos.
- Preparación de las medidas obtenidas con los instrumentos.

A continuación, una descripción de los instrumentos a utilizar:

✓ **Entrevista semiestructurada**

“El propósito de las entrevistas es obtener las respuestas en el lenguaje y perspectiva del entrevistado” (Hernández, 2014, p.405).

Este tipo de entrevista se pretende aplicar al Gerente de la Unidad de Tecnologías de Información y Comunicación, a quien se le consulta y hace una grabación para posteriores anotaciones. Por tratarse de una entrevista semiestructurada se espera que en el transcurso de ésta, surjan nuevas preguntas para realizarse a los participantes y así aporten datos para el análisis de la información que solventa los objetivos. Para conocer las preguntas por realizar, se puede ver el Anexo 1.

Para la aplicación de este instrumento, se ha de considerar terminar la entrevista enviando una nota o presente como agradecimiento por la participación.

El tipo de preguntas que ha de contemplar la entrevista son: generales, para ejemplificar y estructurales.

Se utilizará la guía expuesta en el Anexo 1 de este documento.

✓ **Observación**

Mediante este instrumento, se pretende observar principalmente el ambiente físico, para determinar la distribución, disposición de los equipos físicos, regulación de la temperatura, los dispositivos de seguridad, entre otros. También, mediante la observación se desean identificar los procesos de liderazgo, las jerarquías, frecuencia de interacciones y observar a las personas el conocer mejor a qué se dedican, la manera de desenvolver sus funciones, los medios que usan para comunicarse y lo que puedan usar para contribuir con la seguridad de los activos en la oficina. Incluso, se desea observar los artefactos que utilizan, los cuales contribuyen a asegurar o vulnerar la información que se gestione en la oficina.

En conclusión, una salida esperada mediante este instrumento sería un mapa de relaciones entre el personal de las oficinas que se pretenden observar, estas son la Contable y Financiera, la Administrativa y la Gerencial de TI.

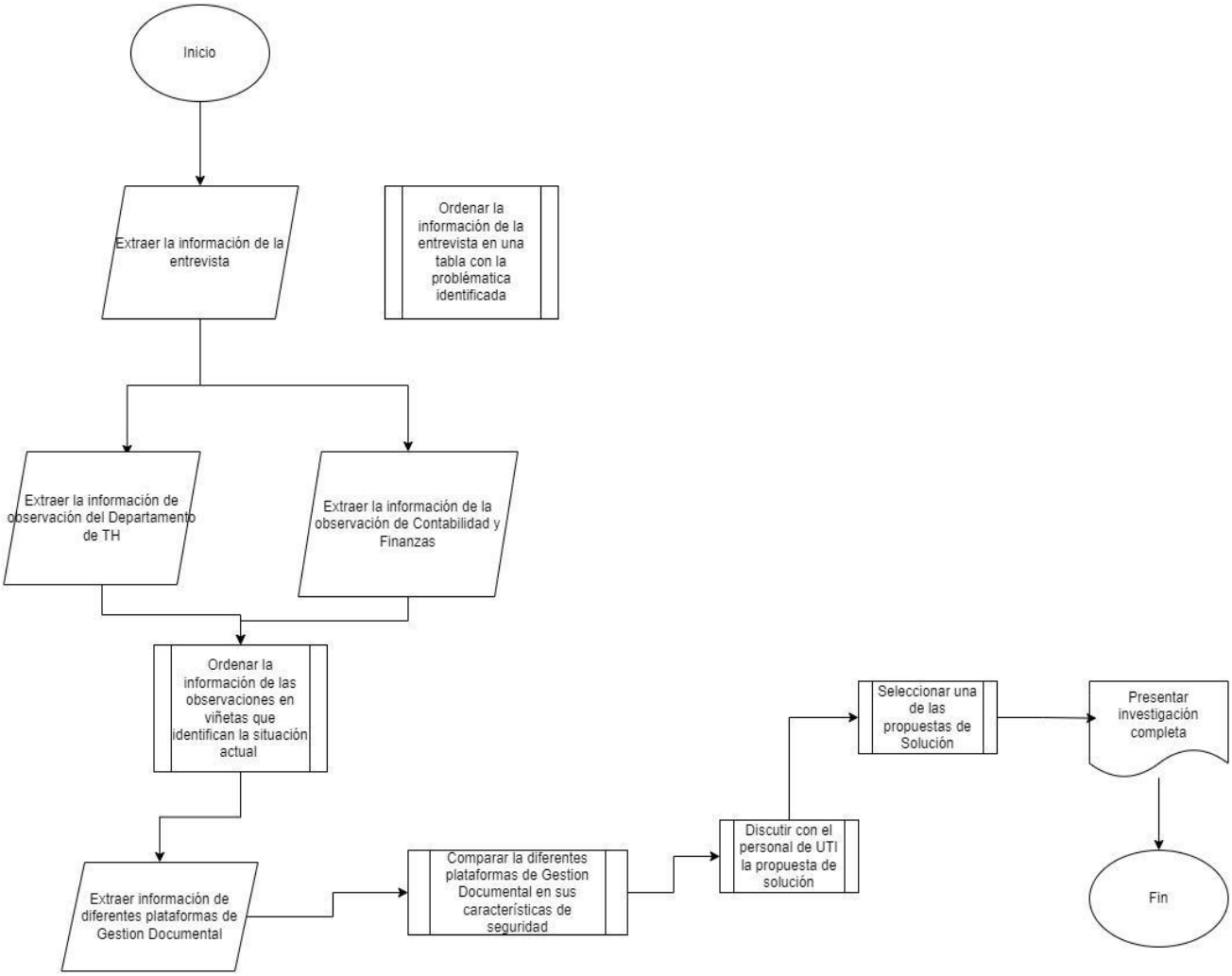
Por lo demás, para la aplicación de este instrumento, se utilizará la guía expuesta en el Anexo 2 de este documento.

3.7 Técnicas de Análisis de Información

Como parte del proceso general de análisis de la información se realiza lo visualizado en la Figura 12:

Figura 12

Diagrama de flujo del Análisis de la información



Capítulo 4. Análisis del diagnóstico

La sección a continuación tiene por objetivo recopilar información que permita analizar todo el proceso para diseñar una estructura de seguridad para los expedientes electrónicos del ICAP.

Para realizar el diagnóstico, se realizaron 4 entrevistas al Gerente de UTI (Unidad de Gestión de Tecnologías de la información y la comunicación), el cual tiene la responsabilidad de coordinar y administrar la arquitectura de Redes y la seguridad de los usuarios y servidores del ICAP en Costa Rica y dos días de observaciones en dos lugares distintos: Contabilidad y Finanzas y Talento

Humano. Con respecto a las entrevistas, se consigue la mayor cantidad de información acerca de la situación actual: programas y servicios usados de la nube, ciclo de vida de los expedientes, arquitectura que rodea los expedientes actualmente y servicios de seguridad complementarios que puedan o no estar usando para asegurar los datos en reposo.

4.1 Análisis de Entrevistas

A continuación, se presenta el análisis de algunas de las respuestas obtenidas como parte de la primera entrevista.

Tabla 5

Análisis de respuesta de la primera entrevista

Pregunta	Respuesta	Problema identificado	Alternativa de solución
¿Conoce los componentes principales que conforman un expediente digital?	No.	No puede existir una estructura de seguridad bien definida alrededor de algo que no es bien conocido.	Educar sobre los componentes principales y dar pautas generales sobre cómo crear los expedientes digitales a los encargados de la implementación de la estructura de seguridad de éstos.
¿Está familiarizado con los 3 pilares de seguridad de la información?	No.	No sería posible establecer todos controles de manera detallada que son pertinentes a los tres pilares de seguridad a causa del desconocimiento parcial de ellos.	Educar acerca de los 3 pilares de seguridad a los encargados de la implementación de la estructura de seguridad de los expedientes digitales.
¿Existe alguna política o	Memorandos, mas no hay	Los empleados no tienen una normativa	La solución propuesta es crear una política de

normativa en la institución que refuerce alguno de los pilares de seguridad de la información?	políticas o normativas.	de control de accesos ni una política de seguridad de la información que seguir; solamente conocen de los memorandos. Además, no están actualizados todo el tiempo con respecto a nuevas medidas de seguridad que puedan llevar a cabo para contribuir con la protección de los activos.	seguridad de la información que establezca una línea base y crear otras normas asociadas a los tres pilares de seguridad, por ejemplo, una normativa de respaldos.
¿Cuentan con arquitectura *OnPremise* o *Cloud*? ¿Cuál cree más valiosa según lo que ha visto en su organización?	Cloud y se considera más valiosa que *OnPremise*.	No existe problemática en este caso; no obstante, la estructura actual de nube no tiene configurados muchos aspectos pertinentes a los 3 pilares de seguridad de la información.	La estructura propuesta va a incluir en todo el ciclo de vida de los expedientes digitales la integridad, la confidencialidad y la disponibilidad de estos, empezando por acciones que promuevan la integridad en el expediente hasta la comprobación de permanencia de los archivos en los expedientes digitales.
¿Qué aspectos considera usted	Sistema de control para	De acuerdo con la respuesta, la	La única alternativa para solucionar la

necesarios reemplazar o mejorar? ¿Cuáles serían los más importantes para la organización?	proyectos, sistema para control y seguimiento documental con una arquitectura basada en la Intranet, considerando los niveles de seguridad.	implementación de este proyecto no tiene prioridad; por tanto, una vez terminada la investigación, es probable que no haya un seguimiento continuo.	problemática de que el proyecto no sea sólo archivado sin efecto en la institución es que siempre se recuerde de la importancia sobre la implementación de este.
Si tuviera que establecer un lugar para almacenamiento de datos en reposo, ¿cuál sería esa ubicación?, ¿por qué?	En Cloud y en discos duros físicos almacenados en el UTI.	Los expedientes digitales pueden estar en determinados momentos en reposo; por tanto, tendría que considerarse si es necesario incurrir en gastos adicionales por expansión del espacio y por el tiempo de almacenamiento en la nube.	El tiempo de almacenamiento de los documentos electrónicos como de los expedientes digitales, puede ocasionar que se vaya reduciendo el espacio disponible de almacenamiento por lo que sería posible tener que pagar por espacio adicional.
¿Cómo considera que sería mejor hacer la visualización de los documentos electrónicos de los expedientes digitales?	Contratos en PDF, *Word Online* / *Work Desktop*, Office 365.	No existe una problemática real en este caso. El único posible impacto sería que la licencia para el software de visualización de documentos	Siempre verificar que las licencias de los programas para visualización de documentos electrónicos se encuentren al día y sean las actas para el uso que se les requiere dar.

		electrónicos caduque o no sea la apropiada.	
¿Conoce acerca de controles de indexación para expedientes digitales?	No.	El desconocimiento de los controles de indexación puede traer brechas en la disponibilidad y la integridad de los expedientes.	Educar a los implementadores del proyecto acerca del índice electrónico que compone un expediente digital.
¿Cuentan con licencias de Microsoft para tener un SSIS?	No.	No se podría usar un *SQL Server Integration Services* para que se puedan importar datos de fuentes diferentes a *SQL Server*.	La solución propuesta sería adquirir la licencia del producto si fuera requerido la migración de datos.
¿Tienen acceso a algún programa o software de visualización de datos de forma analítica mediante gráficas u otros elementos visuales?	*PowerBI* y Excel.	No existe una problemática real en este caso. El único impacto podría ser que la licencia con los softwares usados para analítica caduque.	Siempre verificar que las licencias de los programas para analítica se encuentren al día y que los programas estén con las últimas actualizaciones para evitar recientes brechas de seguridad.
De acuerdo con su experiencia en esta organización, ¿cuáles diría usted que son	Sería el uso de *OneDrive*.	Se considera mantener los documentos en reposo en *SharePoint Online* mientras que cuando no lo estén	Se recomienda dar capacitación acerca de cuándo usar el *OneDrive* y cuándo usar *SharePoint Online*; se recomienda

los medios de almacenamiento más adecuados para salvaguardar expedientes digitales?		sería en *OneDrive*, esto sería problema porque lo ideal es considerar cuándo se requiere compartir el documento con un equipo o varios y cuándo se vuelven relevantes para un proyecto o áreas administrativa, como es el caso de los documentos de los expedientes digitales en cuestión.	especialmente verificar las segregaciones hechas en el *SharePoint* con los respectivos niveles de permisos, así como verificar que los archivos de los expedientes como los expedientes estén compartidos con las personas correctas.
¿Me puede describir de forma detallada el proceso de un documento electrónico desde su ingreso digitalización hasta la visualización de este?	Se crean digitales desde el inicio en forma digital, se imprime, se firma y se escanea y se visualiza con un visor de PDF. Se comparte por medio de *OneDrive* y se envía por correo electrónico, no se encriptan ni	La principal problemática es que no hay un nivel de seguridad adecuado en la impresión, en el escaneo y tampoco en la forma que se distribuyen los documentos electrónicos.	Los índices de los expedientes pueden ser firmados digitalmente. Además, se debe hacer comprobación de que la plataforma usada para compartir los documentos de los expedientes sea el SharePoint. Los documentos digitalizados para ser añadidos al expediente siempre deben pasar por el proceso de añadirle un hash.

	se añaden notas de seguridad. El trabajo de impresión no es exhaustivo.		
¿Cómo calificaría la seguridad en el intercambio de los documentos electrónicos dentro de la institución en una escala del 1 al 5?	2 Muy bueno – En SharePoint hay segregación.	Se puede mejorar la seguridad en el intercambio, ya que a este momento los documentos en estado electrónico pueden adulterarse ya que no hay un control adecuado de a quiénes se les comparte por medio del *OneDrive*. También, al *SharePoint* no se le han añadido todos los controles de seguridad que la misma herramienta permite.	Se sugiere auditar regularmente los archivos o expedientes compartidos externamente y hacer la correcta configuración de compartir que tiene el *SharePoint;* así como seguir buenas prácticas.
¿Cómo calificaría la seguridad en el intercambio de los documentos electrónicos fuera de la	3 Regular	Se puede mejorar la seguridad en el intercambio, ya que a este momento los documentos en estado electrónico pueden compartirse	Se sugiere crear categorías para la información, usar el etiquetado de los datos, de acuerdo con esas categorías desde la creación del documento.

institución en una escala del 1 al 5?		externamente con personas que no necesariamente requieren ver esa información, especialmente cuando el intercambio es mediante correo electrónico. Adicionalmente, al *SharePoint* no se han añadido todos los controles de seguridad que esta herramienta permite.	También, se recomienda evitar el uso de medios externos como USB o discos duros portátiles. Igualmente, se sugiere añadir los controles de seguridad que aconseja Microsoft para *SharePoint*.

Nota: Elaboración propia.

Durante la segunda entrevista, realizada de manera virtual, se revisó el ciclo de vida de los expedientes digitales, en la cual aparece la problemática de que se habilitó el uso de la política de retención en todos los archivos de las bibliotecas que da Microsoft por defecto, la cual es de 90 días y sin revisión de los accesos que pierden los usuarios de los archivos en este flujo.

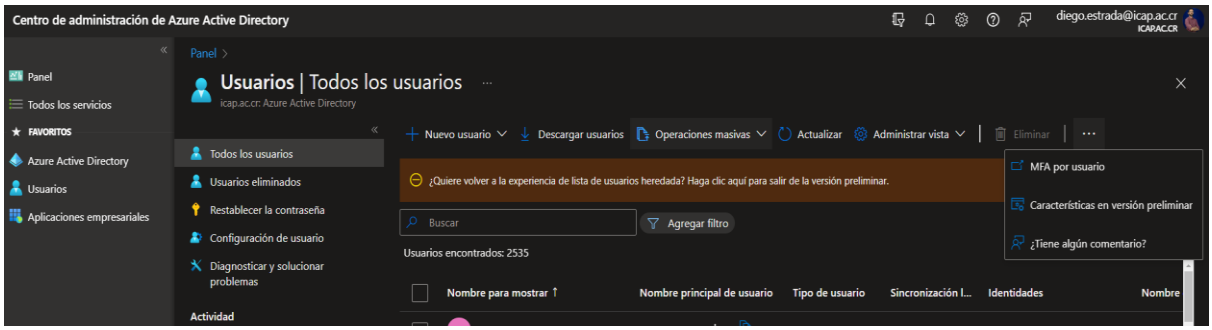
En la tercera entrevista, se discute acerca de la implementación del *Azure Directory* después que la empresa se migró del *Active Directory OnPremise* a la nube; se identifica como problemática que en ese momento el MFA (*Multiple Factor Authentication*) no está implementado al 100% para todos los usuarios de interés, tampoco hay bloqueo o límite de acceso para dispositivos no administrados (acceso condicional basado en dispositivos) o para ubicaciones de red específicas y no hay controles de encriptación para los documentos electrónicos existentes en *SharePoint* como en OneDrive.

Finalmente, en la cuarta entrevista, se revisaron los servicios de los cuales dispone la licencia A3, de allí se distinguen como parte de la solución a la problemática, los servicios que podrían contribuir con la seguridad de la información y por lo tanto de los documentos y expedientes electrónicos:

- Microsoft 365 Defender.
- Prevención de pérdida de datos.
- Azure AD Identity Protection.
- Advance Threat Protection.
- Azure Information Protection.

Figura 13

Todos los usuarios y las configuraciones



Nota: Adaptado de *Configuración del MFA por Usuario*, 2022, 4ta entrevista realizada al gerente de UTIC del ICAP.

La solución que se propone para los servicios existentes que están siendo ignorados actualmente, es que se haga un recorrido a través del portal de *Azure Active Directory* y se revise la configuración del servicio y se realicen las configuraciones que mejor se adapten a las necesidades de protección del ICAP.

4.2 Análisis de las observaciones

A través de las observaciones realizadas, se examinaron las necesidades de los usuarios que acceden a los expedientes digitales; de modo que se identificaron tres factores clave distintos: ambiente físico, ambiente social y humano y los artefactos que utilizan.

Con respecto al ambiente físico, se llegó a las siguientes conclusiones: cada persona en el área tiene un equipo asignado; normalmente la temperatura en las oficinas es regulada por medio de persianas en lugar de usar de manera correcta el sistema de aire acondicionado; en cuanto a la distribución para trabajar y brindar privacidad a los usuarios se puede decir que la distribución es

buena, no existen gafetes electrónicos para abrir puertas y no se usan las puertas cerradas con llave; además, no hay suficientes puertas para asegurar las diferentes áreas.

Con respecto al ambiente social y humano se obtuvieron los siguientes resultados: los procesos de liderazgo son completamente en cascada, pero rápidos, las funciones de los usuarios son de descarga, impresión, archivado, escaneado y visualización de documentos que son compartido mediante el *OneDrive*, *Microsoft Teams* y el correo electrónico. La comunicación entre áreas es constante y diaria. En el área Contable y Financiera, hay un líder y dos asistentes y en el área de Talento Humano hay 3 Coordinadores y 3 asistentes administrativas; los usuarios más frecuentes en este caso serían las asistentes. Los medios de comunicación empleados son el *Microsoft Teams*, el teléfono fijo, en ocasiones el *WhatsApp,* pero sería para comunicaciones más rápidas e informales y desde luego la comunicación frente a frente.

Referente a los artefactos que se utilizan, se lograron obtener las siguientes conclusiones: no hay tarjetas de acceso ni *token* de seguridad. Solo se usa un gafete con foto para identificación de la persona y no se utilizan uniformes como distintivos.

Todas las anotaciones realizadas con respecto a las observaciones se pueden encontrar en los Anexos 3 y 4.

Como parte de un análisis de los datos mencionados con anterioridad, más la investigación de otras brechas genéricas para expedientes digitales, se identificaron los siguientes resquicios que pueden afectar la seguridad de los expedientes digitales a lo largo de su ciclo de vida:

1. Controles de acceso físicos insuficientes, existiendo la amenaza de ingreso a las oficinas de personal no autorizado (especialmente a la oficina donde está el UTI) que aproveche incluso las horas de descanso de los funcionarios.
2. No se comprueban modificaciones sobre los documentos previos al proceso de digitalización.
3. Los archiveros donde se guardan los documentos que no se han digitalizado, usualmente no se encuentran con llave y en algunas ocasiones las llaves están visibles.

4. Algunos documentos quedan a la vista de muchas personas, pues no hay política de escritorio limpio. Además, hay un pizarrón con información sensible como *vouchers* de facturas hechas por el ICAP con firmas de los clientes.
5. Falta de controles de privacidad sobre los documentos electrónicos cuando se comparten externamente.
6. Falta de uso de etiquetas y/o mecanismos de identificación de tipo de información cuando es compartida por correos electrónicos.
7. Ausencia de monitoreo de con quienes se comparte la información de las carpetas compartidas en *OneDrive* como en *SharePoint*.
8. Se distinguió que en ocasiones los gafetes de los usuarios quedaban abandonados en ubicaciones expuestas a personal no deseado.
9. Los usuarios no reciben capacitaciones sobre seguridad de la información ni tampoco se les recuerda de la importancia de no cargar sus identificaciones y en general su colaboración sobre la seguridad física.

Capítulo 5. Propuesta de Solución

La sección de la propuesta de la solución pretende plantear una lista de controles básicos, tecnologías seguras y procesos ordenados para que se pueda diseñar la estructura de seguridad para los expedientes electrónicos de manera que se logre reducir o eliminar el riesgo de pérdidas de datos, accesos no autorizados, incumplimiento con la ley protección de datos personales y distribución a usuarios no autorizados y/o necesarios. La solución propuesta también brinda una posibilidad de llegar a tener documentos y expedientes electrónicos con integridad garantizada.

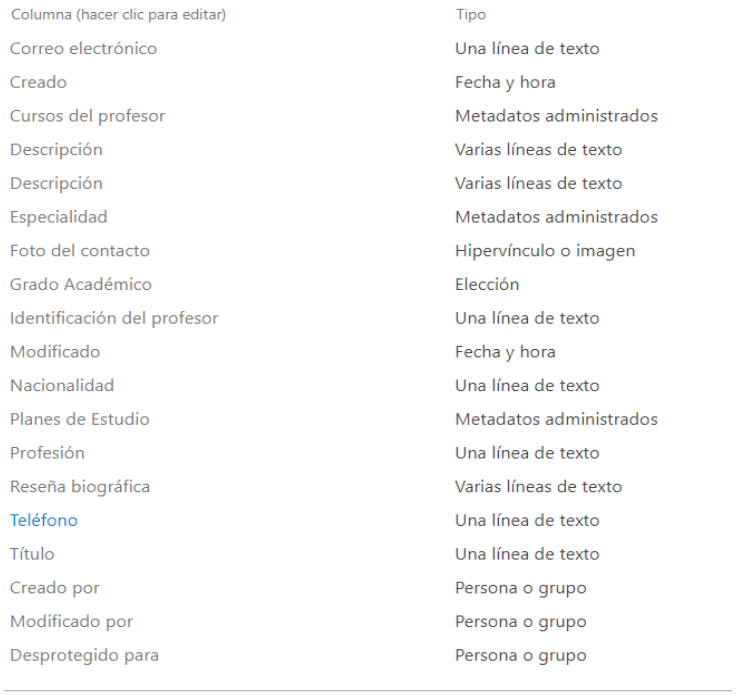
5.1 Estructura del expediente electrónico

Para iniciar con una propuesta clara, primero se dará de manera detallada la estructura del expediente electrónico: uno o varios documentos electrónicos que pueden estar conglomerados o no, el índice electrónico, la firma del índice electrónico y los metadatos del expediente que sean obligatorios (generalmente metadatos administrados) o complementarios. De esta manera el primer paso es crear los expedientes en el medio de almacenamiento con los metadatos previamente configurados por el administrador de TI y los metadatos administrados. Estos últimos se definen como campos obligatorios; asimismo, para hacer una gestión eficiente de los metadatos, las relaciones entre los expedientes electrónicos y estos deben ser permanentes.

