Programa del Curso

Por. Ps. Rodrigo Farías Veloso

PRESENTACIÓN

Durante largos siglos el ser humano ha confiado toda su estructura gubernamental, comercial, administrativa y jurídica en la confianza que daban los documentos físicos y unos trazos de tinta impresos en un papel.

La firma manuscrita ha sido y sigue siendo la mejor una de las mejores prendas de garantía de que alguien, vivo y consciente, estuvo presente y de acuerdo con lo que se manifestaba en el documento firmado. Y probablemente siga estando presente durante un buen tiempo más.

Sin embargo, con el avance de las tecnologías para almacenar y transmitir información, la sociedad humana ha descubierto nuevas maneras de intercambiar documentos y bienes, aumentando exponencialmente su capacidad para transmitir esta información y potenciar el intercambio comercial a velocidades y distancias antes insospechadas.

Las herramientas de la Sociedad de la Información en la que vivimos ofrecen beneficios que, si son bien aprovechados, pueden potenciar el rendimiento de cualquier proceso tradicional que todavía funcione bajo soportes físicos.

Es el caso de la firma electrónica: concepto jurídico equivalente al de la firma manuscrita en papel, donde una persona acepta el contenido de un mensaje electrónico a través de cualquier medio electrónico válido.

La aplicación de la firma electrónica está tomando impulso por sus propios méritos, y se expande hacia el mundo privado mientras los gobiernos se ponen al día en su implementación jurídica.

Los beneficios de firmar documentos electrónicamente son indiscutibles:

1. Se evitan desplazamientos y trámites burocráticos para las personas involucradas en los procesos de firma.
2. Los documentos firmados pueden archivarse en formato digital, sin tener que trasladarlos nunca al papel, con el ahorro y beneficios para el medioambiente que esto implica.
3. La distancia deja de ser un problema, por lo que cualquier documento quedará firmado por todas las partes, mucho más rápidamente, y de forma más eficiente que si se firmara a mano
4. Al quedar archivados en formato digital, su posterior localización también es mucho más fácil y rápida, gracias a las herramientas informáticas de búsqueda
5. Ahorros de costes tangibles, evitando envíos, o reduciendo el consumo de tinta o papel.
6. Es una tecnología más segura que la mera firma manuscrita, aunque la firma electrónica biométrica puede incluso incorporar los gestos gráficos de la singularidad de la antigua firma ológrafa, añadiéndole capas adicionales de seguridad tecnológica, por lo que suplantar una identidad resulta mucho más complejo.

Siendo las ventajas de la firma electrónica respecto a la firma manuscrita tan evidentes, cualquier sector que haga un uso intensivo de la firma manuscrita, público o privado, puede obtener grandes beneficios en ahorro de costes y mejora de servicio, a través de su aplicación. Es el momento de aprovechar estos beneficios e impulsar la utilización de la firma electrónica en su organización.

Este curso prepara a los participantes no sólo para comprender de qué se trata y cuáles son los beneficios de la Firma electrónica, sino además que proporcionará argumentos y competencias para liderar e impulsar el proceso de transformación digital necesario en las instituciones que decidan adoptar esta tecnología.

OBJETIVO GENERAL DEL CURSO

Al final del curso el participante podrá comprender, valorar y promover los beneficios de la firma electrónica.

METODOLOGÍA: "GAMIFICACIÓN"

Este curso online está diseñado para que sea una experiencia de auto-instrucción amena y didáctica, en el que cada avance tiene su recompensa, y contará en todo momento con la posibilidad de contactar a Grafos en caso de requerir ayuda.

El curso se compone de 11 lecciones de autoaprendizaje, estimadas en 4 horas de dedicación para cada una, entre las presentaciones, las lecturas obligatorias, la visualización de las videotutorías y la realización de los ejercicios.

Cada lección cuenta con material didáctico que el participante podrá realizar autónomamente, contando con acceso al Aula virtual de Grafos www.aulavirtualgrafos.com durante los 7 días de la semana y las 24 horas del día, mientras dure su período de acceso al aula virtual.

El participante deberá realizar el curso y las evaluaciones dentro de su período de acceso al Aula Virtual Grafos, y en caso de acabársele el tiempo, puede comprar una extensión de plazo.

Cada lección cuenta con una evaluación parcial que se puede realizar tantas veces como se desee, y le dará al alumno una retroalimentación de su grado de adquisición y manejo de los conceptos revisados.

Cada lección contiene una serie de recursos pedagógicos: Presentaciones, videos, lecturas, ejercicios y evaluaciones, que deben completarse para avanzar a la siguiente lección. El participante debe ir avanzando de niveles, aprobando las evaluaciones parciales, casi como en un juego en el que va "desbloqueando etapas", en la medida que va completando la serie de tareas y asignaciones de cada lección.

Por cada lección aprobada, el participante podrá descargar un certificado digital imprimible, que acreditará este nivel de logro, y que también podrá compartir en sus redes sociales.

