**LA AUDITORÍA DE SISTEMA EN LAS EMPRESAS DE CERTIFICADOS DIGITALES.**

*Autores: Daniel Enrique Galindo Barreto, Jhon Elvis Robledo Martínez*

*Especialización Auditoria de Sistemas, Universidad Antonio Nariño, 2022-1*

Resumen: En el presente artículo se muestra la información general sobre una empresa de certificación digital, el proceso para creación de un certificado digital, beneficios de tener una auditoría de sistemas implementado y cómo generar un departamento de auditoría de Sistemas dentro de una empresa de Certificación Digital.

Palabras Claves: Auditoría de Sistemas, Certificado Digital, Etapas de Auditoría de Sistemas

Abstract: This article shows the general information about a digital certification company, the process for creating a digital certificate, benefits of having an audit of systems implemented and how to create a Systems audit department within a Digital Certification company.

# Introducción

Para las empresas es importante mantener un margen de productividad de alto a un menor costo o esfuerzo, donde se pueda brindar un máximo de la capacidad de producción, interacción Empresa – Cliente, y por qué no, reducir los índices de presión o sobre carga laboral en los diferentes cargos internos, haciendo énfasis en cargos gerenciales y/o administrativos; centralizando las tareas prioritarias y dejando a un lado aquellas que pueden ser importantes pero que no consuman tiempo labor. Es por esto que se han buscado diferentes alternativas o mecanismos donde la persona pueda disminuir sus tiempos atendiendo actividades de papeleo, autorizaciones o documentos de interés interno o externo para cada empresa; y es allí, donde la tecnología y la inversión en la misma juegan un papel importante brindando herramientas de fácil uso, no así su complejidad, para agilizar trámites básicos pero esenciales como firmas de contratos, autorizaciones de facturas electrónicas, verificaciones y validaciones de importaciones, firma de trámites frente a entidades gubernamentales, publicaciones de información para conocimiento interno y externo.

Adicional a esto, y como es sabido en todo ámbito económico la pandemia por COVID-19 y su confinamiento; expuso en su mayoría la mala organización empresarial y la dependencia de ciertos procesos para ejecutarlos de manera presencial; y bajo la imposibilidad de realizarlos de manera oportuna por las diferentes medidas de salud pública tomada por todos los gobiernos; se evidencio la necesidad de buscar herramientas que brindarán una solución oportuna para cumplir dichos procesos con la mayor confianza, no repudio y bajo todo marco legal dispuesto. Es aquí donde la ayuda de los certificados digitales o firmas digitales empezaron a tomar más fuerza y protagonismo en el ámbito empresarial. Aunque no es una tecnología reciente, y su regulación no es tan antigua, entraron a jugar con un gran peso y responsabilidad jurídica validada y avalada por diferentes organismos nacionales e internacionales para su correcta ejecución y uso; empezando la utilización masiva y con crecimiento exponencial por su fácil uso y todo el respaldo que ofrece hacia el uso adecuado.

Para el correcto funcionamiento las empresas de certificación abierta internamente deben de tener un control de procesos muy específico, gestión documental avanzada y detallada para poder cumplir a cabalidad la legislación actual y sobre todo deben tener todo un control riguroso de la información y privacidad de la misma; ya que la referencia que maneja de los usuario que están solicitando un certificado es información sensible con datos financieros, comerciales y privados, que deben tener el mayor rigor para su manejo. La seguridad del manejo de la información debe estar estipulada y clara para el usuario siendo aquí donde se puede encajar una auditoría de sistemas realizando la verificación pertinente de los controles y el flujo de la información entre las diferentes áreas internas de la empresa de certificación, como puede ser el manejo comercial, el ciclo de operaciones de la certificación, validación documental, validación de identidad, verificación de la información y emisión del certificado con publicación y/o entrega del producto final, cumpliendo con los altos estándares que la normativa exige.