Los metadatos obligatorios serían: el identificador que sería definido de forma estándar por los encargados de gestionar la creación del expediente (ejemplo: TH-PR-[# de identificación]), descripción, especialidad, grado académico, nacionalidad, título, profesión y otros que por el tipo de objeto que se usa en SharePoint, en este caso, biblioteca, son añadidos por defectos: creado por (ejemplo: TH, Mariela.rojas@icap.ac.cr), creado (fecha y hora), modificado por (ejemplo: TH, Mariela.rojas@icap.ac.cr), modificado (fecha y hora) y otros. También, están otros metadatos complementarios como el número de entrada de registro usado en el índice electrónico.

Figura 14

Ejemplo de los metadatos que se están empezando a usar para el expediente de un profesor



Columna (hacer clic para editar)	Tipo
Correo electrónico	Una línea de texto
Creado	Fecha y hora
Cursos del profesor	Metadatos administrados
Descripción	Varias líneas de texto
Descripción	Varias líneas de texto
Especialidad	Metadatos administrados
Foto del contacto	Hipervínculo o imagen
Grado Académico	Elección
Identificación del profesor	Una línea de texto
Modificado	Fecha y hora
Nacionalidad	Una línea de texto
Planes de Estudio	Metadatos administrados
Profesión	Una línea de texto
Reseña biográfica	Varias líneas de texto
Teléfono	Una línea de texto
Título	Una línea de texto
Creado por	Persona o grupo
Modificado por	Persona o grupo
Desprotegido para	Persona o grupo

Nota: Adaptado de *Columnas o Metadatos Configurados para el Expediente Profesores*, 2022, 2da entrevista realizada al gerente del Departamento de UTI del ICAP.

Una vez creado el expediente, se procede a añadir los documentos firmados o que se firmarán luego con el *Adobe Sign*. Los documentos heredan los metadatos del expediente.

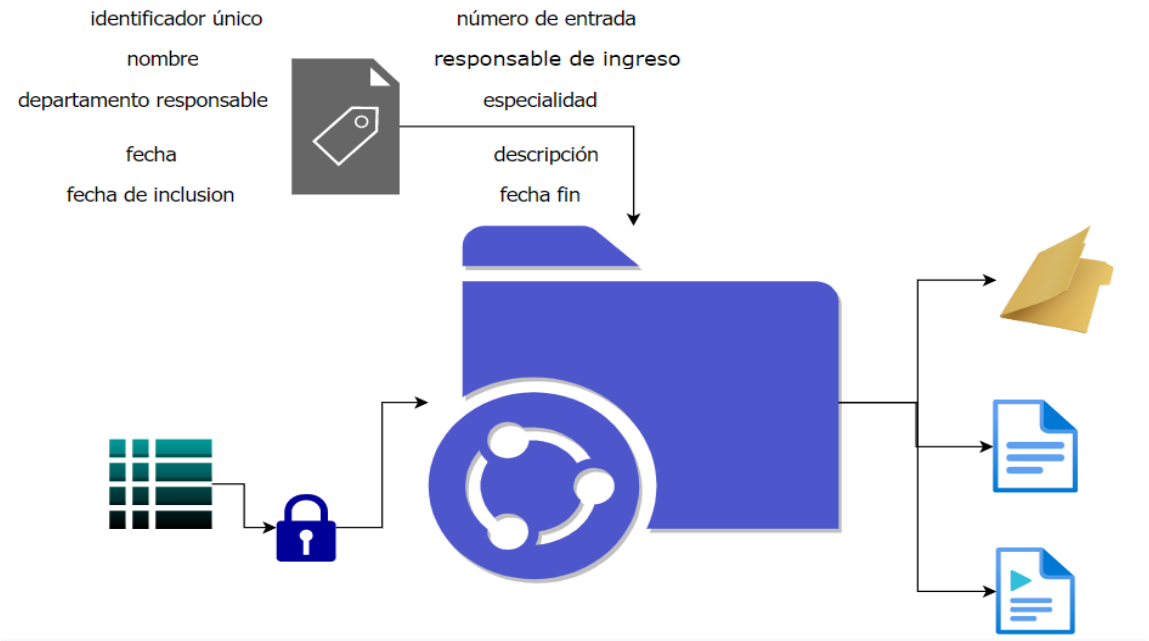
El elemento consecutivo del expediente, el índice electrónico, en adelante conocido como el índice principal, contiene un listado de todos los documentos electrónicos que se incluyen en el expediente. Entre los detalles que este índice debe contener están los siguientes: los identificadores, fecha (metadatos de creado) de inclusión, persona que ingresó el expediente y el número de registro en la inclusión al expediente del documento electrónico.

El siguiente elemento, un índice de búsqueda, que es el que se usa para poder hacer la indexación o el uso de filtros para encontrar documentos dentro del expediente.

Finalmente, el último elemento es la firma del índice principal, la cual es creada previamente por el propietario o las usuarias del expediente.

Figura 15

Estructura del expediente electrónico con algunos de los metadatos



Nota: Elaboración propia.

Por otro lado, cada vez que el expediente sea alterado, varios metadatos van a ser alterados; por ejemplo, cuando nuevos documentos sean añadidos al expediente, los metadatos de “Modificado por” y “Modificado”, van a ser actualizados de acuerdo con la nueva fecha y hora de modificación y la persona responsable de hacer dicha modificación.

Por otra parte, tomando como base lo indicado en el artículo 40 de la Ley del Sistema Nacional de Archivos, la archivalía (el tiempo que el expediente se archiva cuando ya finalizó toda la tramitación) ha de tomar un tiempo de 5 años.

5.2 Tecnologías por utilizar

Este apartado es para indicar las tecnologías que se utilizarán a lo largo del ciclo de vida del expediente electrónico, el cual a su vez debe seguir la estructura sugerida en el apartado anterior. Las tecnologías se deben indicar para la digitalización, creación, visualización, almacenamiento, distribución y archivado.

5.2.1. Medios para visualización de los documentos

Los programas que se utilizan para creación y la visualización segura de los documentos son Microsoft Word online, Microsoft Excel online y Microsoft Power Point online cuando el documento electrónico es creado directamente en el expediente. De igual manera, los documentos se podrán visualizar en esos programas y luego deberán ser convertidos en formato no editable, también se pueden visualizar en los navegadores empleados por los usuarios: Microsoft Edge, Mozilla Firefox y Google Chrome.

Si los documentos electrónicos de tipo de agrupación documental (los que se añaden a expedientes digitales) fueran descargados para ser visualizados localmente y no como parte del expediente, las opciones de visualización serían: el navegador que el usuario tenga por defecto (Microsoft Edge o Chrome) y Adobe Reader.

5.2.2. Medios para digitalización de los documentos.

Para tener los documentos electrónicos, en algunas ocasiones, la organización hace un proceso de digitalización, para lo cual se utilizan las impresoras RICO IMC3000 y RICO IMC300; durante este proceso, los usuarios que tienen acceso a estas deben introducir un código específico para hacer el escaneo; después, indican el correo al que se estará enviando el documento en formato PDF.

5.2.3. Medios de almacenamiento y archivado.

Como parte de esta sección, se ha hecho la Tabla 6 que compara varias funcionalidades básicas y de interés para la implementación de la estructura de seguridad en el Sistema de Gestión documental. Para observar la información de esta tabla, ver los Anexos 8 y 9.

La tabla incluye el SharePoint que es la herramienta actual de gestión documental y que forma parte del Plan A3 de Microsoft para Centros educativos y se destaca que aún no se utiliza para crear de manera específica los expedientes digitales ni tampoco usa aún la recuperación de archivos, ni el *Advanced Thread Protection* [Protección de Amenazas Avanzado] (explicado en este documento más adelante), tampoco la integración con el correo electrónico para subir los documentos y no tiene cambios en los tiempos de retención con respecto a los que dispone por defecto Microsoft. Otro aspecto que actualmente

no considera el SharePoint *online* de la organización es “La configuración de colaboración externa” con las restricciones y asignaciones más seguras.

Tabla 6

Tabla comparativa de software de Gestión Documental

	SharePoint Online	Confluence Cloud	Zoho WorkDrive Empresarial
Recuperación de archivos	X	x	x
Esquema y herencia de metadatos	X	x	
Compartir documentos digitales internamente como externamente	X	x	x
Búsqueda avanzada y simplificada (por contenido y por metadatos)	X	x	
Integración con correo electrónico para añadir los documentos electrónicos	X	x	
Crear y aplicar tiempo de retención para datos	X		x

Controles detallados de acceso	X	x	X
Integración con sistemas anti-malware	X	x	
Integración con programas de visualización de datos de forma analítica mediante gráficas u otros elementos visuales	X	x	
Está en la nube	X	x	x

Nota: Elaboración propia.

Desde luego que el medio de almacenamiento deberá estar correctamente configurado para la colaboración externa. Para obtener la máxima protección de datos (ver instrucciones en el Anexo 6). Esto incluye: configuración de permisos apropiados para un sitio, expediente, carpeta o documento, creación de un nivel de permisos personalizado si es necesario, ajustes de configuración para compartir con dominio específicos, ajustes de herencia de permisos y bloqueos de visibilidad en las búsquedas de documentos a una audiencia meta.

5.2.4. Medios para compartir los expedientes.

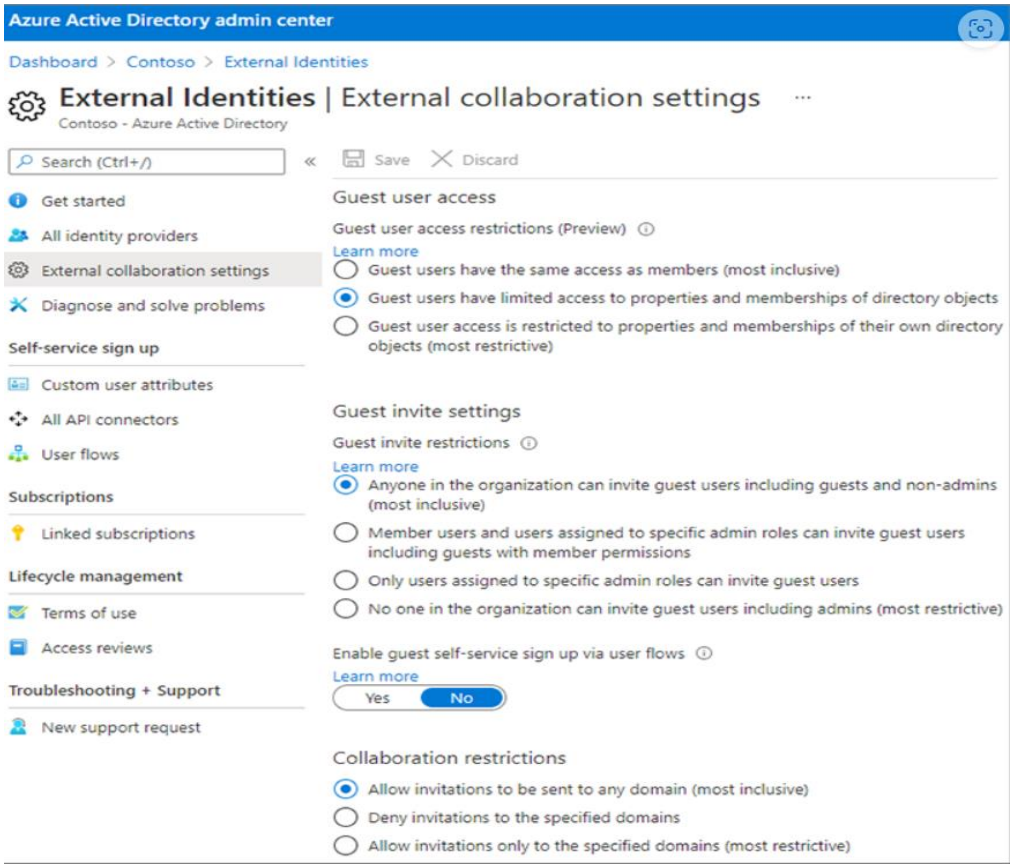
Las mismas herramientas que ha de utilizar el usuario para el almacenamiento de los documentos/expedientes electrónicos serían utilizadas para compartir; asimismo, se complementarían con otros programas como *Exchange* (programa de correo institucional), *Microsoft Teams y Yammer*.

La herramienta seleccionada permite a los administradores configurar que cualquier miembro en la organización pueda tener usuarios invitados sobre un

documento. Por esta razón, es posible para el usuario utilizar un enlace permanente (también conocido como: *sharing-link*) al documento que desea compartir. Para que el usuario miembro tenga la capacidad de compartir con un usuario invitado, el administrador de Azure AD, debe validar que "La configuración de colaboración externa B2B", tenga habilitado "compartir con invitados".

Figura 16

Azure AD External collaboration settings



Nota: Configuración por defecto de la Colaboración Externa de los sitios en SharePoint. Adaptado de *External Collaboration Settings*, 2022, Microsoft docs (https://docs.microsoft.com/en-us/microsoft-365/solutions/collaborate-on-documents?view=o365-worldwide)

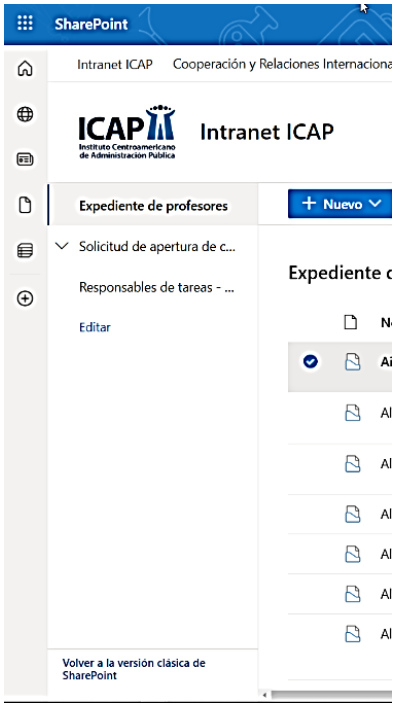
Se recomienda como buena práctica que cuando se cree el enlace permanente para acceder el archivo, este tenga un tiempo de validez predefinido por el usuario que comparte el archivo.

Un caso de uso sería que el usuario de Talento Humano comparta el expediente de un profesor en el área de Administración Financiera a través de

un enlace permanente a un invitado fuera de la organización, para esta acción el usuario tendría los permisos que tiene el invitado sobre el documento y estos pueden variar entre cada invitado.

Figura 17

Vista actual del Sitio de Expediente de profesores



Nota: Adaptado de *Expediente de profesores en el SharePoint Online*, 2022, 3era entrevista realizada al gerente del Departamento de UTI del ICAP.

5.3 Índice y firma del índice del expediente

Es importante recordar que un componente principal del expediente es el índice electrónico que se refiere al contenido de este; a su vez debe contar con un componente que garantice la integridad y la autenticidad del índice y de los documentos electrónicos que conforman el expediente; dicho componente es la firma, la cual para este caso sería la digital basada en certificado, puesto que brinda lo esperado a nivel de seguridad y a la vez legalidad a los documentos como medios probatorios.

El mecanismo que se empleará es la firma digital para personas físicas basada en certificado digital, la cual es proporcionada por el Banco Central de Costa Rica (BCCR), esta posee una Autoridad Certificadora. La firma utilizará la información contenida en el *SmartCard* (la llave pública, la llave privada y el certificado digital) que provee el Banco Central.

Además, se proponen dos tecnologías para ser usados como firmadores y verificadores de firmas, el servicio llamado Gaudi y el servicio de firmas de Adobe, *Adobe Sign* (debido a que el ICAP dispone de la licencia de *Acrobat Standard*).

En el caso de Gaudi, lo pone a disposición el BCCR. Este servicio es contratado por los suscriptores y se recomienda porque cuenta con soporte técnico especializado por parte del BCCR en el uso e implementación, cuenta con documentación técnica de cómo implementarlo en producción como en pruebas; es robusto, no se requieren desarrollos adicionales por parte de los suscriptores para el uso de sus funcionalidades y, lo más importante, ofrece seguridad en la creación del PIN, calidad de interacción con usuarios y otros mecanismos de seguridad que cumplen con los estándares internacionales y mejores prácticas para firma digital (por ejemplo: HTTPS y el algoritmo de SHA-256).

Tabla 7

Tabla de configuración del archivo host

Nombre del sitio	Dirección IP	Puerto
firmador.fdi.cr	X.X.X.38	443
ocsp.sinpe.fi.cr	X.X.X.28	80
fdi.sinpe.fi.cr	X.X.X.28	80
www.firmadigital.go.cr	X.X.X.28	80

Nota: Archivo hosts usado en la configuración del Gaudi en ambiente de pruebas.

Elaboración propia

En el caso de Adobe Sign, es una solución que se instala y configura como un paquete para los sitios de SharePoint. La configuración obligatoria es conectar el SharePoint con *Adobe Sign* con OAuth y otorgar permisos de usuario de SharePoint. Para conectar el SharePoint con *Adobe Sign*, tiene que usar las

credenciales de administrador del *Adobe Sign* y las credenciales del usuario administrador del Office 365.

Para que los usuarios puedan firmar deben estar registrados en la solución *Adobe Sign* y tener al menos permisos para editar en el documento o expediente electrónico en SharePoint.

Toda la documentación sobre cómo hacer la conexión de *Adobe Sign* con SharePoint se encuentra disponible en las páginas de ayuda de Adobe.com y el soporte para el producto es línea a través de esta empresa.

Por otro lado, para la creación del índice, se estarán usando dos maneras: una es mediante cambios en la configuración de bibliotecas en *SharePoint online* y la otra es mediante un reporte generado en Excel. El índice creado en SharePoint online es usado para búsquedas rápidas y otro, sería el índice principal del expediente, el cual llevaría la firma digital proporcionada por el BCCR.

5.4 Lineamientos clave para la estructura de seguridad

Esta sección tiene por objetivo establecer los aspectos de seguridad que deben rodear el medio de almacenamiento para expedientes y documentos electrónicos protegidos. Se trata del Sistema de Gestión Documental llamado *SharePoint Online* que está dentro de toda la arquitectura de nube de Microsoft Azure. Estos aspectos son: autenticación, autorización, integridad, no repudio y disponibilidad.

5.4.1. Autenticación.

El administrador debe tener la capacidad de configurar cuáles usuarios tendrán acceso al expediente abierto y al expediente cerrado.

Para esto el administrador estaría haciendo uso del *Azure Active Directory (Azure AD) Identity Provider* (IdP), en donde tendrá configurado para todos los usuarios el Factor Múltiple de Autenticación (MFA) y se estarían monitoreando los eventos de inicio de sesión y los registros de auditoría (más adelante son explicados estas dos funcionalidades).

También, se bloqueará la autenticación a las aplicaciones que no usen autenticación moderna (ejemplo: bloquea el acceso a Microsoft Office 2010).

5.4.2. Autorización.

El administrador debe tener la capacidad de configurar cuáles usuarios podrán alterar el expediente abierto, indicar si pueden cambiar los metadatos preestablecidos o no y si el usuario puede subir los documentos electrónicos al expediente o si sólo puede leerlos. Para esto, se han creado grupos en SharePoint, por defecto se crean tres grupos con sus propios niveles de permisos: propietarios, miembro y visitantes (Los grupos de Azure AD son diferentes a los grupos de *SharePoint*). Es importante revisar que estos grupos se ajusten a los usuarios del ICAP, pero en caso de no ser así es muy posible que sea requerido crear nuevos grupos y asignarles los respectivos niveles de permisos.

Figura 18

Ejemplo de una plantilla de grupos y niveles de permisos por defecto

SharePoint groups	Default permission level	Applies to team sites
Approvers	Approve	No
Designers	Design, Limited Access	No
Hierarchy Managers	Manage Hierarchy	No
<site name> Members	Edit	Yes
<site name> Owners	Full Control	Yes
<site name> Visitors	Read	Yes
Restricted Readers	Restricted Read	No
Style Resource Readers	Limited Access	No
Quick Deploy Users	Contribute	No
Translation Managers	Limited Access	No

Nota: Adaptado de *Default SharePoint Groups* [Grupos por defecto de SharePoint], 2022, Microsoft docs (https://docs.microsoft.com/en-us/sharepoint/default-sharepoint-groups).

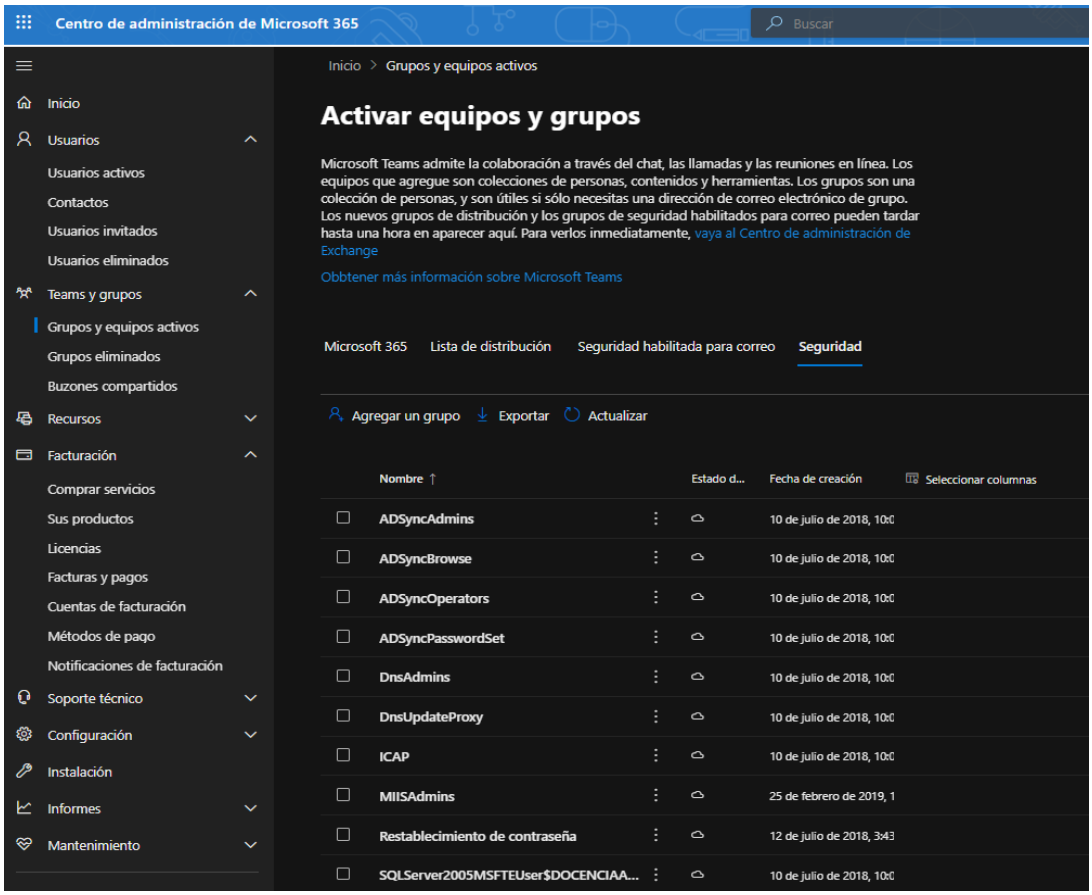
Por otro lado, en Microsoft 365 ya existen los grupos de seguridad, los cuales serán asignados a los de *SharePoint* para no tener que crear así nuevos grupos de seguridad. La Figura 19 muestra los actuales grupos de seguridad.