¿Por qué es importante realizar Auditoria de Sistemas a Empresas de Certificación digital?. La Auditoría de Sistemas1 es una disciplina joven, nacida a principios de los ochenta, en respuesta al avance de las tecnologías de información y comunicaciones, y hoy en los albores de la cuarta revolución industrial, enfrenta grandes retos en el mundo de los negocios digitales, la velocidad de las transformaciones, el crecimiento de la complejidad de los sistemas de información y su fusión con el Internet de las Cosas (IoT),la movilidad, los servicios Cloud, el Big Data y la analítica para manejar los grandes volúmenes de datos, son aspectos que hacen que el riesgo de las Tecnologías de la Información (TI) sea hoy más ambiguo, volátil e incierto. Esta Auditoría de Sistemas puede encargarse de encontrar alguna brecha o fuga de información, ya sea por el personal a cargo de las operaciones o validaciones documentales o en el manejo inadecuado de las bases de datos o durante el proceso digital de la información que se transmite de área a área, donde los procesos de las aplicaciones utilizadas deben estar detalladas y que no se vea manipuladas frente a la información inicial cargada por el usuario solicitante del certificado.

Por esto, se debe conocer que es un certificado digital y el posible flujo de la información que pueda tener una entidad certificadora como se expresa más adelante

Inicialmente se realizó la identificación de las características presentes en las empresas asociadas a certificados digitales, que pueden ser evaluadas a través de una auditoría de sistemas con el fin de realizar una metodología observación percibiendo rasgos característicos de la auditoría de sistemas y así poder aplicar la información hacia un departamento de auditoría de sistemas. Posteriormente se relacionaron las necesidades de la recepción de información para la emisión del certificado digital con los requerimientos técnicos de certificado digital y se identificaron los parámetros de mayor incidencia en la calidad y privacidad de la información, que son la recepción de la información o documentos que el usuario debe entregar para la validación y verificación y posterior emisión de certificado, el almacenamiento de dicha información y el manejo o tratamiento que se le da para concentrarla y plasmarla en el certificado digital. Encontrado que se realiza la recepción de información por medio de una plataforma web tipo formulario donde el usuario diligencia información respecto a documentación emitida por entidades gubernamentales como, documento de identidad del solicitante, documento de existencia y representación legal para el caso de las empresas e información relacionada al solicitante como contrato, tarjeta profesional, registros tributarios; considerando así información sensible y privada. Se distingue el proceso general que una empresa de certificación digital realiza para el manejo de la información anterior mencionada y condensarlo en el certificado digital y su encriptación característica dependiendo del tipo de certificado a emitir; donde se usan aplicaciones de consulta con varias plataformas gubernamentales para la validación de información y compararla con la brindada por el usuario y así otorgar validez de la misma. Sobre estas aplicaciones se realiza la guía de auditoría verificando los controles establecidos para el almacenamiento de información, manejo y/o tratamiento y posterior publicación del certificado digital.

Se continuó con verificar las fases de auditoría de sistemas y así aplicarlas a una empresa de certificación digital, entendiendo su funcionamiento y herramientas que utilizan para la emisión de certificados digitales para los múltiples clientes que poseen; ajustando las fases de planeación, ejecución, comunicación de resultados y controles posteriores al proyecto de auditoria; para poder esclarecer la guía para la implementación de la auditoría de sistemas a la empresa de certificación digital.

# ¿Qué es un certificado digital?

Un certificado digital es un documento informático generado por una entidad de Certificación Abierta, que conecta y relaciona los datos de una identidad, con una persona, organismo o empresa; confirmando absolutamente a nivel jurídico, que esa identidad ha firmado las transacciones electrónicas realizadas. (GSE, Certificados Digitales, 2020)

El certificado digital permite la firma electrónica de documentos; el receptor de un documento firmado puede tener la seguridad de que éste es el original y no ha sido manipulado y el autor de la firma electrónica no podrá negar la autoría de esta firma. (València, 2020)



*Ilustración 1 Certificado digital en dispositivo Criptográfico*

(GSE, Certificados Digitales, 2020)

Dependiendo del uso se pueden determinar diferentes tipos de certificados digitales explicados a continuación:

## Certificado Digital Persona Natural

Es un certificado digital que se emite a quien lo solicita posterior a la validación de su identidad, garantizando que los documentos, o transacciones firmadas digitalmente por esa identidad son legalmente válidos. Si cuentas con una firma de persona Natural podrás usarla en trámites como:

* Contratos.
* Representante de empresas Unipersonales.
* Certificaciones. (GSE, Certificados Digitales, 2020)

## Certificado Digital Representación de Empresa

Es emitido para una persona natural que representa a una determinada entidad jurídica. El titular del certificado se identifica no únicamente como persona física perteneciente a una empresa, sino que añade su cualificación como representante legal de la misma. Si cuentas con una firma como representación de empresa podrás usarla en trámites como:

* Aprobación de documentos internos.
* Firma de declaraciones de impuesto.
* Ordenar gastos. (GSE, Certificados Digitales, 2020)

## Certificado Digital Perteneciente Empresa

Garantiza la identidad de la persona natural titular del certificado, así como su vinculación a una entidad jurídica en virtud del cargo que ocupa en la misma. Este certificado no otorgará por sí mismo mayores facultades a su titular que las que posee por el desempeño de su actividad habitual. Si cuentas con una firma como representante legal podrás usarla en trámites como:

* Firmar contratos.
* Aprobación de presupuestos.
* Firmar informes. (GSE, Certificados Digitales, 2020)

## Certificado Digital Función Pública

Garantiza la identidad de la persona natural titular del certificado, así como su vinculación a una entidad pública en virtud del cargo que ocupe como funcionario público. Si cuentas con una firma de funcionario público podrás usarla en trámites como:

* Emitir reportes ante entidades de control.
* Ordenar gastos.
* Aprobación de compras y proyectos.
* Firmar actos administrativos. (GSE, Certificados Digitales, 2020)

## Certificado Digital Profesional Titulado

Garantiza la identidad de la persona natural titular del certificado, así como su condición de profesional titulado. Este certificado no otorgará por sí mismo mayores facultades a su titular que las que posee por el desempeño de su actividad habitual en el ámbito de su profesión. Si cuentas con una firma como profesional titulado podrás usarla en trámites como:

* Firmar de balances.
* Revisoría fiscal.
* Firmar reportes ante entidades de control. (GSE, Certificados Digitales, 2020)

## Certificado Digital Persona Jurídica

Es un certificado digital que se emite a una entidad representada por una persona quien actúa como responsable y poseedor del certificado emitido bajo esta característica. Si cuentas con una firma de persona jurídica podrás usarla en trámites como:

* Digitalización de archivo físico.
* Pasarelas de pago.
* Facturación electrónica. (GSE, Certificados Digitales, 2020)

## Certificado Digital Factura Electrónica

Es un certificado digital que se emite a una empresa o negocio representado por una persona quien actúa como responsable y poseedor del certificado emitido bajo esta característica con el que se podrá firmar las facturas electrónicas solicitadas por la DIAN como para el caso de Colombia. (GSE, Certificados Digitales, 2020)

## Certificados SSL

Los SSL son pequeños archivos de datos que conectan una llave criptográﬁca con los detalles de una organización. Una vez instalado en el servidor web, activa el candado y el protocolo https (a través del puerto 443) y permite conexiones seguras desde el servidor web hasta el navegador. El certificado SSL garantiza que las comunicaciones que se produzcan entre el navegador de Internet y el servidor Web de una entidad se realicen de una manera segura, protegiendo el intercambio de información entre un usuario y la entidad. (GSE, Certificados Digitales, 2020)

## Normativa para Colombia referentes a certificación digital.

En Colombia existe una normativa, que, aunque no es directamente para la generación de certificados digitales, si se puede enlazar para el manejo de la información confidencial y de manera digital y a su vez también para el tratamiento de datos sensibles para una empresa o una persona que vaya a solicitar el certificado digital para manejo con plataformas gubernamentales online o digitales. Las cuales deben de ser tenidas en cuenta al momento de realizar una auditoría de sistemas y verificar que se cumpla con estas regulaciones.

* + Ley 527 de 1999

“Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones” (Certicamara, 2018)

* + Decreto Ley 019 de 2012

“Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública”. (Sus artículos 160, 161, 162 y 163 modifican los artículos 29, 30, 32 y 34 de la Ley 527 de 1999) (Certicamara, 2018)

* + Decreto 1074 de 2015

“Por medio del cual se expide el decreto Único Reglamentario del Sector Comercio, Industria y Turismo” (Compila al Decreto 333 de 2014) (Certicamara, 2018)

* Decreto 333 de 2014

El presente decreto tiene por objeto definir el régimen de acreditación de las entidades de certificación, en desarrollo de lo previsto en el artículo 160 del Decreto-ley 19 de 2012.

* Decreto 2364 de 2012

Por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.