Adicionalmente, en Azure AD se recomienda crear políticas condicionales de acceso basadas en dispositivos, dominio (para compartir externamente) y de red (para un rango de direcciones IP específicos cuando se trate de un grupo con acceso a los datos más pequeño) para bloquear o limitar el acceso en dispositivos fuera de la administración de TI.

También, a nivel de autorización, el expediente cuenta con el índice electrónico, el cual tiene la firma basada en certificado respaldado por la Autoridad Certificadora del Banco Central.

Figura 19

Grupos de seguridad creados en Office 365



Nota: Adaptado de *Grupos de seguridad del Centro de administración de Office 365*, 2022, 4ta entrevista realizada al gerente de UTIC del ICAP.

También, se podrá tener configurado Identity Protection [Protección de identidad] para proteger las aplicaciones de inicios de sesión considerados riesgosos.

Una buena práctica es que cuando se trate de usuarios nuevos en el *SharePoint*, pendientes de ser entrenados, se les asigne solo a sitios, documentos, carpetas y expedientes donde solo los usuarios que pertenecen al grupo de propietarios puedan compartir. Otra es revisar la herencia de permisos al añadir nuevos usuarios, pues puede ser necesario romper con la herencia de permisos en caso de que ese usuario no requiera los mismos del grupo al que está siendo asignado.

5.4.3. Integridad de los documentos electrónicos.

Mantener la integridad del expediente electrónico mediante la firma digital en el índice electrónico, o bien en los documentos electrónicos, la cual pudo ser añadida con el software firmador.

Además, habiendo diferentes grupos de seguridad en el *SharePoint* se consigue garantizar que solo los usuarios que se les ha dado permisos de edición puedan afectar la integridad del expediente.

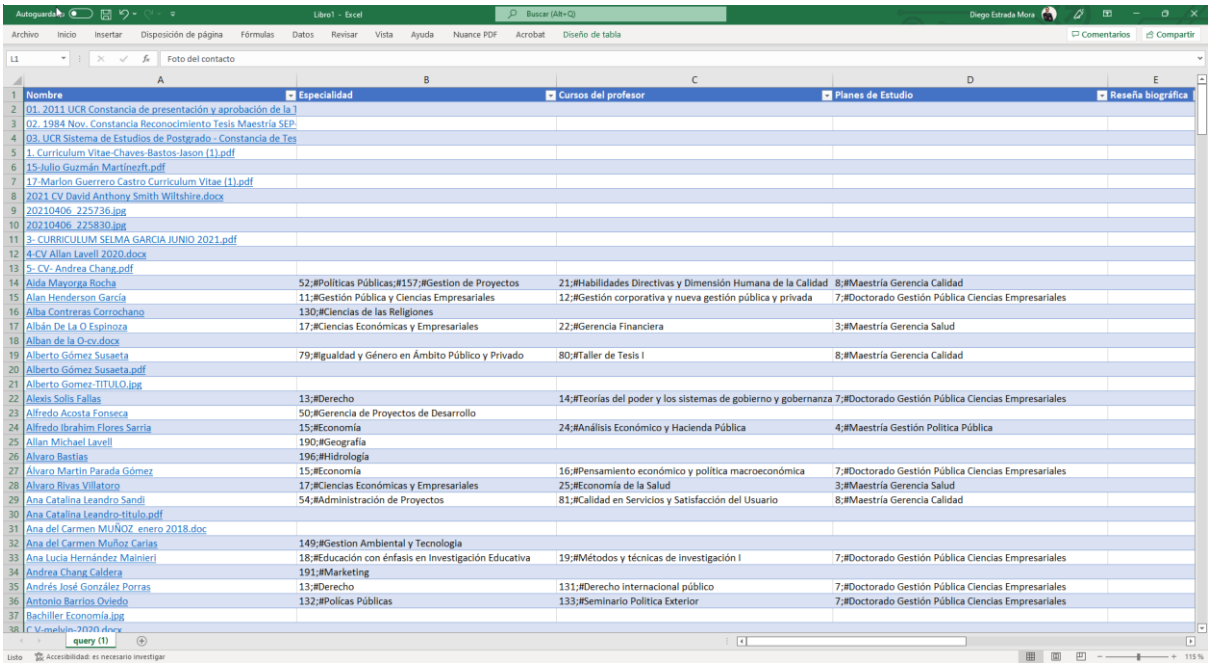
5.4.4. No repudio.

Mantener el no repudio del documento y del expediente electrónico mediante la firma electrónica del índice electrónico. Además, una vez que se dé por cerrado el expediente, quedará registrado el usuario encargado del cierre.

Asimismo, gracias a la existencia de metadatos obligatorios en el *SharePoint online* se logran registrar las acciones del grupo o usuarios, como es la operación de alterar cualquier contenido del expediente. Los datos que quedan registrados son: Modificado (fecha y hora) y Modificado por (Persona o Grupo). Eventualmente se pueden filtrar esas columnas y exportar los resultados del filtrado en Excel o a formato CSV (*comma-separated values*).

Figura 20

Ejemplo de reporte filtrado usando el filtro de año



Nombre	Especialidad	Cursos del profesor	Planes de Estudio	Reseña biográfica
01. 2011 UCR Constancia de presentación y aprobación de la T				
02. 1984 Nov. Constancia Reconocimiento Tesis Maestría SEP.				
03. UCR Sistema de Estudios de Postgrado - Constancia de Tes				
1. Curriculum Vitae-Chaves-Bastos-Jason (1).pdf				
15-Julio Guzmán Martínezft.pdf				
17-Marlon Guerrero Castro Curriculum Vitae (1).pdf				
2021 CV David Anthony Smith Wiltshire.docx				
20210406_225736.jpg				
20210406_225830.jpg				
3- CURRICULUM SELMA GARCIA JUNIO 2021.pdf				
4-CV Allan Lavell 2020.docx				
5- CV- Andrea Chang.pdf				
Aida Mayorga Rocha	52;#Políticas Públicas;#157;#Gestion de Proyectos	21;#Habilidades Directivas y Dimensión Humana de la Calidad	8;#Maestría Gerencia Calidad	
Alan Henderson García	11;#Gestión Pública y Ciencias Empresariales	12;#Gestión corporativa y nueva gestión pública y privada	7;#Doctorado Gestión Pública Ciencias Empresariales	
Alba Contreras Corrochano	130;#Ciencias de las Religiones			
Albán De La O Espinoza	17;#Ciencias Económicas y Empresariales	22;#Gerencia Financiera	3;#Maestría Gerencia Salud	
Alban de la O-cv.docx				
Alberto Gómez Susaeta	79;#Igualdad y Género en Ámbito Público y Privado	80;#Taller de Tesis I	8;#Maestría Gerencia Calidad	
Alberto Gómez Susaeta.pdf				
Alberto Gomez-TITULO.jpg				
Alexis Solís Fallas	13;#Derecho	14;#Teorías del poder y los sistemas de gobierno y gobernanza	7;#Doctorado Gestión Pública Ciencias Empresariales	
Alfredo Acosta Fonseca	50;#Gerencia de Proyectos de Desarrollo			
Alfredo Ibrahim Flores Sarria	15;#Economía	24;#Análisis Económico y Hacienda Pública	4;#Maestría Gestión Política Pública	
Allan Michael Lavell	190;#Geografía			
Alvaro Bastias	196;#Hidrología			
Álvaro Martín Parada Gómez	15;#Economía	16;#Pensamiento económico y política macroeconómica	7;#Doctorado Gestión Pública Ciencias Empresariales	
Alvaro Rivas Villatoro	17;#Ciencias Económicas y Empresariales	25;#Economía de la Salud	3;#Maestría Gerencia Salud	
Ana Catalina Leandro Sandi	54;#Administración de Proyectos	81;#Calidad en Servicios y Satisfacción del Usuario	8;#Maestría Gerencia Calidad	
Ana Catalina Leandro-titulo.pdf				
Ana del Carmen MUÑOZ_enero 2018.doc				
Ana del Carmen Muñoz Carias	149;#Gestion Ambiental y Tecnologia			
Ana Lucia Hernández Mainieri	18;#Educación con énfasis en Investigación Educativa	19;#Métodos y técnicas de investigación I	7;#Doctorado Gestión Pública Ciencias Empresariales	
Andrea Chang Caldera	191;#Marketing			
Andrés José González Porras	13;#Derecho	131;#Derecho internacional público	7;#Doctorado Gestión Pública Ciencias Empresariales	
Antonio Barrios Oviedo	132;#Políticas Públicas	133;#Seminario Politica Exterior	7;#Doctorado Gestión Pública Ciencias Empresariales	
Bachiller Economía.jpg				
C V-melvin-2020.docx				

Nota: Adaptado de *Reporte del SharePoint generado en Excel del Expedientes de profesores*, 2022, 2da entrevista realizada al gerente del Departamento de UTI del ICAP.

5.4.5. Disponibilidad.

Se requiere que la información esté disponible siempre en el horario laboral de lunes a viernes de 7 am a 4:30 pm; no obstante, con *SharePoint online*, la información está disponible 24/7, ya que de acuerdo con la política de Microsoft de que el cliente conozca donde se encuentran los datos, estos se encuentran en Estados Unidos y es posible que en el Centro de Administración de SharePoint, se configure la resistencia a datos multigeográfica (explicado en detalle más adelante).

Para apoyar la disponibilidad, cabe destacar que el *SharePoint* cuenta con un historial de revisiones (también conocido como versionamiento) para los documentos; consiste en que el usuario pueda devolverse a la versión original si el documento fue modificado y ya no se desean esos cambios o si los nuevos cambios corrompieron la versión actual.

5.5 Actores involucrados en la estructura de la seguridad de los expedientes digitales

Los actores que van a hacer uso de los expedientes digitales están constituidos por dos personas: la funcionaria encargada de reclutamiento del personal de profesores y la encargada del perfilamiento de los profesionales en educación. Ambas funcionarias pertenecerán al mismo grupo de seguridad de Microsoft 365.

Las usuarias, el o los administradores del expediente y otros usuarios (invitados de la organización) con permisos de edición pueden compartir internamente los expedientes como documentos electrónicos.

Por otro lado, estas funcionarias tendrán capacidad de compartir los expedientes digitales con usuarios externos a la organización (usuarios con distinto dominio al de la organización) por lo que se ha de considerar lo siguiente:

- El expediente debe estar cerrado para que no haya una sola posibilidad de edición de este.
- El expediente se podrá compartir utilizando el *sharing-link* que se ha de enviar por medio de un correo electrónico que se encuentre con la correcta etiqueta del tipo de información (ver etiquetas en los lineamientos básicos de seguridad).
- Se recomienda que el *sharing-link* tenga caducidad de uso.

5.6 Funcionamiento del expediente electrónico

La siguiente sección describe los pasos de cómo transcurre el ciclo de vida de los expedientes en el ICAP; gran parte de este ciclo se da en el SharePoint, los pasos del 1 al 4 son parte de los pasos que siguen para añadir documentos a una biblioteca con archivos digitales. El paso 5 es un paso que se deberá añadir como parte de la estructura de seguridad y los pasos del 6 al 10 son recomendados porque brindan mayor robustez y certeza (al ser revisado manualmente) al proceso de los expedientes digitales.

1- Los expedientes son creados mediante la digitalización de los documentos en físico. Generalmente, mediante el escaneo, con el contenido deseado (información de los profesores y el historial de cursos).

La digitalización genera un documento electrónico en formato no editable (PDF).

2- El administrador de TI debe revisar la asignación de los niveles de permisos en los Grupos de *SharePoint*, así como los grupos de seguridad de Microsoft 365.
3- La persona que se asigne como propietaria del sitio será la encargada de crear la clasificación de los expedientes, configurar la ficha de metadatos administrados para el expediente, utilizando los correspondientes metadatos (ver la sección 5.1 donde éstos fueron indicados) y abrir y crear los expedientes en el Sitio de Expedientes.
4- El propietario se encargará de inspeccionar que las usuarias del grupo estén asignadas al Sitio designado para los expedientes electrónicos.
5- El propietario y las usuarias tendrán que crear sus firmas digitales usando el *SmartCard* y luego añadir las firmas al documento usando Gaudi o *Adobe Sign*.
6- Las usuarias del expediente tendrán que crear o cargar todos los documentos que vayan a conformar este expediente; todos los archivos que se carguen al expediente van a heredar los metadatos. Como parte de la creación de los documentos electrónicos usando el mismo *SharePoint Online*, se aconseja que inmediatamente se añada la firma digital. Es importante señalar, que las usuarias tienen el poder de extraer del repositorio el archivo cargado, de modo que, si este fuese extraído, nadie más podría accederlo hasta ser publicado nuevamente.
7- El administrador debe crear un índice de búsqueda usando las opciones de configuración del expediente en el Sitio de SharePoint online, para ver todos los pasos a seguir, ver el Anexo 5.
8- El administrador debe crear un índice con firma electrónica, la forma de hacerlo es haciendo click en **Exportar** y selecciona **exportar a un Excel**, a continuación, indica la ubicación para descargar el reporte (el archivo que se descarga tiene una extensión *iqy* que Excel puede abrir) y lo abre. Una vez abierto el reporte, debe guardarlo con la extensión .xls, no sin antes, haber removido varias columnas como la ubicación o *path*, el tipo de archivo o *item type* y otras columnas innecesarias para el índice, considerando que este debe contener la información sustancial que

compone el expediente ordenado para ver la disposición de los documentos. Finalmente, el administrador debe añadir la firma electrónica al documento que recién guardo (“Indice.xls”) mediante Gaudi y cargarlo al expediente.

9- Una vez que el expediente ya no requiera ser alterado, el expediente será cerrado por las usuarias, indicando la fecha de cierre; de modo que se estarán manteniendo los metadatos, pero se estarán removiendo los permisos de modificación para ellas. Solamente, el o los propietarios podrían cambiar el nuevo estado del expediente para que las usuarias le puedan hacer cambios.

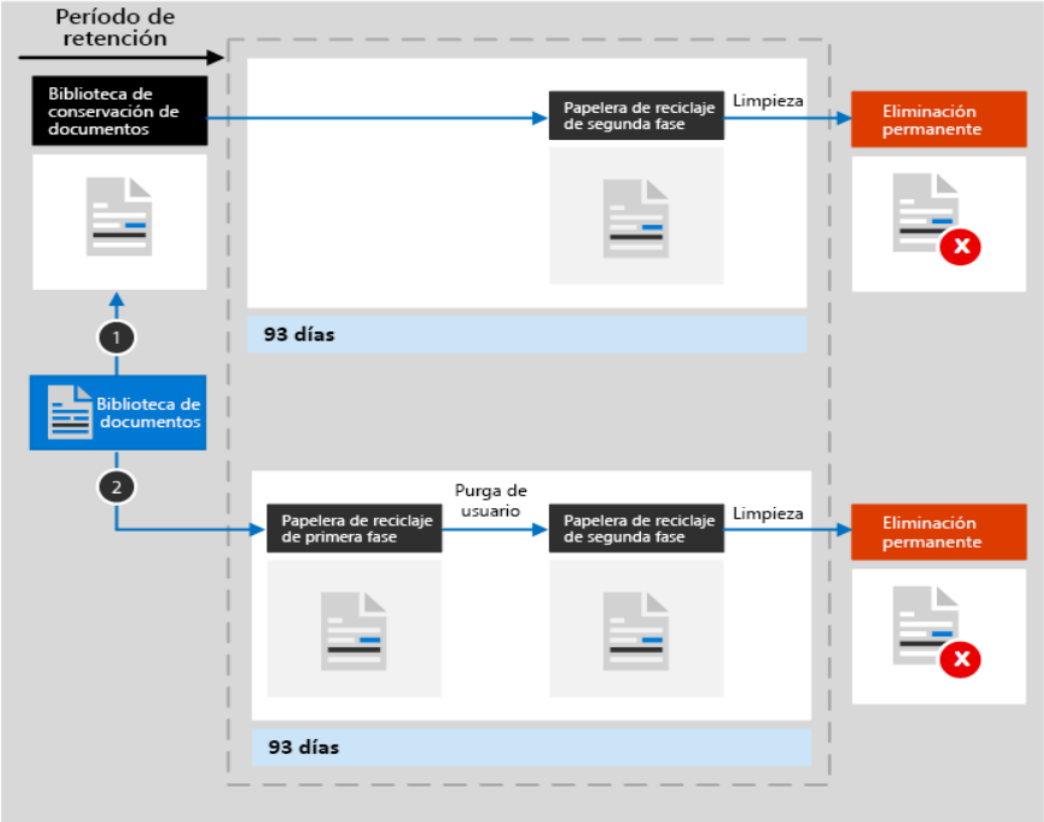
10- El expediente se tiene que quedar un tiempo en ese estado y luego de manera manual, se inicia el proceso de archivaría, en el cual el expediente pasa a Transferencia de archivo General.

11- El propietario selecciona este expediente en la ubicación de Transferencias de Archivo General y selecciona la acción de Archivar, allí le pedirá al usuario introducir la ubicación física de este expediente (un metadato adicional) y lo traslada a la ubicación de Archivo General, donde permanecerá por un período de 5 años.

Actualmente, el administrador de TI tiene puesta la directiva de retención (no hay directiva de etiquetas de retención) para todos los archivos de todas las bibliotecas; la manera en que está funcionando se describe en la Figura 21, en la cual hay hasta 3 papeleras de reciclaje y un periodo configurado por defecto de retención que es por 93 días. La problemática que ocurre en este escenario es que no se está confirmando que el Sitio de SharePoint esté indexado y tampoco se están poniendo las etiquetas de retención en cada biblioteca. Cuando los archivos son purgados a la segunda papelera de reciclaje, el usuario propietario ya no puede moverlos de ahí, solo el administrador de la biblioteca.

Figura 21

Directivas de retención para retener y borrar documentos



Nota: Adaptado de *Funcionamiento de retener y eliminar con retención por* defecto, por Obtenga más información sobre la retención para SharePoint y OneDrive, 2022, Microsoft docs https://docs.microsoft.com/es-es/microsoft-365/compliance/retention-policies-sharepoint?view=o365-worldwide.

Para más información de cómo funciona la retención en SharePoint, ver el siguiente enlace: docs.microsoft.com/es-es/microsoft-365/compliance/retention-policies-sharepoint?view=o365-worldwide

5.7 Lineamientos básicos para una línea de seguridad

Los siguientes son algunos lineamientos y controles básicos que deberían ser incluidos en la aplicación de las Políticas de seguridad de la información (SIP por sus siglas en inglés) una vez que se haya creado el documento:

1. Establecer restricciones de acceso a la información, mediante el etiquetado correcto de esta.
2. Crear la clasificación de la información como Confidencial, Pública, Interna y Confidencial Interna.

3. Proveer las pautas para que los usuarios de la compañía puedan detectar suplantación de direcciones en los correos electrónicos, por ejemplo: crear una política en el correo que indique que el correo viene de un emisor externo y advierte que tenga cuidado descargando imágenes o archivos adjuntos, un ejemplo de este tipo de indicación se puede ver en el Anexo 10.
4. Brindar advertencias de seguridad en los correos que se envían de manera externa con información sensible y/o confidencial de la empresa a dominios de correo externos. Un ejemplo de una nota que se puede usar en estos casos aparece en el Anexo 10.
5. Proveer en cada uno de los equipos controles contra Malware y hacer escaneo de Malware a la información que se encuentre en la nube.
6. Crear una lista de los softwares de pago como los libres, permitidos y bloqueados para los usuarios de la organización.
7. Crear restricciones en los equipos Windows para evitar la instalación de software no autorizados por la organización.
8. Como parte de una supervisión más segura sobre los equipos, deberán tener procedimientos de mantenimientos preventivos para comprobación de que no se encuentren imágenes, videos y audios innecesarios que inclusive puedan contener virus informáticos.
9. Documentar y aplicar controles de dispositivos de almacenamiento externos, estos deben especificar cuáles son aquellos medios que se pueden usar, en qué momentos se pueden usar y cuáles son los equipos que permiten la entrada de estos dispositivos.
10. Redactar y aplicar una política de escritorios limpios, es decir, sin papeles con información sensible o confidencial visibles, sin tarjetas de acceso al alcance de otras personas, sin dispositivos de almacenamiento externo a la vista (incluyendo dispositivos móviles como celulares) y sin anotaciones de trabajo visibles.
11. Imponer estaciones de trabajo seguras, esto implica que los empleados deban cerciorarse de siempre dejar sus equipos bloqueados.
12. Documentar las pautas para hacer la revisión de actualización licencias y parches de seguridad de los programas indicados para visualización de los archivos para evitar interrupciones en las operaciones

regulares como para prevenir vulnerabilidades asociadas a los programas.

13. Documentar los procedimientos para realizar la revisión de actualización licencias y parches de seguridad de los programas indicados para visualización de datos de forma analítica mediante gráficas u otros elementos visuales y así ayudar a mitigar interrupciones en las operaciones regulares como prevenir vulnerabilidades asociadas a los programas.

Además, se debe crear la política de gestión de documentos electrónicos, algunas pautas que deben de estar incluidas en esa son:

1. Definición del alcance y ámbito de aplicación de las políticas.
2. Se deben crear procedimientos a seguir para la transferencia de información ya sea internamente como externamente (Tomar en cuenta algunas de las pautas indicadas en la sección 5.4).
3. Todos los documentos electrónicos o enlaces de documentación electrónica compartidos en correos o mensajería instantánea estarán sujetos al etiquetado con base en las categorías establecidas para la clasificación de la información.
4. Tener constancia de las solicitudes recibidas y atendidas respecto a la remisión y puesta a disposición de los expedientes electrónicos; en este caso, sería mediante el correo electrónico y en algunos casos el historial de conversaciones de *Microsoft Teams*.
5. Tener definido cuando se pueden eliminar los documentos electrónicos y los expedientes para proceder a hacerlo con mayor seguridad.
6. Definir los roles de los actores involucrados: Las personas de interés en la política de gestión de documentos electrónicos y otros responsables de la aprobación de políticas de gestión de documentos y responsables de la conservación y uso de documentos electrónicos.
7. Actuaciones de supervisión y auditoría de los procesos de gestión de documentos.

8. Proceso de revisión del contenido de la política con el fin de garantizar su adecuación a la evolución de las necesidades de la gestión de documentos.