# Beneficios de la Auditoría de Sistemas a Empresas de Certificación Digital

Para los desafíos del mundo actual, es necesario reducir o mitigar los riesgos tecnológicos de manera tal que, no pongan en peligro la información sensible de la organización. Es por esto que nace la importancia de la auditoría de sistemas o auditoría informática, ya que nos asiste a cumplir con lo mencionado. (AMBIT, 2021)

Hoy en día cualquier tipo de empresa depende de elementos y dispositivos tecnológicos para poder realizar sus procesos de negocio, por lo que es necesario que evalúe de forma periódica su seguridad. Los principales beneficios que aporta el realizar una auditoría de sistemas en una empresa de certificación digital son:

* Mejora los controles internos de seguridad de la empresa.
* Detecta debilidades en los sistemas como errores, omisiones o fallos.
* Identifica posibles actuaciones fraudulentas (acceso a datos no autorizados o robos a nivel interno).
* Ayuda a eliminar los puntos débiles de la empresa en cuestión de seguridad (webs, correo electrónico o accesos remotos, por ejemplo).
* Permite controlar los accesos, tanto físicos como virtuales (revisión de privilegios de acceso).
* Permite mantener sistemas y herramientas actualizadas. (AMBIT, 2021)

Adicionalmente, la revisión de controles a los procesos periódicamente alienta a mantener una calidad de los procesos lo que se ve reflejado en la satisfacción del cliente o suscriptor, permitiendo así tener un buen nombre como empresa de certificación digital y lo más importante que el suscriptor vuelva a comprar un producto y pueda traer consigo más clientes o suscriptores; mejorando notablemente el flujo de caja económico.

También es beneficioso para una empresa de certificados digitales el aplicar auditoria de sistema por diversas razones, entre ellas el marketing, al realizar una óptima auditoría le va a permitir a la empresa mejorar la competitividad en el mercado, su Ranking como empresa de certificación digital ya sea nacional o departamental va a ser potencializada partiendo de la disminución de márgenes de errores que conlleva el haber aplicado una auditoría de sistemas, sin olvidarnos la incidencia positiva que va a tener en los registros de todas las operaciones realizadas o en las finanzas de la entidad. Como bien sabemos todas las empresas tecnológicas buscan a diario mejorar sus ingresos, ventas y flujo de caja, información ligada a los resultados de las actividades realizadas y de cómo ve la comunidad los servicios que ofrece la empresa de certificación, tanto en las políticas de uso, en las alertas de seguridad, atención al cliente en preventa y postventa y mejoramiento continuo en estas características y en otras se logra si existen varias evaluaciones y controles a los mismos procesos y que la alta gerencia de la empresa tome las observaciones y hallazgos de primera mano para darle solución o continuidad, para que al final el usuario logre sentir esas mejoras y aumente ese sentimiento de “la empresa piensa en mí como usuario” fortaleciendo la fidelización de los mismos clientes.

# Proceso de Auditoría a una entidad de Certificación Digital

Para los desafíos del mundo actual, es necesario reducir o mitigar los riesgos tecnológicos de manera tal que, no pongan en peligro la información sensible de la organización. Es por esto que nace la importancia de la auditoría de sistemas o auditoría informática, ya que nos asiste a cumplir con lo mencionado. (Ciro Arenas, 2018) En la mayoría de las organizaciones se vienen adelantando análisis de riesgos de TI, sin embargo se observa cómo estos análisis o bien se hacen de forma separada a los del resto de riesgos de negocio o son realizados por un área externa a auditoría interna. Dada la importancia que tienen los proyectos de TI dentro de las organizaciones, no sólo por aspectos de inversión sino por el impacto de negocio que esperan generar, se evidencia gran oportunidad para que los auditores de TI se involucren desde las fases iniciales logrando así un mayor aporte (Ciro Arenas, 2018); por estos motivos y para mantener los procesos empresariales con alta calidad, es importante para una entidad de Certificación Digital contar con un proceso claro o un área de Auditoría de Sistemas interna o de contrato externo pero muy activo para examinar los procesos críticos dentro de la emisión de un certificado digital. Y a continuación se dará una guía frente a los aspectos para tener en cuenta dentro de la auditoría de sistemas.

Dentro del proceso de certificación se tienen que realizar varias actividades como el cargue de documentos por parte del solicitante y la validación de los mismos en el grupo encargado en la empresa certificadora, donde se usan múltiples herramientas informáticas y en algunos casos APIs de consulta con plataformas gubernamentales para constatar la veracidad de la información entregada por el solicitante y así sea emitido el certificado digital; y es aquí donde la Auditoría de Sistemas juega un papel importante no solo verificando el proceso de uso de plataformas digitales sino también realizando la verificación y prueba de los controles de seguridad tanto en base de datos de la información como de la interacción de la misma, publicación entre diferentes áreas de la entidad certificadora y la validación de identidad del suscriptor para poder así entregar el certificado a la persona que lo requirió.