Adicional a las pautas anteriores, es importante para la organización que se creen políticas de control de acceso, entre ellas: tener un *log-on* (un cierre de sesión) seguro que evite que los usuarios dejen la sesión abierta en el navegador, indicar cuáles son los controles de entrada física de forma escrita y con revisión cada seis meses, crear reglas para el uso correcto del gafete del personal de la institución, configurar un control de acceso, según la ubicación de la red y desde luego colocar cerraduras o lectores de tarjetas de seguridad a los cuartos del departamento de UTI.

También, es necesario contar con una normativa de respaldos que incluya los procedimientos para proteger toda la información electrónica; por ejemplo, que se especifique la frecuencia para revisar la ubicación de los datos en reposo del *Exchange*, *SharePoint Online* y *Microsoft Teams* (actualmente, Microsoft especifica que estos datos están en Estados Unidos). Por otro lado, en caso de que se decidan hacer los respaldos *OnPremise*, se debe indicar cuáles son los dispositivos por utilizar y la ubicación precisa de éstos.

Finalmente, será indispensable tener políticas de auditoría de procesos y documentos que contemplen lo siguiente:

i. Establecer los períodos de auditoría durante el año, habiendo un documento planificador con las actividades a auditar en cada fecha.
ii. Establecer los procesos que deben ser auditados y el tiempo recomendado para la duración con cada uno de ellos, tomando en consideración la documentación que hace parte los procesos seleccionados.
iii. Seleccionar los participantes encargados de llevar a cabo la auditoría de cada proceso.
iv. Indicar los programas que se utilizarán para auditorias como los Log de Eventos de *Azure AD* y los programas que se usarán para revisar los reportes como Excel.

v. Determinar los encargados de generar los reportes de auditoría para que los auditores puedan revisar toda la información.

5.8 Complementos de la estrategia de seguridad

Complementando con la sección anterior, se crea esta sección para indicar otros servicios que refuerzan los tres pilares de la seguridad, los cuales pone a disposición Microsoft 365 para las empresas y centros educativos que son los siguientes:

1. Pérdida de Datos (DLP por sus siglas en inglés): en los distintos servicios que se acceden *online*, un ejemplo, en SharePoint online se pueden crear políticas DLP para identificar documentos y prevenir que estos sean compartidos. Estas políticas son aquellas que se crean para indicar que el archivo tiene información sensible (tarjetas de crédito, datos de salud, etc.) y relevante que debe retenerse y que es delicada de compartir; el punto principal de este servicio es prevenir que la información se pierda o sea robada por compartir inapropiadamente.
2. Resistencia a datos multigeográfica: de acuerdo con la documentación de Microsoft (2022l): “las capacidades multigeográficas de OneDrive y SharePoint Online permiten el control de recursos compartidos, como los sitios de grupo de SharePoint y los buzones de correo de grupo de Microsoft 365 almacenados en reposo en una ubicación geográfica especificada” en este caso, Estados Unidos.

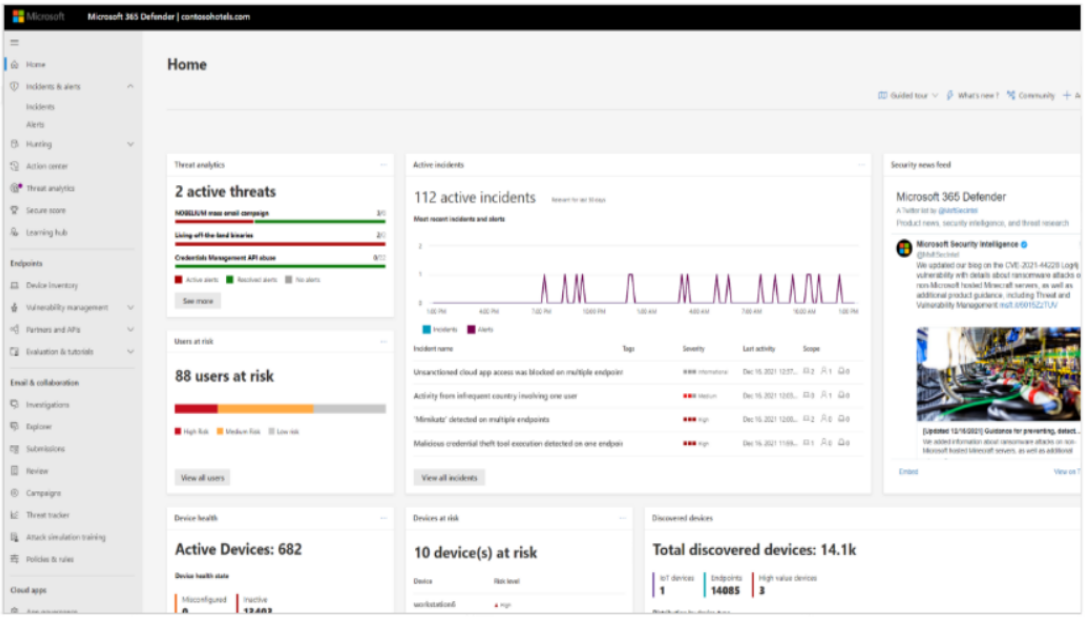
   Por otro lado, el administrador global configura una ubicación de datos preferida (PDL por sus siglas en inglés) para almacenar los datos relacionados de cada usuario, buzón de grupo y sitio de SharePoint.

   La administración de la característica Multi-Geo está disponible a través del Centro de administración de SharePoint.

3. Microsoft Defender para Office 365 y aplicaciones de nube. De acuerdo con la documentación de este servicio de Microsoft docs (2022m), el portal de Microsoft 365 Defender permite supervisar y administrar diferentes tareas de seguridad de las identidades, los dispositivos, las aplicaciones, los datos y la infraestructura desde una sola ubicación.

Figura 22

Portal de Microsoft 365 Defender



Nota: Adaptado de *Acceso del portal de Microsoft 365 Defender*, 2022, Microsoft (https://www.microsoft.com/es-ww/security/business/siem-and-xdr/microsoft-365-defender).

Microsoft Defender para aplicaciones en la nube es un agente de seguridad de acceso a la nube (CASB) que admite varios modos de implementación, incluida la recopilación de registros, los conectores de API y el proxy inverso (Microsoft docs, 2022n, párrafo 1). Las funcionalidades que admite son: monitoreo de las direcciones IP, registro de actividades, valoración de las cuentas y los usuarios, descubrimiento de dispositivos, identificación de la Postura de seguridad, entre muchas otras.

4. Etiquetas de sensibilidad o en inglés *Sensitive Labels*: se trata de una clasificación de la información que se da mediante etiquetas, para brindar los controles de seguridad apropiados, según la clasificación seleccionada. De acuerdo con Microsoft Docs (2022i), las etiquetas de sensibilidad se usan para:
    - Clasificar el contenido sin usar ninguna configuración de protección.
    - Proporcionar configuraciones de protección que incluyan cifrado y marcas de contenido.

- Proteger el contenido de las aplicaciones de Office en diferentes plataformas y dispositivos (Word, Excel, PowerPoint y Outlook en las aplicaciones de escritorio de Office y Office en la web)
- Proteger los contenedores que incluyen *Teams*, grupos de Microsoft.

5. *Azure Identity Protection* (AIP): es una funcionalidad que forma parte de *Microsoft Purview Information Protection* (anteriormente *Microsoft Information Protection* o MIP) […] le ayuda a descubrir, clasificar, proteger y controlar la información confidencial de documentos y correos electrónicos (Microsoft docs, 2022b, párrafo 1).

   Según Microsoft docs (2022c), los administradores de SharePoint pueden definir reglas y condiciones para aplicar etiquetas automáticamente, mientras que los usuarios pueden aplicarlas manual o automáticamente también (párrafo 5).

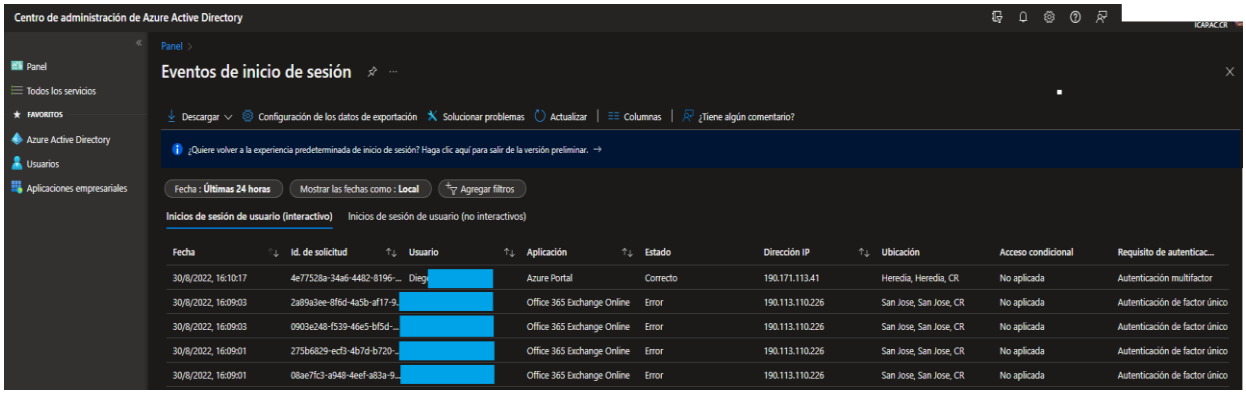
   AIP amplía la funcionalidad de etiquetado y clasificación proporcionada por *Microsoft Purview* con las siguientes capacidades: el cliente de etiquetado unificado, un analizador local, y el SDK. (Microsoft, 2022b, párrafo 3).

   Es importante que el AIP se puede adquirir de forma independiente o a través de un conjunto de licencias de Microsoft, como el plan *Enterprise Mobility + Security* y AIP para Office 365 A3/A5.

6. Eventos de inicio de sesión en *Azure AD*: son los registros que se hacen acerca de los inicios de sesión de los usuarios y sus interacciones con los recursos, en la vista predeterminada se observa: cuál usuario inicio sesión, en qué momento lo hizo, desde dónde lo hizo (aplicación y ubicación geográfica), estado del inicio de la sesión (si hubo un error o no), dirección IP, si se le aplicaba algún acceso condicional y si usaba Autenticación de factor único o Múltiple Factor de autenticación. La vista predeterminada puede ser cambiada para mostrar otros campos como ID del recurso por el Administrador de seguridad, un administrador global, un lector de seguridad, un lector global y un lector de informes.

Figura 23

Eventos de inicio de sesión de Azure AD



Nota: Adaptado de *Los eventos de inicio de sesión del Azure Active Directory*, 2022, 2da entrevista realizada al gerente del Departamento de UTI del ICAP.

Si se produjera un error al iniciar la sesión, se puede indagar más sobre este, dirigiéndose a Información básica del elemento que registro el error, de modo que podrá observar el código de error asociado con la respectiva razón del porque el error.

7. Registros de auditoría: los registros de auditoría de *Azure AD*, brindan información de los registros de actividades del sistema para el cumplimiento. De acuerdo con Microsoft docs (2022p) Las vistas más comunes para el registro de auditoría se basan en: Administración de usuarios, Administración de grupos y Administración de aplicaciones (párrafo 3).

   El informe de actividad de auditoría está disponible en todas las ediciones de *Azure AD.*

   La vista predeterminada muestra en qué momento ocurrió el evento, el servicio que se accede, la categoría que se está viendo afectada, el evento sobre el servicio afectado, el estado del evento, a qué iba destinado dicho evento y el actor que lo realiza. La vista por defecto puede ser cambiada por el Administrador de seguridad, el lector de seguridad, el lector de informes, el lector y administrador global.

8. *Microsoft Defender para Office 365* (*MS Defender* para *Office 365 P2*) y *Exchange Online Protection* (EOP): de acuerdo con la documentación de Microsoft docs (2022d), Microsoft Defender para Office 365:

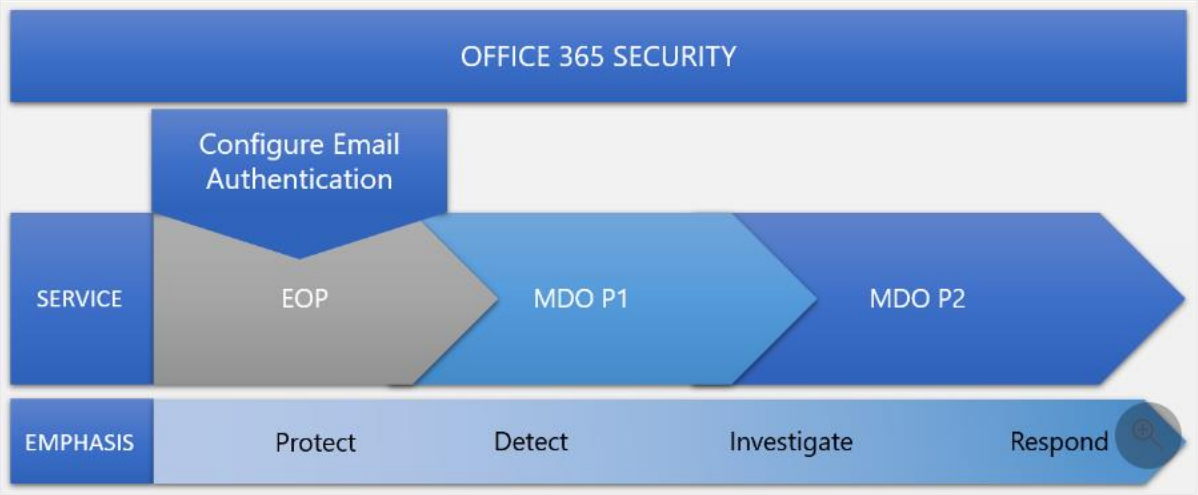
   Previene ataques conocidos amplios basados en volúmenes. Se protege la colaboración y el correo electrónico de malware desde el día cero, de suplantación de identidad y se protege el cumplimiento del correo electrónico empresarial. Se agrega investigación, seguimiento y

respuesta posteriores a la violación, así como automatización y simulación (para capacitación).

En general, el objetivo de este servicio es proteger, detectar, investigar y dar respuesta sobre las vulnerabilidades de seguridad que se detecten.

Figura 24

Servicios de Seguridad de Microsoft Office 365



Nota: Adaptado de Microsoft Defender for Office 365 security overview [Microsof Defender para Seguridad Office 365], 2022, Microsoft Docs (https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/overview?view=o365-worldwide)

EOP lo que brinda es la capacidad multicapa de protección contra Malware para proteger Linux, Mac y Windows. EOP tiene respuesta de amenazas en tiempo real puesto que usa políticas de reglas ya preconfiguradas para la detección de amenazas, esas reglas son las que son publicadas cada dos horas en una red global y que pueden ser empleadas por las organizaciones; además, EOP tiene la posibilidad de usar otras definiciones de malware encontradas por buscadores anti-malware antes de que esas sean públicamente liberadas, esto por las sociedades que tiene Microsoft.

9. Líneas base de seguridad para Azure: son documentos estandarizados para las ofertas de productos de Azure, que describen las capacidades de seguridad disponibles y las configuraciones de seguridad óptimas para ayudarle a reforzar la seguridad mediante herramientas, seguimiento y características de seguridad mejoradas (Microsoft docs, 2022r, párrafo 1).

En el caso de Azure y de acuerdo con la documentación de Microsoft doce (2022r), la línea base se enfoca en controles en la nube, los cuales son consistentes con estándares conocidos de la industria como: *Center for Internet Security* (CIS) y el del *National Institute for Standards in Technology* (NIST).

Cada línea base consta de los siguientes componentes:

1. ¿Cómo se comporta un servicio?
2. ¿Qué características de seguridad están disponibles?
3. ¿Se recomiendan configuraciones para asegurar el servicio? (párrafo 6).

10. Plan de Protección de información de Office 365: esta funcionalidad que poseen como parte del Office 365, actualmente no explorada:

> …permite a las organizaciones descubrir, clasificar, etiquetar y proteger documentos y correos electrónicos confidenciales. Los administradores pueden definir reglas y condiciones para aplicar etiquetas automáticamente, los usuarios pueden aplicar etiquetas manualmente o se puede usar una combinación de las dos, donde los usuarios reciben recomendaciones sobre la aplicación de etiquetas (Microsoft docs, 2022r, párrafo 2).

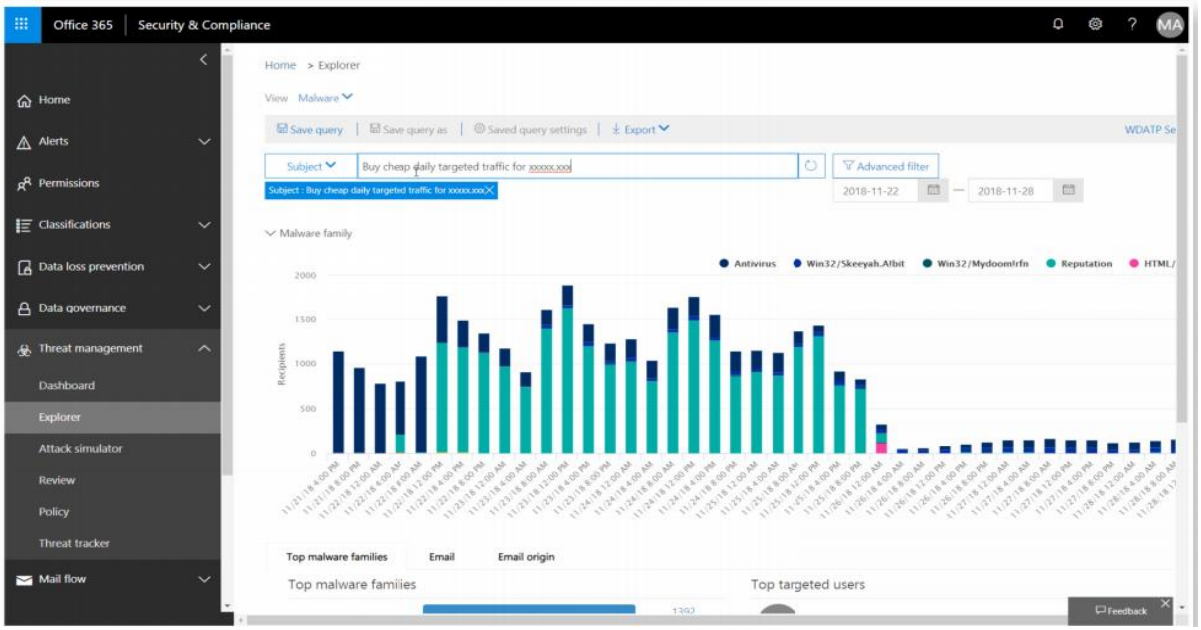
La desventaja es que este producto tiene una licencia con funcionalidades limitadas en comparación con el plan Premium 1 y Premium 2, por ejemplo: permite el control administrativo de la protección de los documentos, pero no se puede hacer la clasificación de los documentos de manera automática.

11. *Microsoft Advanced Thread Protection* (ATP): se puede tener acceso desde la pantalla principal del Microsoft Defender como parte de todo el monitoreo, se trata de otro producto más para la protección contra los Malware desconocidos, este ofrece protección desde el día cero, contra *phishing* y otros enlaces inseguros en tiempo real haciendo uso de múltiples canales de información. Además, automatiza las alertas de seguridad y la corrección de amenazas complejas de manera muy rápida. Finalmente, cuando se usa junto con Microsoft 365, puede compartir la

detección y la exploración entre dispositivos, identidades e información para acelerar la respuesta y la recuperación.

Figura 25

Portal de Microsoft 365 Defender



Nota: Adaptado de *Pantalla de monitoreo principal del Microsoft Defender*, por Microsoft 365 Defender, 2022 Microsoft (https://www.microsoft.com/en-us/security/business/siem-and-xdr/microsoft-365-defender).

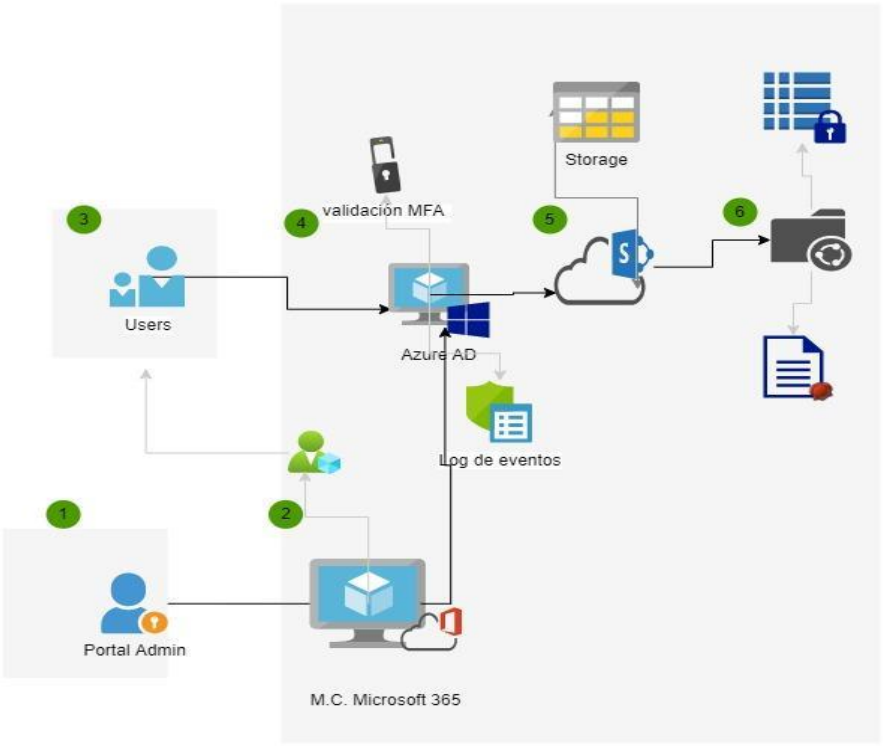
5.9 Descripción de la estructura de seguridad

Esta sección repasa el concepto más importante de esta investigación, la estructura de seguridad; esta consiste en ser una estrategia que define las políticas, controles de seguridad y procedimientos de detección y control de amenazas, todo con el fin de resguardar los tres pilares conocidos de seguridad: confidencialidad, integridad y disponibilidad.

Contemplando la definición anterior, se desarrolla en la propuesta de solución lo necesario para tener una estructura de seguridad robusta; esta contempla, en la sección 5.7, una línea base para el aseguramiento de la información; también enlista algunas políticas de acceso, normativas de respaldos y políticas de auditoría de procesos y documentos. De modo que al tomar en cuenta la sección 5.1 sobre la estructura del expediente, la sección 5.4 sobre lineamientos claves y la sección 5.7 se construye la Figura 26.

Figura 26

Estructura de seguridad de los expedientes en el ICAP



Nota: Elaboración propia.

1- Portal admin: son los usuarios administradores del Portal de Microsoft que acceden al Panel de Centro de Administración de Microsoft 365 (M.C Microsoft 365). El Portal admin también puede acceder desde allí al portal del *Azure AD*. Desde el M.C. Microsoft 365 puede verse los usuarios activos, los usuarios invitados y los usuarios eliminados.
2- M.C. Microsoft 365: se trata del Portal principal, dónde ocurren todos los mandos de Microsoft 365, desde portal es posible asignar los usuarios miembros que se asignarán a los equipos y los grupos que se formen. Además, se pueden obtener de este portal variedad de informes.
3- Usuarios registrados en Microsoft 365 que usan los grupos de seguridad previamente asignados.
4- *Azure Active Directory*: es el sistema contra el que el usuario se valida con el Múltiple Factor de Autenticación y tiene la respectiva autorización según

lo permita el acceso condicional. El panel de administración de *Azure AD* es accedido a través de *M.C Microsoft 365*. En el Azure AD se pueden ver los eventos de inicio de sesión de todos los usuarios y otros registros de auditoría.

5- *SharePoint Online*: es el sitio de almacenamiento de los expedientes, el Sistema de Gestión Documental en línea, el cual usaría una configuración de Colaboración externa muy específica, los permisos y los grupos de seguridad previamente configurados para el acceso restringido a los expedientes y documentos.

6- Expedientes digitales: conformados por los documentos electrónicos con firma digital y el índice del contenido del expediente con su respectiva firma digital basada en certificado.

Capítulo 6. Conclusiones y recomendaciones

6.1 Conclusiones

De la investigación aplicada al ICAP se extraen las siguientes conclusiones por objetivos:

Conclusiones del objetivo 1: Analizar la seguridad actual desde el inicio del ciclo de vida de los expedientes electrónicos para encontrar vulnerabilidades y amenazas en la seguridad. El objetivo se logró y de ahí se concluye:

La seguridad se analizó en el diagnóstico de la situación actual. En esa etapa, se detectaron usuarios a quienes no se les ha configurado un segundo factor de autenticación, ausencia de reportes de registros de auditoría, usuarios con poca conciencia acerca de la seguridad de la información, falta de controles de privacidad sobre los documentos electrónicos cuando se comparten externamente, controles de acceso físicos insuficientes, falta de uso de etiquetas para la clasificación de la información para conocer la sensibilidad de esta y falta de encriptación para la información. El ICAP ya contaba con un conocido sistema de gestión documental como lo es el SharePoint, pero no está usando todos los servicios que le dan mayor robustez y seguridad a lo almacenado por este en sus bases de datos en Estados Unidos.

Entre los problemas detectados, se observa que no se revisaban las maneras en que se tiene dispuesta la remisión y puesta a disposición de la documentación electrónica ni tampoco quedaba un registro de las solicitudes de los documentos electrónicos y no se comprueba la integridad de estos con ningún tipo de certificado, firma o CSV.

Por tanto, se analizó de manera profunda tanto la parte lógica como física de la estructura actual, lo cual permite tener una salida de información para completar el siguiente objetivo.

Conclusiones del objetivo 2: Aplicar las acciones adecuadas de control y correctivas que proporcionen integridad, disponibilidad y confiabilidad a los expedientes mediante una línea base de seguridad de la información. El objetivo alcanzado y se concluye:

El diagnóstico realizado sobre las medidas que proporcionan integridad, disponibilidad y confiabilidad mostró que en cuanto a la información electrónica no había políticas creadas ni normativas a seguir y tampoco personal capacitado

sobre cómo contribuir con la seguridad de la información. Como parte de lo encontrado en diagnóstico, en la sección 5.7 se proponen lineamientos para las políticas de seguridad de la información, políticas de control de acceso, normativas de respaldo y políticas de auditoría de procesos y documentos; todo con el fin de tener una línea base de seguridad de seguridad de la información para la implementación de los 3 pilares de seguridad.

Conclusiones del objetivo 3: Evaluar las necesidades de los usuarios que acceden a los expedientes digitales para seleccionar el medio de almacenamiento más adecuadamente seguro. El objetivo fue alcanzado y se concluye:

Sobre cuáles son las usuarias que harán uso de los expedientes (expedientes de profesores en este momento), se concluye que se trata del personal de los departamentos de Contabilidad y Finanzas y de Talento Humano. Dicho personal le dará el uso interno y externo; de manera interna, compartiría los expedientes entre miembros del mismo apartamento y de manera externa, muy a menudo compartiría los expedientes con empresas con dominios distintos.

Además, se llega a conocimiento que los documentos por el momento no requerirían un valor legal dentro del territorio nacional.

Aparte, se pretende un alineamiento con instituciones de la misma índole que el ICAP, por ello se recomendó que los expedientes se creen en un medio de almacenamiento que permita seguir la Normativa Técnica de Interoperabilidad de Expediente Electrónico; en este caso se seleccionó el SharePoint, el cual formó parte del estudio comparativo, junto con otros dos sistemas de gestión de documentos electrónicos: Zoho WorkDrive y *Confluence*.

Conclusiones del objetivo 4: Describir un método de control digital de integridad de la información a través de una indexación en los expedientes digitales. El objetivo es logrado y se concluye:

Los expedientes se han de encontrar en sitios en SharePoint que son objeto de la funcionalidad de Análisis de Sitios, ofrecida por la misma plataforma; el análisis se considera como un instrumento para la indexación puesto que permite conocer la interacción con el sitio y cuántos usuarios lo visitan; no obstante, el principal control digital que permitirá que los expedientes puedan tener integridad mediante indexación se logra mediante la misma composición del expediente; es decir, mediante la firma del índice electrónico, la cual

garantiza la autenticidad de los documentos en el expediente y el contenido del índice. Las ventajas del índice incluyen hacer búsquedas más simplificadas, encontrando rápidamente lo que se desea conocer que está en el expediente y obtener información de cuál y cuándo se añadió un nuevo elemento y cuándo se alteró un elemento ya existente.

Adicional a los controles mencionados, se cuenta con la indexación de búsqueda en la biblioteca de expediente, la cual permite hacer búsqueda avanzada a través de los metadatos obligatorios y opcionales que tienen los expedientes.

Conclusiones del objetivo 5: Explicar la estructura de seguridad de la información que garantice la integridad, disponibilidad y confiabilidad de los datos incluidos en cada expediente digital mediante una representación gráfica. El objetivo está logrado y se concluye:

La estructura de seguridad es una estrategia que define las políticas, controles de seguridad y procedimientos de detección y control de amenazas, todo con el fin de resguardar la confidencialidad, la integridad y disponibilidad; esta estructura se muestra completa de manera gráfica, el lector la encontrará representada en la Figura 26 de la sección 5.9 del documento. La estructura tiene a los usuarios que se autentican y autorizan contra el *Azure AD*, que a su vez ofrece los registros de auditoría y los eventos de inicio de sesión; el gráfico tiene el Centro de Administración de Office 365, el cual posee a los administradores, usuarios y grupos de seguridad, defensas contra Malware y finalmente tiene representados a los expedientes electrónicos que cuentan con la firma del índice electrónico y documentos firmados.

Conclusiones del objetivo general: Diseñar una estructura de seguridad de la información de los expedientes digitales especializados para el ICAP como parte del proceso de transformación digital. El objetivo se alcanzó y se concluye:

El proceso de transformación digital del ICAP ha conllevado variaciones para su mejoramiento, estos han implicado cambios en la arquitectura y en la estructuración organizacional. El ICAP tuvo que adquirir más impresoras y añadir códigos de seguridad para la impresión segura de documentos. Además, el ICAP hizo migraciones a la nube y los usuarios empezaron a usar más las aplicaciones de Word, Excel y lector de PDF online; de modo que ya crean sus propios

documentos digitales de forma directa. Sin embargo, empiezan a implementar la digitalización de sus inventarios, facturas, seguimiento del personal educativo por contratar y otros documentos administrativos sin considerar una estructura de seguridad, ya que los pilares de seguridad eran conocidos de manera parcial por el personal gerencial y los usuarios de la institución. En resumen, la seguridad era un factor que estaría entrando de modo lento en la ecuación de la transformación digital y posiblemente hasta el final de todo el proceso.

Gracias al ingreso del proyecto de investigación aplicada, el personal gerencial estaría informándose mejor de los pilares de seguridad, acerca de en qué consiste cada uno de ellos y los riesgos que estos ayudan a prevenir. De manera que, con mayor conocimiento, se logra una concienciación acerca de crear políticas para seguridad de la información que robustecen la disponibilidad y confidencialidad de esta; asimismo, se alcanza que el Gerente de TI preste mayor atención a los eventos de inicio de sesión de los usuarios y a los registros de auditoría, se consigue que se desee brindar firmar digitales a todos aquellos usuarios que requerían cargar documentos a expediente digitales y se logra que los expedientes vayan a constituirse siguiendo la Norma Técnica de Interoperabilidad de Expediente Electrónico y dentro de una Política de gestión de documentos electrónicos que considera la remisión y puesta a disposición de los documentos electrónicos.

En general, se concluye que el objetivo general se alcanza gracias al conglomerado de acciones correctivas y controles aplicables que se sugieren a lo largo de la Propuesta de solución que además incluye la exposición gráfica de la estructura de seguridad para una mayor comprensión de esta.

6.2 Recomendaciones

En esta sección se proporcionan algunas recomendaciones desde el punto de vista de la gestión de las actividades principales para la investigación y desde el punto de vista técnico:

- Debido a la dependencia que este tipo de estudio tiene con la disponibilidad de la población de investigación (empleados del ICAP), se recomienda tramitar las reuniones y solicitudes de información con suficiente antelación, para no ocasionar interrupciones en las

operaciones regulares de la institución ni tampoco sufrir retrasos en los tiempos y entregables esperados de la investigación.

- A causa de que no se cuenta con una opinión de experto en el área de Arquitectura de Seguridad de la Información en el ICAP o en la Universidad Cenfotec, es aconsejable coordinar con un experto en área similares; o bien en el caso de la implementación de complementos para seguridad, es aconsejable tener sugerencias de un *Azure Security Engineer Associate* [Ingeniero Asociado de Seguridad en Azure] o de un Security Operations Analyst Associate [Analista Asociado de Operaciones de Seguridad].
- Se recomienda brindar una capacitación a los empleados del ICAP acerca de la seguridad de la información al menos dos veces al año y extenderla a los nuevos ingresos. Esta debe incluir la política de escritorios limpios, el uso de etiquetas para clasificación de la información, la encriptación de correos con información sensible y/o confidencial, el uso de una clave de impresión por departamento o por usuario, el almacenamiento de los documentos en lo escritorios y archiveros, entre otros aspectos.

Capítulo 7. Reflexiones finales

En esta sección se destacan todos los temas aprendidos durante la investigación. Se utilizaron conocimientos en criptografía, controles de seguridad física, procedimientos de auditoría, análisis de riesgos de seguridad y productos de seguridad en la nube de Microsoft. En el primer caso, tomaron mucho realce los conocimientos acerca de los tipos de firma, incluyendo la firma digital y las ventajas que esta proporciona: integridad, no repudio y autenticación. En el último caso, fue más notorio aprender y recordar que se trataban muchos de los productos de Microsoft, los cuales fortalecen la postura de seguridad con Azure.

También, a lo largo de la investigación se dieron nuevos aprendizajes que incluyeron el ciclo de vida de los expedientes digitales y los estándares de administración de información electrónica.

Finalmente, se valoran las lecciones aprendidas desde el punto de vista de la gestión de las actividades principales para la investigación:

- Brindar información más amplia acerca de lo que se pretende en las observaciones para evitar extraer información confusa para la investigación o innecesaria.
- Evitar hacer re-entrevistas (las cuales se realizaron de forma muy frecuente) para obtener la información que era requerida desde la primera entrevista o bien que se pudo obtener en una entrevista previa.
- Apegarse al calendario de actividades planificadas para avanzar en la investigación de la mejor manera posible.
- Establecer más tiempo para seleccionar con mayor anticipación las referencias que se usaría para investigar cada tema del Marco Conceptual.

Capítulo 8. Trabajos a futuro

De la investigación sostenida durante más de dos cuatrimestres y después de haber indicado una solución para la problemática identificada, se pueden detectar otros proyectos que complementan de manera óptima la solución sugerida, se trata de tres proyectos que se describen a continuación:

- ✓ La creación de la política de gestión de documentos electrónicos que deberá seguir la Normativa Técnica de Gestión de Documentos Electrónicos en el Sistema Nacional de Archivos y que a su vez irá ligada con las políticas de control de accesos y con los actores que se definan para la implementación de las medidas para el aseguramiento de la información electrónica.
- ✓ La institución de un equipo cuyo objetivo sea llegar a implementar el estándar británico, BSI BS 10008, que hace referencia a los sistemas de gestión de información electrónica.
- ✓ La creación de un Plan de Contingencia que documente los procesos de cómo el negocio continuará sus funciones críticas durante y después de un evento de emergencia o interrupción en el negocio (pueden ser por causa natural, ciberataques, cortes de corriente, violencia en el lugar de trabajo, cierres administrativos, etc.). El documento pretenderá considerar

las expectativas y los estándares de regularidad que provienen de las partes interesadas externas. El documento debe incluir el análisis de impacto del negocio (principales áreas de negocio impactadas) y la estrategia de continuidad del negocio.

Glosario

Cadena de custodia:

Es el registro de todos los aspectos de los flujos de trabajo utilizados en el manejo de pruebas, desde la adquisición hasta la presentación ante el tribunal. Muchas veces la evidencia es asegurada para prevenir cambios con *hash* criptográficos y así poder viajar por la cadena de custodia. La integridad de una investigación de un caso puede verse afectada haciendo que gane o se pierda según los procedimientos que se hayan seguido para proteger el mantenimiento de la cadena de custodia.

CASB:

> Cloud Access Security Broker es un mecanismo de defensa, administra y hace cumplir todas las políticas y prácticas de seguridad de datos, incluida la autenticación, la autorización, las alertas y el cifrado. Los CASB mejoran la visibilidad de una organización en cuanto a quién accede a sus datos y cómo se utilizan en los puntos finales. Un CASB protege a la organización a través de una combinación de técnicas de prevención, monitoreo y mitigación (Puzas, 2022).

Certificate Revocation List (CRL):

La lista de revocación de certificados es una lista que contiene los certificados que pierden su validez o que han sido revocados por la Autoridad Certificadora. Esa lista es creada y enviada por la misma Autoridad Certificadora y es revisada cada vez que una aplicación recibe una petición de validación de certificado para contrastar con la CRL que ya tiene almacenada, comparando los nuevos ingresos y actualizando los registros.

CNSED:

Comisión Nacional de Selección y Eliminación de Documentos, es el Órgano de la Dirección General del Archivo Nacional, encargado de dictar las normas sobre selección y eliminación de documentos, de acuerdo con su valor científico cultural.

Gaudi:

Es una solución tecnológica de acceso electrónico que permite realizar una serie de funcionalidades con su tarjeta de firma digital, tales como firmar y validar documentos y la autenticación de los suscriptores.

***Hash**:*

> Las funciones hash o de resumen son usadas en la criptografía para: …comprobar, entre otras cosas, la integridad de determinada información. Las funciones hash son públicamente conocidas que transforman una información o mensaje de cualquier tamaño en una información que tiene un tamaño fijado de antemano […] por ejemplo, 256 bits, el número de tales resúmenes solo es de 2^{256}, mientras que el número de posibles mensajes de cualquier longitud es infinito (Hernández, 2016, p.111).

***Identity Provider* (IdP):**

El proveedor de identidad es un sistema que crea y almacena las identidades digitales. Se usa para autenticar directamente a un usuario o para brindar servicios de autenticación a las plataformas web y plataformas digitales.
ISO 15489-1-2001:

Es una Norma Internacional cuyo título general es Información y documentación – Gestión de documentos de archivo, se compone de dos secciones Generalidades y Directrices [Informe técnico], en ella se indican políticas y procedimientos de la gestión de documentos de archivo para brindar protección de éstos y permite que la evidencia y la información que contienen puedan ser recuperadas más eficiente y eficazmente usando prácticas y procedimientos normalizados.

Malware:

"Es todo el software dañino para los sistemas, englobándose dentro del término a virus, gusanos, troyanos, bombas lógicas (Alvarez, 2004, p.442)".

Algunas de las mayores categorías de malware son: Virus, Spyware, Ransomware (Microsoft Docs, 2022a). Algunos son capaces de eliminar o robar la información, otros de espiar en los procesos y la información de las aplicaciones y otros de hasta bloquear el sistema completo y volver inaccesible.

Metadatos administrados:

> Los metadatos administrados en *SharePoint* le permiten controlar cómo los usuarios agregan metadatos al contenido. Por ejemplo, mediante el uso de conjuntos de términos y términos administrados, puede controlar qué términos pueden agregar los usuarios al contenido y puede controlar quién puede agregar nuevos términos. También puede limitar las palabras clave de empresa a una lista específica configurando el conjunto de términos: Palabras clave como “cerrado” (Microsoft Docs, 2022h).

OAuth:

Abreviación de “Open Authorization”, es un estándar de autorización que permite a las aplicaciones obtener acceso a los recursos de las cuentas de usuario de otras aplicaciones, como Facebook, Twitter, LinkedIn, Google y muchos más. Es decir, se trata de un tipo de acceso de delegación en nombre de una aplicación basada en navegación.

OnPremise:

También conocido como En Premisa, hace referencia a los ambientes que están localmente en el sitio de la organización. Es todo lo contrario a las estructuras en la nube.

PII (*Personal Identifiable Information*):

Es todo aquel dato que, uniéndose con otro, permite que se pueda identificar y localizar a las personas, ejemplo de este tipo de información: cédula, nombre completo, dirección, número de teléfono, número de seguro social, entre otros.

PowerBI:

Es un producto de Microsoft de inteligencia empresarial que sirve para obtener conocimientos sobre datos de múltiples fuentes. Permite analizar, compartir y promover los datos en toda la organización, siendo una herramienta bastante robusta en seguridad y precisa. El producto permite la creación de informes memorables personalizados con la marca de la organización y es posible mediante estos informes tomar decisiones informadas para el negocio.

SISS:

SQL Server Integration Services es una plataforma para la creación de soluciones empresariales de transformaciones de datos e integración de datos. Tiene funcionalidades como la extracción y transformación de los datos de

diversos orígenes como archivos de datos XML, archivos planos y orígenes de datos relacionales, la carga de almacenamientos de datos, la limpieza y minería de datos y la administración de datos y objetos de SQL Server. Además, ofrece herramientas gráficas que permiten crear las soluciones (haciendo uso paquetes programados) que ejecutan las funciones como la extracción y transformación de datos.

SmartCard:

Se trata de un dispositivo empleado para asegurar la información de la llave pública y la llave privada proporcionada por el BCCR.

***Sharepoint*:**

Es una herramienta software de gestión de contenidos y documental. Está disponible con la plataforma de Office365 de Microsoft; permite centralizar y compartir toda la información gestionada por cualquier empresa de forma sencilla. Se usa mucho como Intranet, para realizar comunicaciones internas y desde luego como gestor documental, con firma electrónica y flujos de trabajo, que permitan controlar el ciclo de vida de un documento, aprobaciones, firmas etc.

Subfondo:

Es un identificador de sección al que pertenece un expediente o un documento electrónico, normalmente se específica como parte del índice electrónico.

Referencias bibliográficas

Adobe (18 de marzo, 2022). Adobe sign para SharePoint Online: Guía de Instalación (v2.0). https://helpx.adobe.com/la/sign/using/microsoft-sharepoint-installation-guide.html

Álvarez Marañón, G. (2004). Seguridad informática para empresas y particulares. McGraw-Hill, España. https://elibro.net/es/lc/bibliouia/titulos/50050

Atlassian (2022). Learn about Confluence Cloud plans [Aprende sobre los planes de Confluence Cloud]. https://support.atlassian.com/confluence-cloud/docs/learn-about-confluence-cloud-plans/

Ley 7202 de 1990. Ley del Sistema Nacional de Archivos. 27 de noviembre de 1990. http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=8885&nValor3=75177&strTipM=TC

Archivo Nacional (2020). Norma técnica nacional: Lineamientos para la conformación de expedientes administrativos. https://www.archivonacional.go.cr/web/dsae/norma_lineamientos_%20expedientes.pdf

BCCR (2019). Definiciones. https://www.bccr.fi.cr/firma-digital/informaci%C3%B3n-general/definici%C3%B3n

BCCR (2007). Gaudi. https://www.bccr.fi.cr/firma-digital/gaudi

BCRR. (26 febrero, 2021). Guía Técnica de Configuración del Servicio firmador Canal Privado. https://www.bccr.fi.cr/firma-digital/DocFirmaDigital/Guia-tecnica-configuracion-servicio-firmador-canal-privado.pdf

Biolchini, Gomes, Cruz y Horta (2005). Systematic Review in Software Engineering [Revisión Sistemática en Ingeniería de Software]. https://www.scribd.com/document/358630767/Biolchini-et-al-2005-Systematic-Review-in-Software-Engineering-pdf

ERI Economic Research Institute (2022). Salary Report [Reporte de Salario]. https://www.erieri.com/salaryreport/report

Gallardo, G. (1ero de abril, 2015). Seguridad en Bases de Datos y Aplicaciones Web. IT Campus Academy.

https://es.scribd.com/read/313053050/Seguridad-en-Bases-de-Datos-y-Aplicaciones-Web

Glassdoor (marzo, 2022). Security architect salary [Salario de Arquitecto de Seguridad]. https://www.glassdoor.com/Salaries/security-architect-salary-SRCH_KO0,18.htm

Hernández Encinas, L. (2016). La criptografía. Editorial CSIC Consejo Superior de Investigaciones Científicas. https://elibro.net/

Hernández, R. (2014). Metodología de la investigación. Sexta Edición. McGraw Hill, México.

ISO (julio, 2008). ISO 32000 -1: 2008 https://www.iso.org/standard/51502.html.

ISO (2001). Norma internacional ISO 15489-1. Información y documentación – Gestión de documentos. ISO copyright office, Ginebra.

LinkedIn (2021) Security Solutions Architect salaries in United States [Salarios de Arquitectos de Seguridad en Estados Unidos]. https://www.linkedin.com/salary/security-solutions-architect-salaries-in-united-states

MICITT (2022). Firma Digital Certificada. https://www.mifirmadigital.go.cr/

Microsoft (2022a). Advanced Threat Protection and Analytics [Protección de Amenazas Avanzado y Analítica]. https://www.microsoft.com/en-ph/dpa-trustcenter/privacy/advancedthreatprotection

Microsoft (sin fecha). Agregar un índice a una columna de lista o biblioteca. https://support.microsoft.com/es-es/office/agregar-un-%C3%ADndice-a-una-columna-de-lista-o-biblioteca-f3f00554-b7dc-44d1-a2ed-d477eac463b0#:~:text=Agregar%20un%20%C3%ADndice%20a%20una%20columna%20de%20lista,hasta%2020%20columnas%20en%20una%20lista%20o%20biblioteca.