Dentro de los riesgos que se pueden presentar es la pérdida de información sustancial para un solicitante o la publicación indebida de la información, es decir fallos de base datos en integridad, confidencialidad y por qué no confiabilidad; esto implica que los controles sean estrictos por el mismo manejo que representa la confidencialidad de la información del solicitante y a su vez la privacidad de la misma. Por esto mismo cuando una entidad de certificación abierta entra a operar debe tener claro los CRITERIOS ESPECÍFICOS DE ACREDITACIÓN ENTIDADES DE CERTIFICACIÓN DIGITAL (ONAC, 2015) dictados por ONAC; donde se establecen los lineamientos principales para el proceso de Certificación y garantía de la información así mismo como el ciclo de vida del certificado y el soporte que debe tener para su publicación y manejo. Bajo estos criterios para emisión de certificados digitales se debe establecer el primer pase de enfoque de la Auditoría, donde se debe evaluar a cuidado, los eventos de riesgo y críticos para el cumplimiento de la cadena de emisión y custodia de la información. Dentro del proceso de auditoría se debe enfocar las fases de la auditoría hacia las aplicaciones o sistemas empleados para la creación del certificado digital y todos los pasos que la emisión conlleva; basándose en los riesgos que este proceso conlleva y de manera que se abarquen las etapas de planificación ejecución, comunicación de resultados, y control.

## Planificación:

Lo primero consiste en elaborar un plan de auditoría lo más detallado posible, en donde se defina la naturaleza de la auditoría aplicada a la certificación digital, el alcance verificando si el proceso es igual para todos los tipos de certificación digital o si se va a realizar sobre uno en específico, los objetivos, el período de revisión, la estrategia para analizar los riesgos establecidos por la entidad certificadora y sus controles para minimizar dichos riesgos, las actividades y los recursos necesarios para llevarla a cabo. Es importante que el auditor tenga un entendimiento claro del negocio de certificación digital y su emisión, así como los conocimientos y experiencia previa acerca de los sistemas (bases de datos, aplicaciones web, API si existen, entre otros como lenguajes de programación) que formarán parte del alcance de revisión. Además, en esta etapa se identifican los riesgos más críticos y los controles relacionados a dichos riesgos, que deben ser evaluados por parte del equipo auditor para su propio proyecto de auditoría.

## Ejecución:

El equipo auditor realiza las actividades según lo planificado (etapa previa), en base a una metodología y mediante la aplicación de programas de trabajo basado en buenas prácticas y conocimientos obtenidos anteriormente en proyectos de auditoría; adicional a esto se validará también el conocimiento en el tema de certificación digital para seguir la hoja de ruta y llevar a buen término el proyecto de auditoria. En esta etapa es importante la elaboración adecuada de papeles de trabajo que sustentan los hallazgos u observaciones. Para ello, las evidencias deben obtenerse de manera adecuada bajo los parámetros establecidos en la planeación.

Asimismo, es importante tener en cuenta que una situación se vuelve relevante y es candidata para convertirse en un hallazgo, en la medida que dicha situación (lo que ocurre) se aleje de su línea base o estándar (el cómo debería ser) establecido para la certificación digital o su proceso de validación documental o de identidad usando la plataforma establecida por la entidad certificadora.

## Comunicación de resultados

Luego de empezar la ejecución, el auditor elabora un borrador del informe y lo discute previamente con la gerencia o responsable del manejo de las plataformas de certificación, adicional a esto el auditor tiene la potestad de ir comunicando directamente los hallazgos u observaciones a medida que se van encontrando de manera verbal. Dicho informe debe contener principalmente los hallazgos, los riesgos asociados, y las recomendaciones para subsanar los hallazgos encontrados dentro de las diferentes plataformas o aplicaciones usadas. Aquí es fundamental que el equipo auditor revise junto al auditado, cada uno de los hallazgos encontrados, y que ambas partes estén de acuerdo frente a las observaciones ofrecidas. Adicionalmente, como resultado de esta revisión, deben añadirse al informe los comentarios del auditado con respecto a cómo, cuándo y quién será responsable del levantamiento de las observaciones o ejecución de las recomendaciones. Posteriormente, el auditor emite el informe final y comunica los resultados a la gerencia o quien solicitó la auditoría.