Microsoft (2022b). Compare office 365 education plans [Comparar planes de Educación Office 365]. https://www.microsoft.com/es-ww/microsoft-365/academic/compare-office-365-education-plans?market=cr&activeab=tab:primaryr1

Microsoft (2022c). ¿Qué es Power BI? https://powerbi.microsoft.com/es-es/what-is-power-bi/

Microsoft (2022d) Microsoft 365 Defender. https://www.microsoft.com/en-us/security/business/siem-and-xdr/microsoft-365-defender

Microsoft Docs (06 septiembre, 2022a). Anti-malware Protection [Protección Anti-malware]. https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-malware-protection?view=o365-worldwide

Microsoft Docs (23 de mayo, 2022b). Azure Information Protection [Protección de Información de Azure]. https://docs.microsoft.com/en-us/office365/servicedescriptions/azure-information-protection

Microsoft Docs (29 de agosto, 2022c). Azure Information Protection service description [Descripción del Servicio de Protección de Información de Azure]. https://docs.microsoft.com/en-us/office365/servicedescriptions/azure-information-protection

Microsoft Docs (09 de febrero, 2022d). Collaborate with guests on a document [Colaboración con invitados en documentos]. https://docs.microsoft.com/en-us/microsoft-365/solutions/collaborate-on-documents?view=o365-worldwide

Microsoft Docs (04 de febrero, 2022f). Default SharePoint groups [Grupos por defecto de SharePoint]. https://docs.microsoft.com/en-us/sharepoint/default-sharepoint-groups

Microsoft Docs (25 de agosto, 2022g). How SharePoint and OneDrive safeguard your data in the cloud [Cómo SharePoint y OneDrive protegen su información en la nube]. https://docs.microsoft.com/en-us/sharepoint/safeguarding-your-data

Microsoft Docs (25 de agosto, 2022h). Introduction to managed metadata [Introducción a los metadatos administrados]. https://docs.microsoft.com/en-us/sharepoint/managed-metadata

Microsoft Docs (31 de agosto, 2022i). Learn about sensitive labels [Aprenda acerca de las Etiquetas de sensibilidad]. https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide

Microsoft Docs (22 de agosto, 2022j). Manage sharing settings. https://docs.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off

Microsoft Docs (22 de agosto, 2022k). Manage security groups [Administrar grupos de seguridad]. https://docs.microsoft.com/en-us/sharepoint/manage-security-groups

Microsoft Docs (20 de mayo, 2022l). Multi-Geo capabilities in OneDrive and SharePoint Online [Capacidades de multigeo-localización en OneDrive y SharePoint Online]. https://docs.microsoft.com/en-us/microsoft-365/enterprise/multi-geo-capabilities-in-onedrive-and-sharepoint-online-in-microsoft-365?view=o365-worldwide

Microsoft Docs (09 de julio, 2022m). Microsoft Defender for Cloud Apps [Microsof Defender para Cloud Apps]. https://docs.microsoft.com/en-us/defender-cloud-apps/what-is-defender-for-cloud-apps

Microsoft Docs (30 de agosto, 2022n). Microsoft Defender for Cloud Apps in Microsoft 365 Defender [Microsoft Defender para Cloud Apps en Microsoft 365 Defender]. https://docs.microsoft.com/en-us/microsoft-365/security/defender/microsoft-365-security-center-defender-cloud-apps?view=o365-worldwide

Microsoft Docs (29 de agosto, 2022o). Obtenga más información sobre la retención para SharePoint y OneDrive. https://docs.microsoft.com/es-es/microsoft-365/compliance/retention-policies-sharepoint?view=o365-worldwide

Microsoft Docs (26 de agosto, 2022p). Registros de auditoría en Azure Active Directory. https://docs.microsoft.com/es-es/azure/active-directory/reports-monitoring/concept-audit-logs

Microsoft Docs (30 de agosto, 2022q). Registros de inicio de sesión en Azure Active Directory. https://docs.microsoft.com/es-es/azure/active-directory/reports-monitoring/concept-sign-ins

Microsoft Docs (02 agosto, 2022r). Security baselines for Azure overview [Líneas base de seguridad para Azure]. https://docs.microsoft.com/en-us/security/benchmark/azure/security-baselines-overview

Microsoft Docs (28 enero, 2022s). SQL Server Integration Services [Servicios de Integración de SLQ Server]. https://docs.microsoft.com/es-mx/sql/integration-services/sql-server-integration-services?view=sql-server-ver16

Microsoft Docs (01 de agosto, 2022t). What is information Azure Information Protection? [¿Qué es la Protección de Información de Azure?]. https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection

Ministerio de Hacienda y Administración Pública de España (2016a). Guía de aplicación de la Norma Técnica de Interoperabilidad de Documento electrónico (2ª edición electrónica). http://administracionelectronica.gob.es

Ministerio de Hacienda y Administración Pública de España (2016b). Guía de aplicación de la Norma Técnica de Interoperabilidad de Expediente Electrónico (2ª edición electrónica). https://administracionelectronica.gob.es/pae_Home/dam/jcr:4386988b-c99d-4bd5-9729-ae5709bca284/Guia_NTI_expediente_electronico_PDF_2ed_2016.pdf

Ministerio de Hacienda y Administración Pública de España (2016c). Guía de aplicación de la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos (2ª edición electrónica). https://administracionelectronica.gob.es/pae_Home/dam/jcr:34e78339-de2e-4fe5-b576-3107e9d3a54c/Guia_NTI_Politica_Gestion_DocElect_PDF_2ed_2016.pdf

Puzas, David (07 de febrero de 2022). Cloud Access Security Broker (CASB) [Corredor de Seguridad de Acceso a la nube]. https://www.crowdstrike.com/cybersecurity-101/cloud-security/cloud-access-security-broker-casb/

Rafael Ángel Prieto de Lope. (2015). SGBD e instalación: administración de bases de datos (UF1469). IC Editorial. https://elibro.net/es/lc/bibliouia/titulos/44145

Ramakrishnan, R. (2007). Sistemas de gestión de bases de datos (3a. ed.). McGraw-Hill, España. Sitio web: https://elibro.net/

Rangel, E.L. (noviembre, 2017). Guía de Implementación de un Sistema de Gestión de Documentos Electrónicos de Archivo. https://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/5_Consulte/Recursos/Publicacionees/V15_Guia_SGDEA_WEB.pdf

Rangel, E.L (octubre, 2019). G.INF.08 Guía para la gestión de documentos y expedientes electrónicos. https://www.mintic.gov.co/arquitecturati/630/w3-article-61594.html

Regidor-Barboza Harrys (2010). La cooperación académica entre el ICAP y las universidades centroamericanas: hacia el fortalecimiento de la gestión del conocimiento. Publicaciones ICAP. http://publicaciones.icap.ac.cr/images/PDF-REVISTA/revista-58-59/el_icap_en_ca.pdf

Tenorio, G.A. y Salazar, E.F. (2020). Evaluación de la precisión de los modelos de clasificación binaria para la identificación de noticias verdaderas o falsas en Costa Rica. [Tesis de Maestría, Universidad Cenfotec]. Librarika.

Vargas, Zoila (2009). La investigación aplicada: Una forma de conocer las realidades con evidencia científica. Universidad de Costa Rica. https://www.redalyc.org/pdf/440/44015082010.pdf

Vindas, Eduardo (2019). Blockchain como solución para la administración de expedientes digitales. [Tesis de Maestría, Universidad Cenfotec]. Librarika.

Wiese, Lena (2015). Advanced Data Management: For SQL, NoSQL, Cloud and Distributed Databases [Administración Avanzada de Datos: Para SQL, NoSQL, Nube y Bases de Datos distribuidas]. Gruyter. https://link-springer-com.ezproxy.sibdi.ucr.ac.cr/

Zelfong, Greg (22 junio, 2022). 15 Ways to make your SharePoint Site more secure [15 Maneras de hacer su Sitio de SharePoint más seguro]. https://sharepointmaven.com/15-ways-to-make-your-sharepoint-site-more-secure.

Zoho (2022) Comparison Plan [Plan Comparativo]. https://www.zoho.com/es-xl/workdrive/plan-comparison.html

Apéndices

Anexo 1 – Guía de Entrevista semi estructurada

Fecha:

Lugar:

Nombre:

Puesto que desempeña:

1. ¿Tiene alguna duda respecto al objetivo de esta entrevista?
2. ¿Conoce los componentes principales que conforman un expediente digital?
3. ¿Está familiarizado con los 3 pilares de seguridad de la información?
4. ¿Existe alguna política o normativa en la institución que refuerce alguno de los pilares de seguridad de la información?
5. ¿Conoce acerca de tecnologías para encriptación de la información?
6. ¿Cuentan con arquitectura *OnPremise* o *Cloud*? ¿Cuál cree más valiosa según lo que ha visto en su organización?
7. Sé que le gustaría mejorar el diseño de la estructura de los expedientes digitales, ¿qué aspectos considera usted necesarios reemplazar o mejorar? ¿Cuáles serían los más importantes para la organización?
8. Si tuviera que establecer un lugar para almacenamiento de datos en reposo ¿Cuál sería esa ubicación?, ¿por qué?
9. ¿Cómo considera que sería mejor hacer la visualización de los documentos electrónicos de los expedientes digitales?
10. ¿Cuál sería el personal con mayor necesidad de disponibilidad de los expedientes digitales?
11. ¿Conoce acerca de controles de indexación para expedientes digitales?
12. ¿Cuentan con licencias de Microsoft para tener un SIS?
13. ¿Tienen acceso a algún programa o software de visualización de datos de forma analítica mediante gráficas u otros elementos visuales?
14. De acuerdo con su experiencia en esta organización, ¿cuáles diría usted que son los medios de almacenamiento más adecuados para

salvaguardar expedientes digitales? Por ejemplo: share files systems usando Samba en Linux.

15. ¿Me podría describir de forma detallada el proceso de un documento electrónico desde su ingreso digitalización hasta la visualización de este?
16. ¿Cómo calificaría la seguridad en el intercambio de los documentos electrónicos dentro de la institución en una escala del 1 al 5?

    1 excelente 2 muy bueno 3 regular 4 insuficiente 5 malo

17. ¿Cómo calificaría la seguridad en el intercambio de los documentos electrónicos fuera de la institución en una escala del 1 al 5?

    1 excelente 2 muy bueno 3 regular 4 insuficiente 5 malo

18. Me gustaría que me comentara sobre, ¿cómo visualiza usted la estructura de seguridad para los expedientes digitales?
19. ¿Le gustaría comentar algo más al respecto para mejorar los procesos que rodean los documentos electrónicos en su organización?

Anexo 2 – Guía de Observación

Fecha

Lugar

Hora de inicio

Hora de terminación

Departamento Cantidad de personas

Cantidad de accesos

Objetivo:

Ambiente físico

	Observaciones
Disposición de los equipos	
Regulación de temperatura	
Distribución (privacidad)	
Dispositivos de seguridad	
Puntos de conexión a red	

Ambiente Social y Humano

	Observaciones
Procesos de liderazgo	
Funciones	
Frecuencia en la comunicación	
Jerarquías	
Medios de comunicación	

Artefactos que utilizan

	Observaciones

Tarjetas de acceso	
Uniformes	
Token de seguridad	
Tarjetas de identificación	
Accesorios personales	

Anexo 3 – Notas de la primera observación

Figura 27

Parte I - Notas de la primera observación

Guia de Observación para ambiente físico

Fecha: 16/02/2022

Lugar: Coordinación

Hora de inicio: 15:30

Hora de terminación: 16:00

Departamento: Coordinación académica Cantidad de personas: 1

Cantidad de accesos: 2 accesos

Objetivo: _____

Ambiente físico

	Observaciones
Disposición de los equipos	Un equipo.
Regulación de temperatura	Por medio de persianas
Distribución (privacidad)	Buena distribución, cada quien con su espacio
Dispositivos de seguridad	No existe más que una puerta con llave
Puntos de conexión a red	No hay puntos de conexión en red, la conexión es inalambrica.

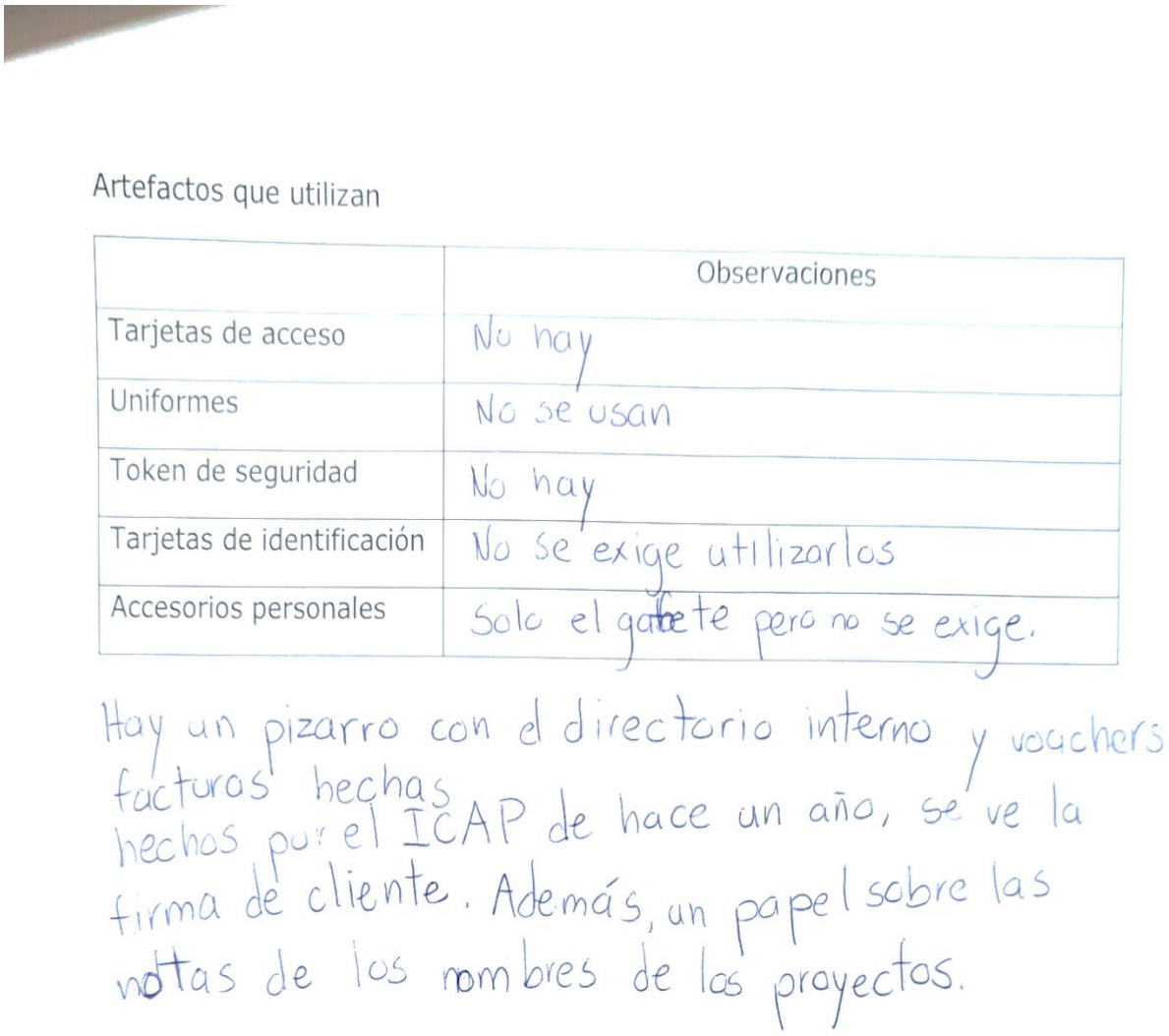
Ambiente Social y Humano

	Observaciones
Procesos de liderazgo	En cascada muy directo
Funciones	Archivación de documentos, se accede a documentos desde OneDrive.
Frecuencia en la comunicación	Diaria y constante
Jerarquías	3 Coordinadores y 3 asistentes administrativas
Medios de comunicación	Telefono fijo, en persona, whatsapp, teams

Anexo 4 – Notas de la segunda observación

Figura 28

Parte II – Notas de la primera observación



Artefactos que utilizan

	Observaciones
Tarjetas de acceso	No hay
Uniformes	No se usan
Token de seguridad	No hay
Tarjetas de identificación	No se exige utilizarlos
Accesorios personales	Solo el gafete pero no se exige.

Hay un pizarro con el directorio interno y vouchers facturas hechas hechos por el ICAP de hace un año, se ve la firma de cliente. Además, un papel sobre las notas de los nombres de los proyectos.

Figura 29

Parte I - Notas de la segunda observación

Guía de Observación para ambiente físico

Fecha: 16/02/2022

Lugar: ICAP sede 2

Hora de inicio: 16: 15

Hora de terminación: 17:00

Departamento: Contable y Financiera Cantidad de personas: 2

Cantidad de accesos: Un acceso

Objetivo: _____

Ambiente físico

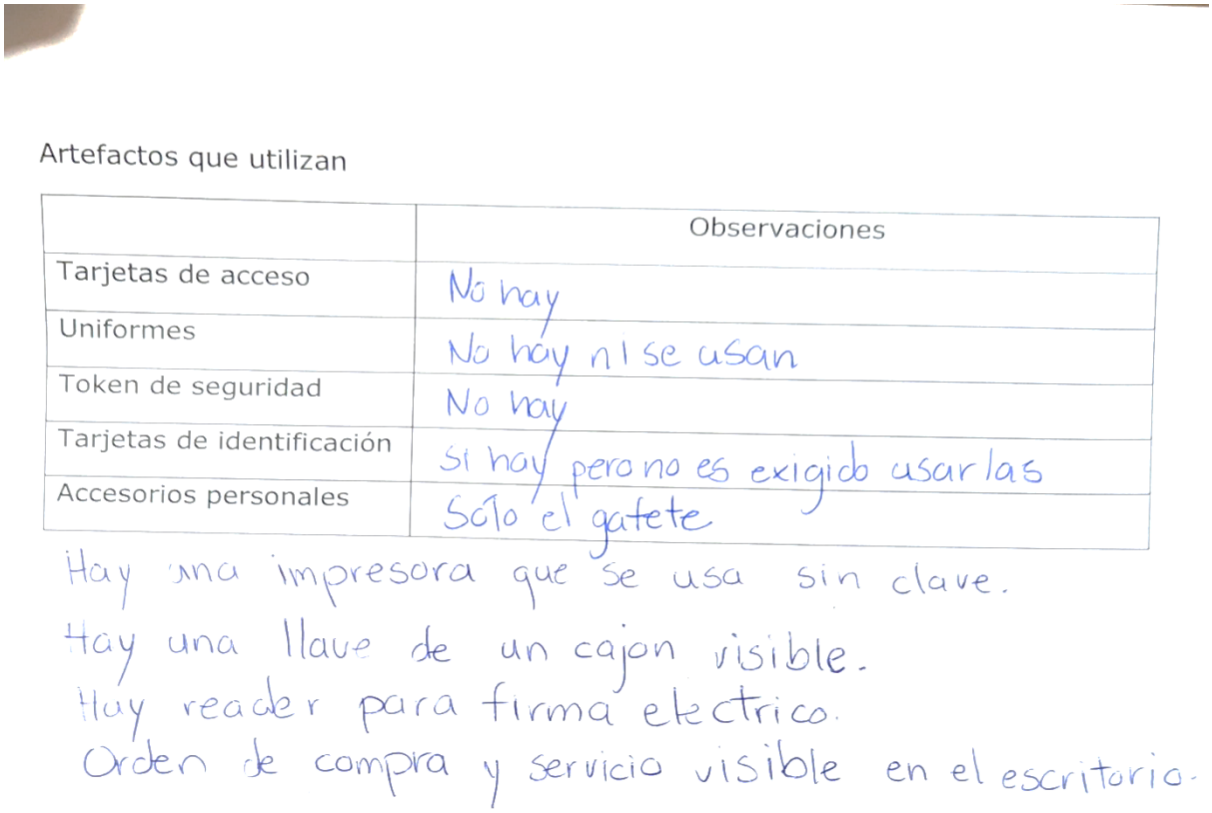
	Observaciones
Disposición de los equipos	Dos equipos
Regulación de temperatura	No hay un sistema de aire acondicionado la ventilación es mediante persianas
Distribución (privacidad)	Cada quién cuenta con su propio espacio.
Dispositivos de seguridad	No hay lectores de tarjeta de seguridad.
Puntos de conexión a red	La conexión es inalámbrica

Ambiente Social y Humano

	Observaciones
Procesos de liderazgo	Un líder, proceso en cascada
Funciones	Control de las facturas por pagar y de proveedores
Frecuencia en la comunicación	Diaria y constante
Jerarquías	Un líder y 2 asistentes
Medios de comunicación	En persona, por correo, por teléfono y teams

Figura 30

Parte II – Notas de la segunda observación



Artefactos que utilizan

	Observaciones
Tarjetas de acceso	No hay
Uniformes	No hay ni se usan
Token de seguridad	No hay
Tarjetas de identificación	Si hay pero no es exigido usarlas
Accesorios personales	Sólo el gafete

Hay una impresora que se usa sin clave.
Hay una llave de un cajon visible.
Hay reader para firma electrico.
Orden de compra y servicio visible en el escritorio.

Anexo 5 – Guía para agregar un índice

Paso 1 – Verificar las columnas para usarse para la indexación: Tomando como base la Figura 32, escoger las columnas para la creación del índice, la Columna principal para el índice será el Identificador del Documento y la columna Secundaria será la fecha y hora de ingreso de creación del documento.

Paso 2 – Configurar la biblioteca para tener un índice compuesto de columnas.

Seleccione **Configuración** y, a continuación, seleccione **Configuración de biblioteca.**

Paso 3 – Seleccionar las columnas indezadas.

Desplácese hacia abajo hasta la **sección** Columnas, a continuación, seleccione las **Columnas indizadas**.

Paso 4 – Crear el nuevo índice compuesto.

En la página Columnas indizadas, seleccione **Crear un nuevo índice.** Después, seleccione una columna de búsqueda como **Columna principal** para este índice. Luego, seleccione la **Columna secundaria**, que no será para búsqueda**.** Finalmente, seleccione **Crear.**

Figura 31
Selección de columna Primaria y Secundaria

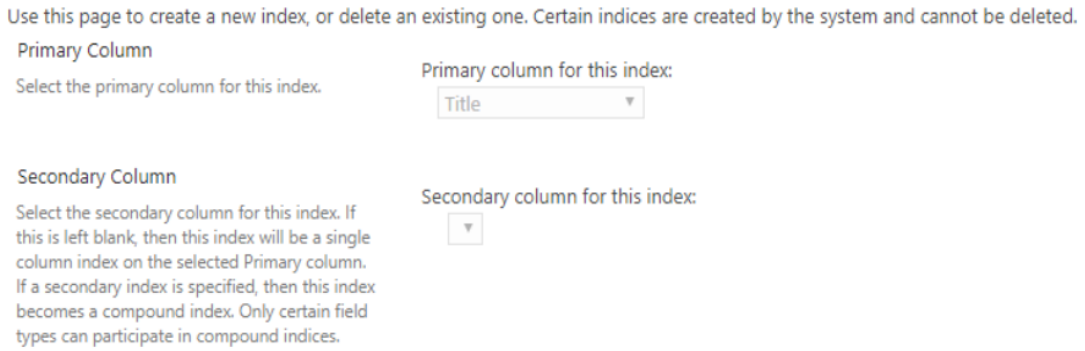


Figura 32
Columnas admitidas y no admitidas para indexación

Tipos de columna admitidos	Tipos de columna no admitidos
▪ Una línea de texto	▪ Varias líneas de texto
▪ Opción (valor único)	▪ Opción (multivalor)
▪ Número	▪ Calculada
▪ Moneda	▪ Hipervínculo o imagen
▪ Fecha y hora	▪ Columnas personalizadas
▪ Persona o grupo (valor único) (búsqueda)	▪ Persona o grupo (multivalor) (búsqueda)
▪ Metadatos administrados (búsqueda)	▪ Datos externos
▪ Sí/No	
▪ Búsqueda (búsqueda)	

Anexo 6 – Guía para la configuración para compartir en *SharePoint*

Paso 1 – Ir a **Sharing** en el Centro de Administración de SharePoint, desde luego se debe hacer con un usuario que tenga los permisos de administración en la organización.