## Control

Dado que el proceso de auditoría es cíclico, luego de la emisión y comunicación de los resultados a través del informe final, la empresa debe realizar un seguimiento para el cumplimiento de las recomendaciones emitidas en dicho informe. Adicional a esto es muy importante que la Alta Gerencia de la empresa de Certificación Digital genere los canales y espacios para que se pueda continuar el desarrollo de las actividades solventando los posibles hallazgos u observaciones encontradas dentro del proceso de auditoría de sistemas; evitando así reprocesos o que resurjan nuevamente dichas observaciones con el mismo nivel de criticidad o más grande.

# Conclusiones

Para una empresa de Tecnología y para este caso particular una empresa de Certificación Digital Abierta es importante tener un control estricto de los procesos que se realicen de manera virtual o de manera digital, para que se cumpla con la normativa vigente y no se presenten fugas de información, o en el peor de los casos un hurto de información sensible, ya sea de la propia empresa o de algún suscriptor o cliente, siendo la auditoría de sistemas una herramienta o proceso útil, y versátil en la verificación de riesgos y controles que se puedan presentar dentro de una empresa, siendo muy conveniente crear un protocolo para realizar la auditoría y en el mejor de los casos crear todo un departamento para el desarrollo de la misma de manera constante y programada.

El desarrollo adecuado de la auditoría de sistemas dentro de una empresa de certificación digital abierta trae consigo múltiples beneficios tecnológicos y económicos como la detección de posibles fallas en el manejo de información sensible de los solicitantes y/o suscriptores, rastreo de puntos de fuga o no control de dicha información lo que podría acarrear sanciones o multas por entes de control gubernamental, adicional si los proceso están en regla o funcionan con calidad, esto dará un buen nombre entre las empresas de certificación digital haciendo que se destaque por su calidad conllevando a que más usuarios la elijan como opción a la hora de solicitar un certificado digital.

Contar con un departamento de Auditoría de Sistemas o el proceso establecido brinda a la empresa de certificación digital una supervisión al detalle de los procesos internos y externos referentes a la emisión y expedición de certificados digitales aumentando y manteniendo la calidad del trabajo interno por los diferentes departamentos que interfieran en la emisión de un certificado digital.

# Referencias

AMBIT, T. (9 de Febrero de 2021). *¿Qué es una auditoría de seguridad informática? Tipos y Fases*. Obtenido de Ambit BST: https://www.ambit-bst.com/blog/qu%C3%A9-es-una-auditor%C3%ADa-de-seguridad-inform%C3%A1tica-tipos-y-fases

Certicamara. (2018). *Marco Legal*. Obtenido de web.certicamara.com: https://web.certicamara.com/marco\_legal

Ciro Arenas, F. J. (Junio de 2018). *Panorama de la auditoría de sistemas en Colombia. ISACA capítulo Medellín.* Obtenido de ISACA Medellín Chapter: https://www.researchgate.net/publication/326017599\_Panorama\_de\_la\_auditoria\_de\_sistemas\_en\_Colombia\_ISACA\_capitulo\_Medellin#:~:text=La%20auditor%C3%ADa%20de%20sistemas%20de,aseguramiento%20tecnol%C3%B3gico%20con%20que%20cuentan.

GSE, G. d. (2020). *Certificados Digitales*. Obtenido de gse.com.co: https://gse.com.co/certificados-digitales/

GSE, G. d. (21 de Septiembre de 2021). *POLÍTICA DE REVOCACIÓN Y REPOSICIÓN.* Obtenido de https://gse.com.co/wp-content/uploads/2021/10/Politica\_de\_Revocacion\_y\_Reposicion.pdf

ONAC. (11 de Agosto de 2015). *CRITERIOS ESPECÍFICOS DE ACREDITACIÓN ENTIDADES DE CERTIFICACIÓN DIGITAL.* Obtenido de onac.org.co: https://onac.org.co/documentos/cea-4-1-10/

Valdes, A. A. (2019). *Firma Digital y Certificados Digitales.* Obtenido de www.academia.edu: https://www.academia.edu/38287305/Firma\_Digital\_y\_Certificados\_Digitales

València, U. P. (2020). *¿Qué es un Certificado Digital?* Obtenido de www.upv.es: https://www.upv.es/contenidos/CD/info/711545normalc.html

ZHILDEER, E. (s.f.). *Certificado digital.* Obtenido de www.academia.edu: https://www.academia.edu/38746204/Certificado\_digital