Paso 2 – En la sección de **Colaboración externa**, indicar el Nivel para compartir: Sólo invitados existentes en el Directorio de la organización. También en esa sección, marcar la casilla de “Limitar colaborar por dominio” y añadir todos los dominios de red de los usuarios invitados a los que siempre se comparten los archivos.

Paso 3 – Configurar los grupos de seguridad que se les permitirá compartir: En la misma sección, selecciona la casilla: “Permitir sólo a usuarios en grupos de seguridad específicos para compartir externamente”. Después seleccione: “Administrar grupos de seguridad” y en la casilla de “Añadir un grupo de seguridad”, busca los grupos de seguridad que se desean añadir. Seguido de eso, en la parte de “Puede compartir con”, seleccionar: “Sólo invitados autenticados” y guarda la configuración.

Paso 4 – Configurar para que haya más seguridad con respecto a los Invitados: En la misma sección, marca la casilla para que los usuarios Invitados deban hacer la autenticación usando la misma cuenta a la cual le fue enviada

la invitación de compartir; ya que, por defecto, los Invitados pueden recibir una invitación en una cuenta, pero hacer la autenticación con una cuenta distinta.

Paso 5 – Configurar un tiempo de expiración para el acceso de los invitados: establece un tiempo de caducidad para el acceso de Invitados, cada Invitado que invite al sitio o con el que se compartan archivos y carpetas individuales tendrá acceso durante un número determinado de días.

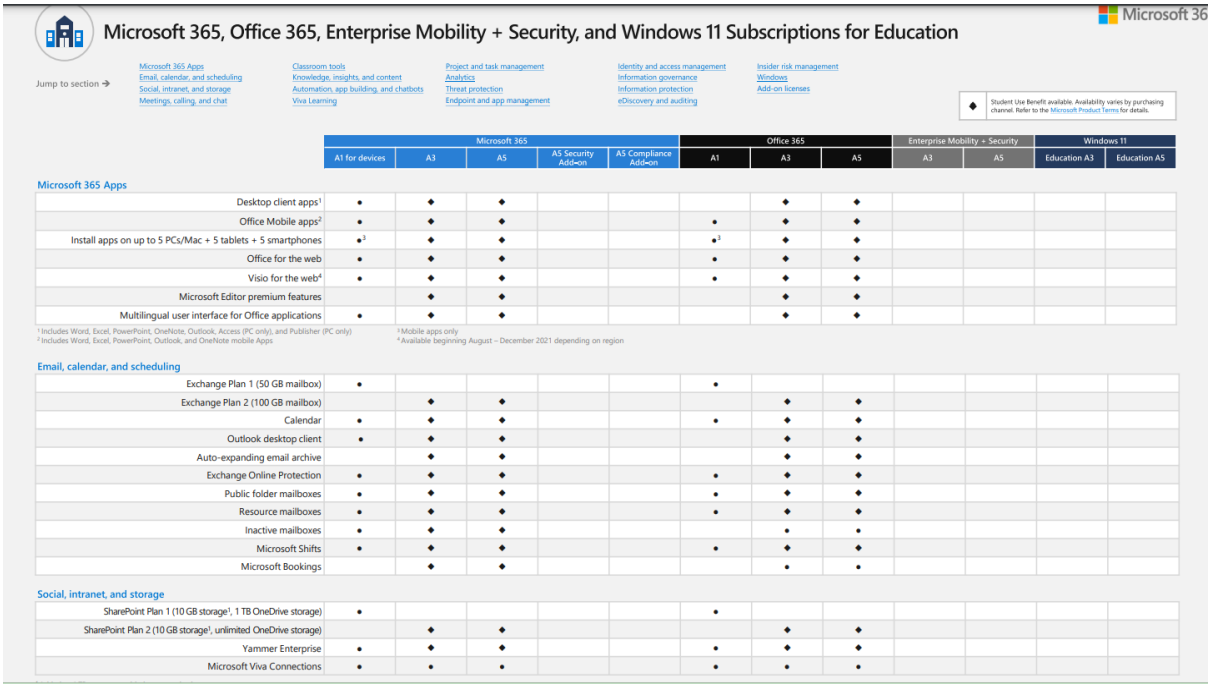
Paso 6 – Escoger la opción por defecto para cuando se envía el *sharing-link*: Se cambia la configuración por defecto de “Cualquiera con el enlace” a “Personas específicas en la organización (sólo las personas que el usuario especifique)”.

Paso 7 – Configurar la vista de los nombres de las personas que vieron los archivos o páginas: Esta configuración le permite especificar a los propietarios de Sitios si pueden permitir que los usuarios que tienen acceso a un archivo, página o publicación vean en la información del archivo quién ha visto el elemento. La configuración es activada por defecto en el nivel de organización y desactivada en el nivel de sitio para los sitios existentes.

Anexo 7 – Microsoft Modern Work Plan Comparison Education 11-2021

Figura 33

Parte I - Comparación de la suscripción de los planes para Educación



Microsoft 365, Office 365, Enterprise Mobility + Security, and Windows 11 Subscriptions for Education

Jump to section → Microsoft 365 Apps · Email, calendar, and scheduling · Social, intranet, and storage · Meetings, calling, and chat · Classroom tools · Knowledge, insights, and content · Automation, app building, and chatbots · Viva Learning · Project and task management · Analytics · Threat protection · Endpoint and app management · Identity and access management · Information governance · Information protection · eDiscovery and auditing · Insider risk management · Windows · Add-on licenses

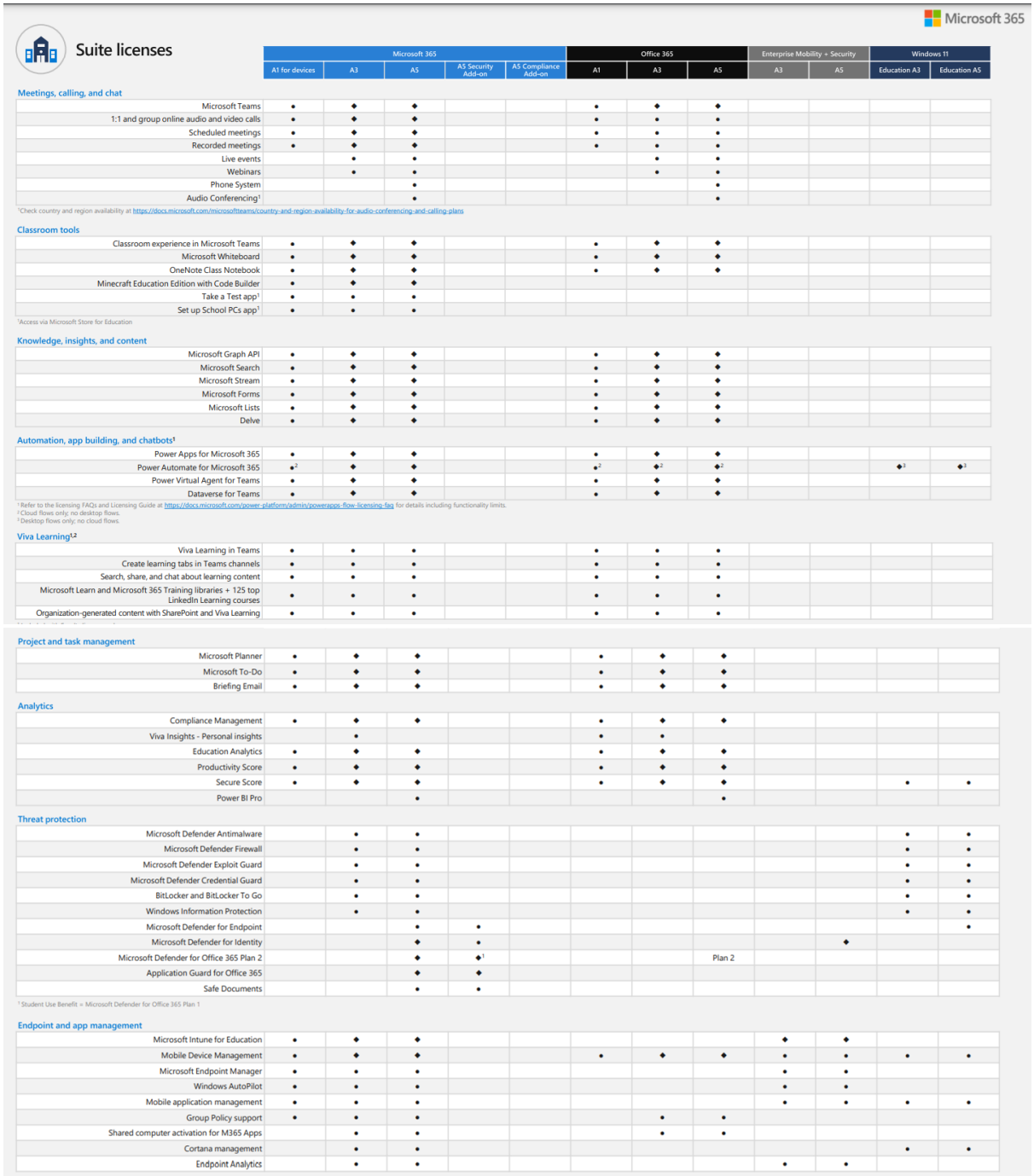
◆ Student Use Benefit available. Availability varies by purchasing channel. Refer to the Microsoft Product Terms for details.

	Microsoft 365					Office 365			Enterprise Mobility + Security		Windows 11	
	A1 for devices	A3	A5	A5 Security Add-on	A5 Compliance Add-on	A1	A3	A5	A3	A5	Education A3	Education A5
Microsoft 365 Apps												
Desktop client apps[1]	•	◆	◆				◆	◆				
Office Mobile apps[2]	•	◆	◆			•	◆	◆				
Install apps on up to 5 PCs/Mac + 5 tablets + 5 smartphones	•[3]	◆	◆			•[3]	◆	◆				
Office for the web	•	◆	◆			•	◆	◆				
Visio for the web[4]	•	◆	◆			•	◆	◆				
Microsoft Editor premium features		◆	◆				◆	◆				
Multilingual user interface for Office applications	•	◆	◆				◆	◆				
Email, calendar, and scheduling												
Exchange Plan 1 (50 GB mailbox)	•					•						
Exchange Plan 2 (100 GB mailbox)		◆	◆				◆	◆				
Calendar	•	◆	◆			•	◆	◆				
Outlook desktop client	•	◆	◆				◆	◆				
Auto-expanding email archive		◆	◆				◆	◆				
Exchange Online Protection	•	◆	◆			•	◆	◆				
Public folder mailboxes	•	◆	◆			•	◆	◆				
Resource mailboxes	•	◆	◆			•	◆	◆				
Inactive mailboxes	•	◆	◆				•	•				
Microsoft Shifts	•	◆	◆			•	◆	◆				
Microsoft Bookings		◆	◆				•	•				
Social, intranet, and storage												
SharePoint Plan 1 (10 GB storage[1], 1 TB OneDrive storage)	•					•						
SharePoint Plan 2 (10 GB storage[1], unlimited OneDrive storage)		◆	◆				◆	◆				
Yammer Enterprise	•	◆	◆			•	◆	◆				
Microsoft Viva Connections	•	•	•			•	•	•				

[1] Includes Word, Excel, PowerPoint, OneNote, Outlook, Access (PC only), and Publisher (PC only)
[2] Includes Word, Excel, PowerPoint, Outlook, and OneNote mobile Apps
[3] Mobile apps only
[4] Available beginning August – December 2021 depending on region

Figura 34

Parte II - Comparación de la subscripción de los planes para Educación



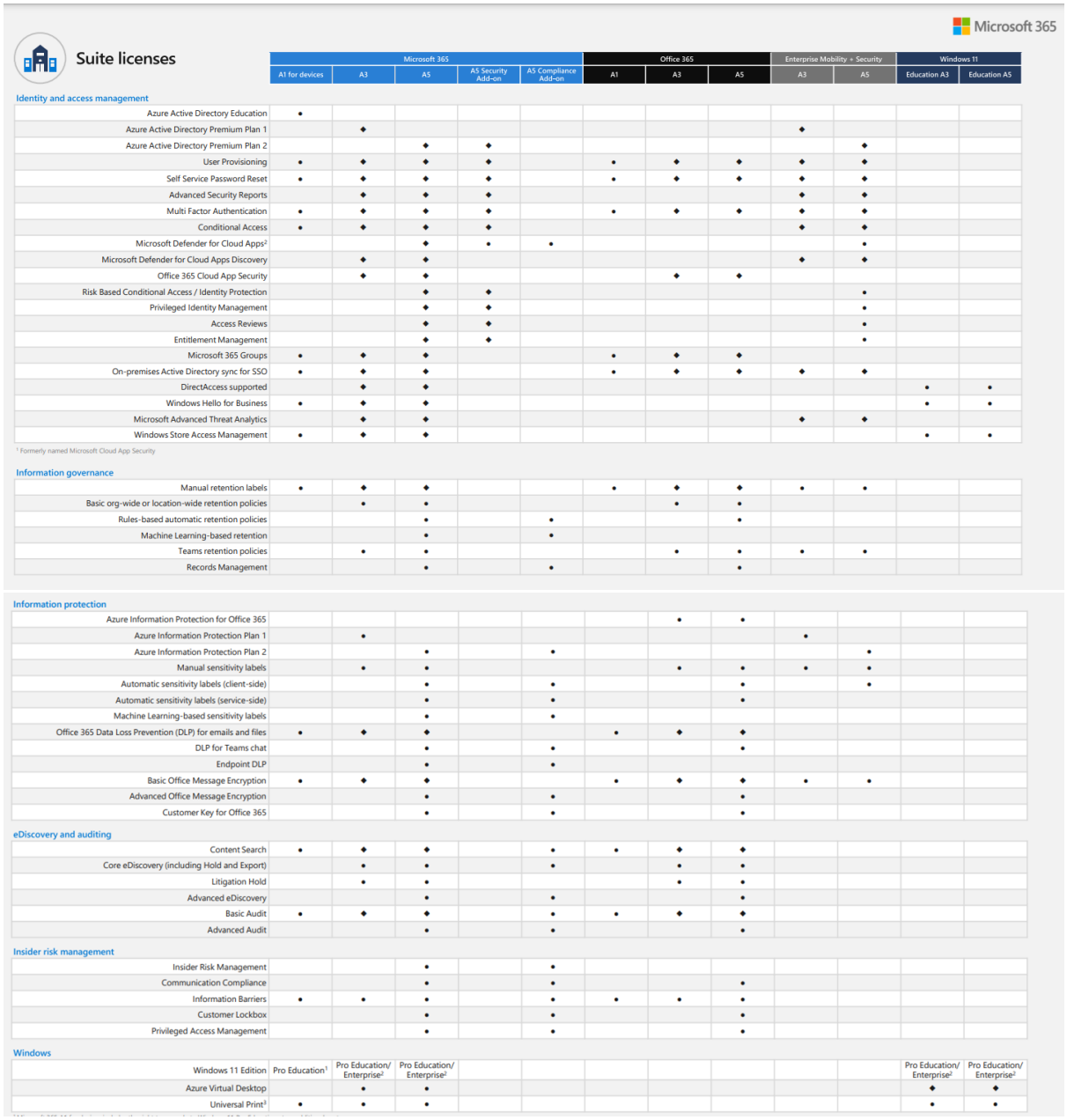
Microsoft 365

Suite licenses

	Microsoft 365					Office 365			Enterprise Mobility + Security		Windows 11	
	A1 for devices	A3	A5	A5 Security Add-on	A5 Compliance Add-on	A1	A3	A5	A3	A5	Education A3	Education A5
Meetings, calling, and chat												
Microsoft Teams	•	◆	◆			•	◆	◆				
1:1 and group online audio and video calls	•	◆	◆			•	•	•				
Scheduled meetings	•	◆	◆			•	•	•				
Recorded meetings	•	◆	◆			•	•	•				
Live events		•	•				•	•				
Webinars		•	•				•	•				
Phone System			•					•				
Audio Conferencing[1]			•					•				
[1]Check country and region availability at https://docs.microsoft.com/microsoftteams/country-and-region-availability-for-audio-conferencing-and-calling-plans												
Classroom tools												
Classroom experience in Microsoft Teams	•	◆	◆			•	◆	◆				
Microsoft Whiteboard	•	◆	◆			•	◆	◆				
OneNote Class Notebook	•	◆	◆			•	◆	◆				
Minecraft Education Edition with Code Builder	•	◆	◆									
Take a Test app[1]	•	•	•									
Set up School PCs app[1]	•	•	•									
[1]Access via Microsoft Store for Education												
Knowledge, insights, and content												
Microsoft Graph API	•	◆	◆			•	◆	◆				
Microsoft Search	•	◆	◆			•	◆	◆				
Microsoft Stream	•	◆	◆			•	◆	◆				
Microsoft Forms	•	◆	◆			•	◆	◆				
Microsoft Lists	•	◆	◆			•	◆	◆				
Delve	•	◆	◆			•	◆	◆				
Automation, app building, and chatbots[1]												
Power Apps for Microsoft 365	•	◆	◆			•	◆	◆				
Power Automate for Microsoft 365	•[2]	◆	◆			•[2]	◆[2]	◆[2]			◆[3]	◆[3]
Power Virtual Agent for Teams	•	◆	◆			•	◆	◆				
Dataverse for Teams	•	◆	◆			•	◆	◆				
[1] Refer to the licensing FAQs and Licensing Guide at https://docs.microsoft.com/power-platform/admin/powerapps-flow-licensing-faq for details including functionality limits. [2] Cloud flows only; no desktop flows. [3] Desktop flows only; no cloud flows.												
Viva Learning[1,2]												
Viva Learning in Teams	•	•	•			•	•	•				
Create learning tabs in Teams channels	•	•	•			•	•	•				
Search, share, and chat about learning content	•	•	•			•	•	•				
Microsoft Learn and Microsoft 365 Training libraries + 125 top LinkedIn Learning courses	•	•	•			•	•	•				
Organization-generated content with SharePoint and Viva Learning	•	•	•			•	•	•				
Project and task management												
Microsoft Planner	•	◆	◆			•	◆	◆				
Microsoft To-Do	•	◆	◆			•	◆	◆				
Briefing Email	•	◆	◆			•	◆	◆				
Analytics												
Compliance Management	•	◆	◆			•	◆	◆				
Viva Insights - Personal insights		•				•	•					
Education Analytics	•	◆	◆			•	◆	◆				
Productivity Score	•	◆	◆			•	◆	◆				
Secure Score	•	◆	◆			•	◆	◆			•	•
Power BI Pro			•					•				
Threat protection												
Microsoft Defender Antimalware		•	•								•	•
Microsoft Defender Firewall		•	•								•	•
Microsoft Defender Exploit Guard		•	•								•	•
Microsoft Defender Credential Guard		•	•								•	•
BitLocker and BitLocker To Go		•	•								•	•
Windows Information Protection		•	•								•	•
Microsoft Defender for Endpoint			•	•								•
Microsoft Defender for Identity			◆	•						◆		
Microsoft Defender for Office 365 Plan 2			◆	◆[1]				Plan 2				
Application Guard for Office 365			◆	◆								
Safe Documents			•	•								
[1] Student Use Benefit = Microsoft Defender for Office 365 Plan 1												
Endpoint and app management												
Microsoft Intune for Education	•	◆	◆						◆	◆		
Mobile Device Management	•	◆	◆			•	◆	◆	•	•	•	•
Microsoft Endpoint Manager	•	•	•						•	•		
Windows AutoPilot	•	•	•						•	•		
Mobile application management	•	•	•						•	•	•	•
Group Policy support	•	•	•				•	•				
Shared computer activation for M365 Apps		•	•				•	•				
Cortana management		•	•								•	•
Endpoint Analytics		•	•						•	•		

Figura 35

Parte III - Comparación de la subscripción de los planes para Educación



Microsoft 365

Suite licenses

	Microsoft 365					Office 365			Enterprise Mobility + Security		Windows 11	
	A1 for devices	A3	A5	A5 Security Add-on	A5 Compliance Add-on	A1	A3	A5	A3	A5	Education A3	Education A5
Identity and access management												
Azure Active Directory Education	•											
Azure Active Directory Premium Plan 1		◆							◆			
Azure Active Directory Premium Plan 2			◆	◆						◆		
User Provisioning	•	◆	◆	◆		•	◆	◆	◆	◆		
Self Service Password Reset	•	◆	◆	◆		•	◆	◆	◆	◆		
Advanced Security Reports		◆	◆	◆					◆	◆		
Multi Factor Authentication	•	◆	◆	◆		•	◆	◆	◆	◆		
Conditional Access	•	◆	◆	◆					◆	◆		
Microsoft Defender for Cloud Apps[2]			◆	•	•					•		
Microsoft Defender for Cloud Apps Discovery		◆	◆						◆	◆		
Office 365 Cloud App Security		◆	◆				◆	◆				
Risk Based Conditional Access / Identity Protection			◆	◆						•		
Privileged Identity Management			◆	◆						•		
Access Reviews			◆	◆						•		
Entitlement Management			◆	◆						•		
Microsoft 365 Groups	•	◆	◆			•	◆	◆				
On-premises Active Directory sync for SSO	•	◆	◆			•	◆	◆	◆	◆		
DirectAccess supported		◆	◆								•	•
Windows Hello for Business	•	◆	◆								•	•
Microsoft Advanced Threat Analytics		◆	◆						◆	◆		
Windows Store Access Management	•	◆	◆								•	•

[1] Formerly named Microsoft Cloud App Security

Information governance												
Manual retention labels	•	◆	◆			•	◆	◆	•	•		
Basic org-wide or location-wide retention policies		•	•				•	•				
Rules-based automatic retention policies			•		•			•				
Machine Learning-based retention			•		•							
Teams retention policies		•	•				•	•	•	•		
Records Management			•		•			•				
Information protection												
Azure Information Protection for Office 365							•	•				
Azure Information Protection Plan 1		•							•			
Azure Information Protection Plan 2			•		•					•		
Manual sensitivity labels		•	•				•	•	•	•		
Automatic sensitivity labels (client-side)			•		•			•		•		
Automatic sensitivity labels (service-side)			•		•			•				
Machine Learning-based sensitivity labels			•		•							
Office 365 Data Loss Prevention (DLP) for emails and files	•	◆	◆			•	◆	◆				
DLP for Teams chat			•		•			•				
Endpoint DLP			•		•							
Basic Office Message Encryption	•	◆	◆			•	◆	◆	•	•		
Advanced Office Message Encryption			•		•			•				
Customer Key for Office 365			•		•			•				
eDiscovery and auditing												
Content Search	•	◆	◆		•	•	◆	◆				
Core eDiscovery (including Hold and Export)		•	•		•		•	•				
Litigation Hold		•	•				•	•				
Advanced eDiscovery			•		•			•				
Basic Audit	•	◆	◆		•	•	◆	◆				
Advanced Audit			•		•			•				
Insider risk management												
Insider Risk Management			•		•							
Communication Compliance			•		•			•				
Information Barriers	•	•	•		•	•	•	•				
Customer Lockbox			•		•			•				
Privileged Access Management			•		•			•				
Windows												
Windows 11 Edition	Pro Education[1]	Pro Education/ Enterprise[2]	Pro Education/ Enterprise[2]								Pro Education/ Enterprise[2]	Pro Education/ Enterprise[2]
Azure Virtual Desktop		•	•								◆	◆
Universal Print[3]	•	•	•								•	•

Figura 36

Parte IV - Comparación de la subscripción de los planes para Educación

● = Included
+ = Can be added
N/A = Not available

	Microsoft 365 E3	Microsoft 365 E5	Office 365 A1	Office 365 A3	Office 365 A5
Security and Compliance					
Microsoft Defender for Office 365 Plan 1	+	●	+	+	+
Microsoft Defender for Office 365 Plan 2	+	●	+	+	+
Microsoft Defender for Cloud Apps[1]	+	●	+	+	+[2]
App governance add-on for Microsoft Defender for Cloud Apps	+	+	+[3]	+[3]	+[3]
Microsoft Defender for Endpoint Plan 1	+	●	+	+	+
Microsoft Defender for Endpoint Plan 2	+	●	+	+	+
Privacy Management for Microsoft 365 - risk	+	+	+	+	+
Privacy Management for Microsoft 365 - subject rights requests	+	+	+	+	+
Premium Assessments add-on for Compliance Manager	+	+	+	+	+
Microsoft 365 A5 Security	+	●	+[5]	+[5]	+[5]
Microsoft 365 A5 Compliance	+	●	+[5]	+[5]	+[5]
Microsoft 365 A5 Info Protection and Governance	+	●	+[6]	+[6]	●+[6,7]
Microsoft 365 A5 Insider Risk Management	+	●	+	+	●+[8]
Microsoft 365 A5 eDiscovery and Audit	+	●	+	+	●
Office 365 Data Loss Protection	●	●	+	●	●
Exchange Online Archiving	●	●	+	●	●

[1] Formerly named Microsoft Cloud App Security
[2] Office 365 A5 includes Office 365 Cloud App Security only, which is a subset of Microsoft Cloud App Security capabilities.
[3] Requires Microsoft Defender for Cloud Apps
[4] For details on available assessments see https://docs.microsoft.com/en-us/office365/servicedescriptions/microsoft-365-service-descriptions/microsoft-365-tenantlevel-services-licensing-guidance/microsoft-365-security-compliance-licensing-guidance#compliance-manager
[5] EMS A5/E5 required
[6] EMS A5/E5 or Azure Information Protection Plan 1 standalone required
[7] Office 365 A5 includes DLP for Teams chat, Rules-based auto classification, advanced Information Governance, Advanced Message Encryption, and Customer Key value of Microsoft 365 A5 Information Protection and Governance but does not include Machine Learning-based auto classification (trainable classifiers).
[8] Office 365 A5 includes the Communication Compliance, Information Barriers, Customer Lockbox, and Privileged Access Management value of M365 A5 Insider Risk Management but does not include the Insider Risk Management product/service.

	Microsoft 365 E3	Microsoft 365 E5	Office 365 A1	Office 365 A3	Office 365 A5
Microsoft Viva					
Viva Topics	+	+	+	+	+
Viva Insights[1,2]	+	+	+	+	+
Viva Insights Capacity[1]	+	+	+	+	+
Viva Learning[1]	+	+	+	+	+
Viva suite[1]	+	+	+	+	+
Viva suite with Glint add-on[1]	+	+	+	+	+

[1] Faculty licenses only; student licenses not available

● = Included
+ = Can be added
N/A = Not available

	Microsoft 365 A3	Microsoft 365 A5	Office 365 A1	Office 365 A3	Office 365 A5
Teams Services[1,2]					
Audio Conferencing	+	●	+	+	●
Phone System	+	●	+	+	●
Domestic Calling Plan[3]	+	●	+	+	●
International Calling Plan (includes Domestic)[3]	+	+	+	+	+
Teams Calling Essentials for US and Canada[4]	+	N/A[5]	+	+	N/A[5]

[1] Availability and included minutes may vary by region. To verify service availability, refer to https://docs.microsoft.com/en-us/microsoftteams/country-and-region-availability-for-audio-conferencing-and-calling-plans/ Consumption charges may apply for additional services, such as toll-free, international minutes for domestic plans, etc. Customers can disable these features to avoid additional billing.
[2] Faculty licenses only; student licenses not available
[3] Phone System required
[4] Includes Phone System and Domestic Calling Plan. Available for purchase in US (including Puerto Rico) and Canada only.
[5] Microsoft 365 A5 and Office 365 A5 include Phone System. Choose a Calling Plan to add calling minutes.

	Microsoft 365 A3	Microsoft 365 A5	Office 365 A1	Office 365 A3	Office 365 A5
Storage					
Office 365 Extra File Storage	+	+	+	+	+
eDiscovery Storage	+	+	+	+	+
Power Platform					
Power BI Pro	+	●	+	+	●
Power BI Premium	+	+	+	+	+
Other					
Scheduler[1]	+	+	+	+	+
Universal Print Volume Add-on (500 print jobs)[2]	+	+	N/A	N/A	N/A
High Efficiency Video Codec (HEVC)[2]	+	+	N/A	N/A	N/A
Education Insights Premium[3]	+	+	+	+	+
Career Coach[3]	+	+	+	+	+

Anexo 8 – Información de Zoho

Figura 37

Precios de los planes que tiene Zoho Drive.

	INICIAL	EQUIPO	EMPRESARIAL
	COMENZAR AHORA	COMENZAR AHORA	COMENZAR AHORA
PRECIOS (Los impuestos locales (IVA, impuesto sobre bienes y servicios, etc.) se cobrarán de manera adicional con respecto a los precios que se mencionaron.)			
Facturación anual	$2/usuario/mes	$4/usuario/mes	$8/usuario/mes
Facturación mensual	$2.5/usuario	$5/usuario	$10/usuario
Almacenamiento	Comienza con 1 TB/equipo	Comienza con 3 TB/equipo	Comienza con 5 TB/equipo
Almacenamiento adicional	Después de 10 usuarios, obtenga almacenamiento compartido adicional de 100 GB/nuevo usuario.	Después de 10 usuarios, obtenga almacenamiento compartido adicional de 300 GB/nuevo usuario.	Después de 10 usuarios, obtenga almacenamiento compartido adicional de 500 GB/nuevo usuario.
Límite de carga	1 GB	5 GB	50 GB

Figura 38

Parte I - Funcionalidades disponibles para los Usuarios

PARA USUARIOS

Colaboración interna			
Carpetas de equipo	sí	Sí	Sí
Controles detallados de acceso	Sí	Sí	Sí
Uso compartido de subcarpetas	Sí	Sí	Sí
Vista previa	Sí	Sí	Sí
Vista previa y extracción de archivos Zip	-	-	Sí
Búsqueda de contenido universal	Sí	Sí	Sí
Bloqueo de archivos	-	Sí	Sí
Comentarios en archivos	Sí	Sí	Sí
Generación ilimitada de versiones de archivos	Sí	Sí	Sí
Actualizaciones de seguimiento	Sí	Sí	Sí
Recolección de archivos - Recolección interna	-	Sí	Sí
Notificaciones no leídas y globales	Sí	Sí	Sí
Zoho Office Suite			
Zoho Writer	Sí	Sí	Sí
Zoho Sheet	Sí	Sí	Sí
Zoho Show	Sí	Sí	Sí
Colaboración externa			
Enlaces personalizables de archivos	Sí	Sí	Sí
Enlaces con fecha de vencimiento protegidos con contraseña	Sí	Sí	Sí
Control de acceso externo a archivos	Sí	Sí	Sí
Recolección de archivos - Recolección externa	-	Sí	Sí
Usuarios de cliente	$1 /usuario de cliente/mes $12 /usuario de cliente/año	$1 /usuario de cliente/mes $12 /usuario de cliente/año	$1 /usuario de cliente/mes $12 /usuario de cliente/año

Figura 39

Parte II - Funcionalidades disponibles para los Usuarios

Clasificación de datos			
Etiquetas	Sí	Sí	Sí
Mis Plantillas	Sí	Sí	Sí
Grupos			
Añada grupos a carpetas de equipo	Sí	Sí	Sí
Comparta archivos y carpetas con grupos	Sí	Sí	Sí
Acceso móvil			
Aplicaciones móviles para Android y iOS	Sí	Sí	Sí
Aplicaciones de escritorio			
Sincronización de escritorio	Sí	Sí	Sí
Sincronización bidireccional	Sí	Sí	Sí
WorkDrive Genie para Windows	Sí	Sí	Sí
Generación y análisis avanzados de informes			
Estadísticas de acceso a archivos	-	Sí	Sí
Cronología de actividades de archivos	-	Sí	Sí
Zoho Directory			
Integración de inicio de sesión único basada en SAML	-	-	Sí
Seguridad			
Cifrado en reposo AES de 256 bits	Sí	Sí	Sí
Cifrado TLS, SSL y PFS durante el tránsito	Sí	Sí	Sí
Sistemas de detección y prevención de intrusiones	Sí	Sí	Sí
Autenticación de dos factores	-	-	Sí
Soporte			
Asistencia telefónica y por correo electrónico continua de lunes a viernes	Sí	Sí	Sí

Figura 40

Funcionalidades disponibles para los Administradores

PARA ADMINISTRADORES

Controles de administración			
Administración de usuarios	Sí	Sí	Sí
Administración de dispositivos	-	-	Sí
Personalización de marca	-	Sí	Sí
Personalización de dominio	-	-	Sí
Control del uso compartido externo	Sí	Sí	Sí
Clasificación de datos			
Plantillas de datos y campos personalizados	-	-	Sí
Plantillas organizacionales	Sí	Sí	Sí
Administración de datos			
Transferencia de la propiedad de los archivos privados	Sí	Sí	Sí
Retención personalizada de datos	-	-	Sí
Visibilidad y administración completa de contenido	-	-	Sí
Recuperación de archivos	-	-	Sí
Generación y análisis avanzados de informes			
Panel de administración	Sí	Sí	Sí
Genere y exporte informes personalizados de actividad	-	-	Sí
Cronología de actividades de la carpeta de equipo	-	Sí	Sí
Seguridad			
Política de contraseñas personalizada	-	-	Sí
Restricción de IP	-	-	Sí
Integración SAML basada en SSO	-	-	Sí

Anexo 9 – Información de Confluence Cloud

Figura 41

Free Plan [Plan Gratuito]

Learn about Confluence Cloud plans

Plans in Confluence Cloud let you choose the right features and functionality for your stage of business. From teams of three where you share everything, up to large enterprises with thousands of staff where visibility and control are paramount, there's a plan to suit your needs.

To see pricing for Confluence Cloud plans, go to this page.

Find billing and account information for Atlassian Cloud plans on this page.

What do I get with each plan?

Free

The Free plan is for small teams of fewer than 10 people who are just getting started with Confluence.

On the Free plan you get:

- Up to 10 users
- 2 GB of file storage
- Atlassian Community support

Permissions aren't customizable and anonymous access isn't available on the Free plan. If your site has always been on the Free plan, everyone who can log in to your Confluence site can view, add, and edit spaces and pages. If you change to the Free plan or migrate from Confluence Server to the Free plan, existing global, space, and page permissions will be kept in their current state, but anonymous access will be disabled. You'll need to upgrade again to change permissions or enable anonymous access. Read more about permissions and restrictions in the Free plan.

You won't have access to audit logs to track events related to spaces, users, and administration on your site. Once you upgrade to Standard, you'll be able to use audit logs for your Confluence Cloud site.

Figura 42

Niveles de permisos y restricciones disponibles en Confluence Cloud

Levels of permission

There are three levels of permissions in Confluence: global permissions, space permissions, and page restrictions.

Global permissions

Global permissions are site-wide permissions, and are assigned by Confluence administrators.

These permissions are pretty broad, and don't really interact with space permissions or page restrictions.

For full details, check out the Manage global permissions in the *Administrator's Guide*.

Space permissions

Every space has its own independent set of permissions, managed by the space admin(s), which determine the access settings for different users and groups.

They can be used to grant or revoke permission to view, add, edit, and delete content within that space, and can be applied to groups, users, and even to anonymous users (users who aren't logged in) if need be.

One thing to watch out for is where a user is a member of multiple groups. You may have revoked permission for that individual user to add pages, for example, but if they're a member of a groups that *is* allowed to add pages, they'll still be able to create new pages in the space.

If you can't get the result you want from space permissions, or you're not sure, check with one of your Confluence administrators to determine what permissions you should apply to individuals and groups.

Page restrictions

Page restrictions work a little differently to global and space permissions. Pages are open to viewing or editing by default, but you can restrict either viewing or editing to certain users or groups if you need to.

Don't forget, every page in Confluence lives within a space, and space permissions allow the space admin to revoke permission to view content for the whole space. Even the ability to apply restrictions to pages is controlled by the 'restrict pages' space permission.

Figura 43

Audit log [Registro de auditoría].

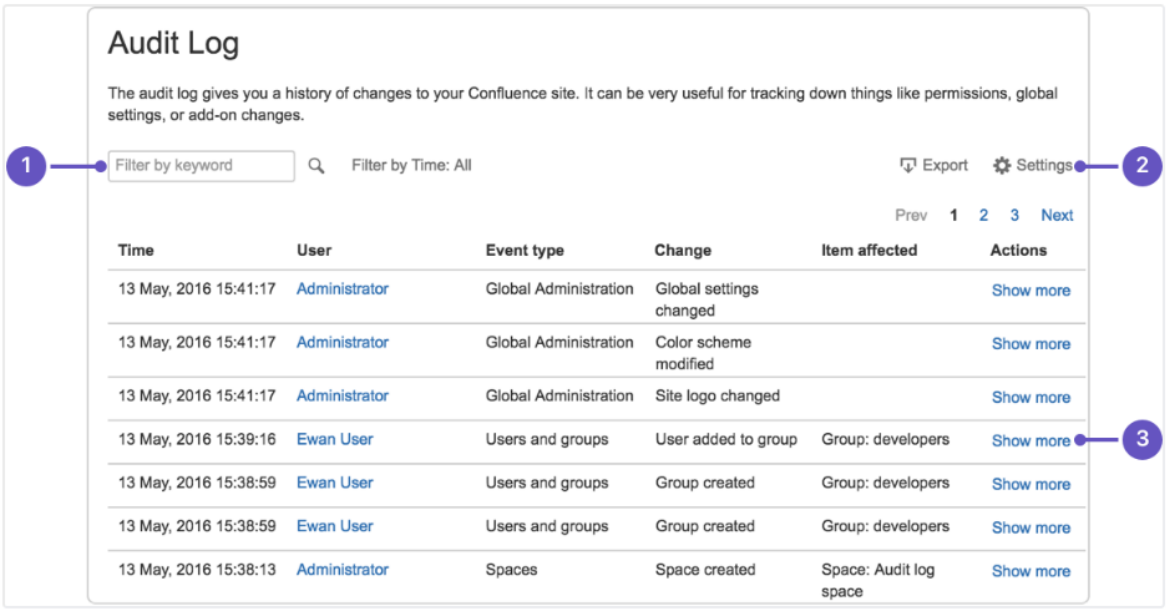
View the audit log

You'll need Confluence Administrator permissions to view the audit log. The audit log isn't available on the Free plan.

The audit log allows administrators to look back at changes that have been made in your site. This is useful when you need to troubleshoot a problem or if you need to keep a record of important events, such as changes to global permissions.

To view the audit log, select (Settings) in the Confluence navigation, then **Audit log**.

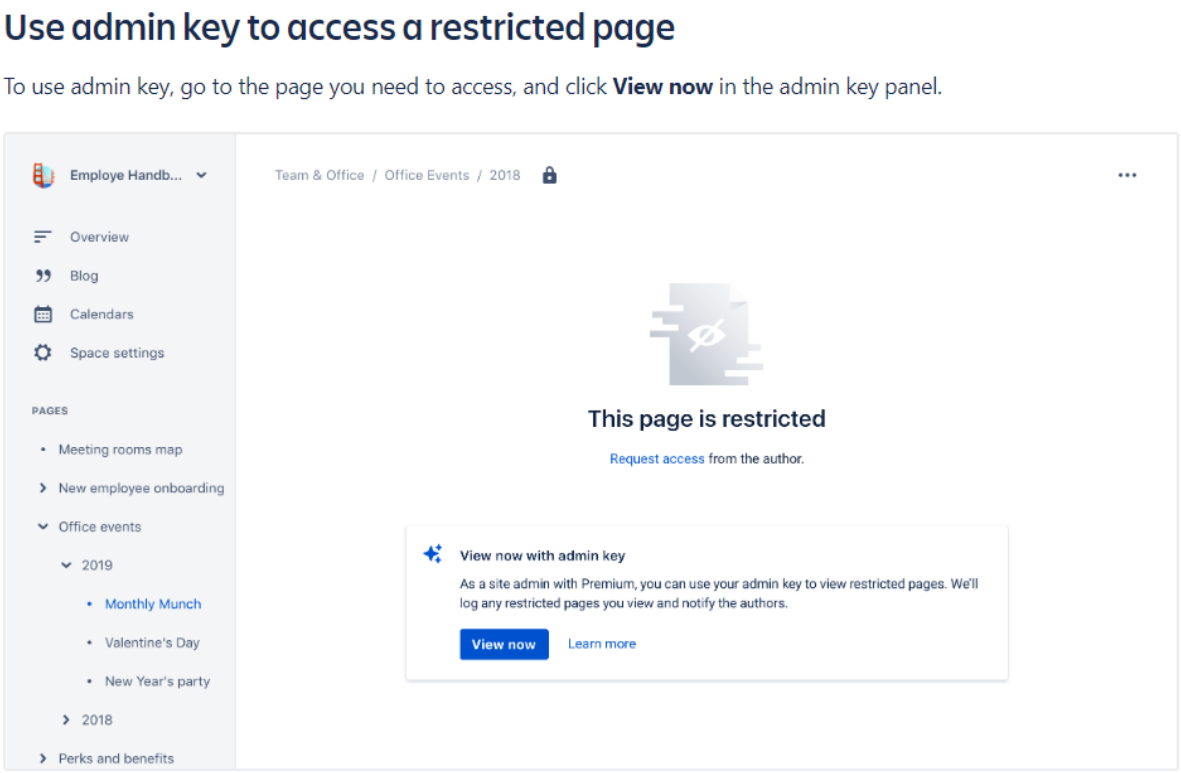
You can then filter the log by keyword and time to narrow down the results. Here's how it looks.



1. **Filter it:** dig into the log by keyword or by time.
2. **More control:** export the whole log or change how long to keep events
3. **Get detailed:** see the details of each change.

Figura 44

Seguridad para páginas restringidas usando una Llave de Acceso



This enables admin key and gives you full access to the page. When you use admin key to access a page, we'll record it in your site's audit log and send an email notification to the page owner. We'll also record any changes you make in the audit log and page history.

Once admin key is enabled, you'll be able to see and navigate to other restricted content on your site. If a page is restricted, there will be a red lock icon next to its name in the page tree.

Figura 45

Descripción de lo que incluye los planes Standard y Premium

Standard

As your team grows and you need tighter access control, more file storage, and better support, you can move to Standard or Premium.

On the Standard plan you get:

- Up to 35,000 users
- 250 GB of file storage
- Permissions, including global, space, and page permissions
- Audit logs for keeping track of important changes
- Page archiving
- Public links
- Data residency (control over where your in-scope product data is hosted)
- Standard Support (available 9am–5pm Monday to Friday for your time zone)

⚠ If you'll need more than 5,000 users and expect more than 50% of them will be actively using Confluence at the same time (concurrently), then the premium plan's optimized cloud infrastructure may better suit you. Most enterprise organizations that use our products regularly tend to have heavier concurrent usage.

Premium

The Premium plan is currently available for Confluence Cloud. This plan gets you everything from the Standard plan, plus:

- Analytics
- Admin key
- Team Calendars
- Bulk archive
- Unlimited file storage
- Optimized cloud infrastructure to better handle 5,000+ concurrent users
- Premium dedicated Atlassian 24/7 support
- 99.9% uptime service level agreement (SLA)
- Sandboxes
- Release tracks

Analytics includes insights on:

- The usage of your Confluence Cloud site
- How many total and unique views your spaces and pages have had
- Who's viewed the latest updates to your pages

Admin key lets admins troubleshoot restricted pages by giving them temporary access to the pages.

Enterprise

The Enterprise plan is available for Confluence Cloud. This plan gets you everything from the Premium plan, plus you can:

- Give users access to an unlimited number of Confluence Enterprise products and only pay for each user once
- Get our 99.95% uptime service level agreement (SLA)

To inquire about an Enterprise trial or change to an Enterprise plan, fill out our contact form and someone from our team will reach out.

Anexo 10 – Alertas de seguridad para correos

Figura 46

Etiqueta para indicar que el correo proviene de una dirección externa

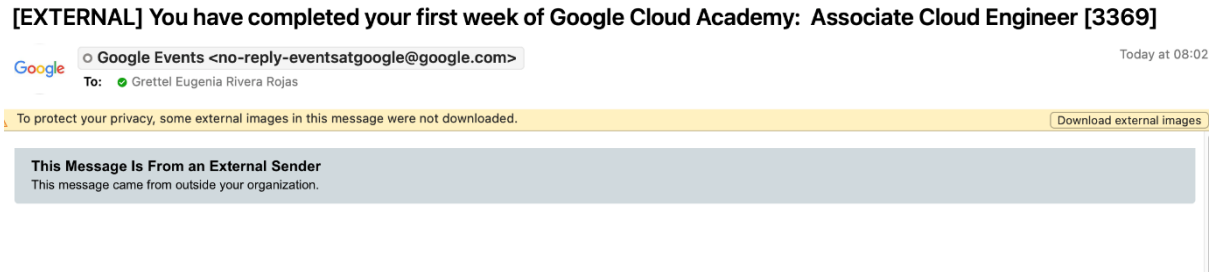


Figura 47

Leyenda de advertencia para envíos de correo con información confidencial

LA INFORMACION CONTENIDA EN ESTE MENSAJE VIA INTERNET ES CONFIDENCIAL Y DESTINADA SOLAMENTE PARA EL USO DE LA PERSONA O ENTIDAD MENCIONADA. SI EL RECEPTOR DE ESTE MENSAJE NO ES LA PERSONA DE DESTINO MENCIONADA,CUALQUIE DIVULGACION, DISTRIBUCION O COPIA DE LA INFORMACION CONTENIDA EN ESTE MENSAJE VIA INTERNET SE ENCUENTRA ESTRICTAMENTE PROHIBIDA, SI USTED RECIBE ESTE MENSAJE POR ERROR, POR FAVOR NOTIFIQUE AL EMISOR DEL MISMO DE INMEDIATO.