Si el participante lo desea, podrá explorar sin necesidad de crear un nuevo usuario, los conocimientos de los otros cursos de que dispone el Aula Virtual del Instituto de Grafología Grafos.

PRERREQUISITOS

Este curso no tiene prerrequisitos, y está dirigido a cualquier persona que tenga interés en comprender, valorar e impulsar la utilización de la firma electrónica al interior de una empresa, en los trámites con el Estado o en el ejercicio independiente de su quehacer profesional o empresarial.

Lección Introductoria: La búsqueda de confianza y seguridad en la sociedad de la información

1. La creciente relevancia de la seguridad de la información digital
2. La contraposición de intereses en torno a la seguridad tecnológica
3. Lo "tradicional" v. lo "nuevo"
4. El modelo regulatorio uniforme global v. la recepción local
5. La seguridad de la información vs la privacidad de los datos
6. La dimensión teórica vs la aplicación práctica

Lección 1: desmaterialización documental: De la firma manuscrita a la firma electrónica.

1. Los mensajes de datos y la prueba digital
2. La evolución de la escritura
3. Concepto de desmaterialización documental
4. Alcance práctico de la desmaterialización documental
5. Cartas y comunicaciones escritas privadas y empresariales
6. Registros en bases de datos de información digital
7. Fotografías, memes y sitios web
8. Contratos y términos y condiciones por medios electrónicos
9. Perfiles de redes sociales y blogs (bitácoras de información)
10. La historia clínica electrónica
11. Certificados de existencia y representación
12. Libros electrónicos
13. Aplicaciones móviles
14. Correo electrónico
15. Los títulos valores y los valores desmaterializados
16. Circulación

Lección 2: Tipos de datos personales electrónicos

1. Qué son los Datos personales electrónicos.
2. Datos económicos
3. Datos sensibles.
4. Datos biométricos.
5. Datos de geolocalización.
6. Datos de menores de edad.
7. El mensaje de datos como documento sin soporte material como tal
8. El mensaje de datos como documento privado y público
9. Legalidad de la prueba electrónica
10. Valoración probatoria de los mensajes de datos
11. La prueba pericial y el documento electrónico
12. La autoría y autenticidad de mensaje de datos

Lección 3: La protección de los datos personales electrónicos

1. Principios de la seguridad documental:
    a. Confidencialidad.
    b. Integridad.
    c. Disponibilidad.
    d. No repudio

2. Principios que orientan la protección de datos personales de terceros:
    a. Licitud.
    b. Finalidad.
    c. Calidad.
    d. Seguridad.
    e. Transparencia

3. Derechos sobre los datos personales:
    a. Rectificación.
    b. Cancelación.
    c. Oposición.
    d. Portabilidad.
    e. Acceso.

Lección 4: La identidad digital:

- Definición de identidad digital
- Características de la identidad digital.
- Funcionamiento de la firma digital
- Los formatos de la firma digital
- Computación en la nube: almacenamiento y procesamiento de información digital
- Mecanismos de autenticación e integridad de las comunicaciones electrónicas.

Lección 5. Evolución de la firma manuscrita a la firma electrónica

- La identificación personal y la firma
- La evolución del concepto de firma manuscrita
- El concepto funcional de firma
- El origen de la desmaterialización de la firma: la firma por medios mecánicos
- La firma electrónica y la firma digital
- Definición de la firma electrónica
- Definición de la firma digital

Lección 6. Criptografía

- Criptografía
- Aplicación de la criptografía a la protección de los datos personales y a la firma electrónica.
- Orígenes y uso de la criptografía.
- Evolución de la criptografía tradicional a la criptografía matemática de dos claves
- Criptografía de clave simétrica
- Criptografía de clave asimétrica.
- Equivalencia de la firma electrónica y la firma manuscrita.

Lección 7. Tipos de firma electrónica

- Firma electrónica simple
- Tipos de firma electrónica simple
- Firma electrónica avanzada.
- Tipos de firma electrónica avanzada
- Legislación internacional y chilena respecto de la firma electrónica.

Lección 8: Certificados digitales y entidades de certificación digital

- El concepto de tercero de confianza
- Definición de certificado digital.
- Solicitud de certificados digitales
- Definición Contenido de los certificados digitales
- Clases de certificados digitales
- La revocación de certificados digitales.
- Instalación del certificado digital en un dispositivo.
- Entidades de certificación en Chile
- Las fuentes de reglamentación de las entidades de certificación digital
- Condiciones para la acreditación
- Los deberes, obligaciones y forma de proceder de las entidades de certificación
- Clases de entidades de certificación digital
- Entidades de certificación cerradas
- Entidades de certificación abiertas
- Otros servicios prestados por las entidades de certificación digital
- Cesación de actividades por parte de las entidades de certificación
- Modelos de negocios exitosos de aplicación de firmas digitales por las entidades de certificación.

Lección 9. Amenazas y fraudes típicos para la firma electrónica

- Robo de identidad, los fraudes y los plagios.
- Hacker
- Cracker
- Phishing.
- La Deep Web.
- Vulneración de la firma electrónica por hackers.
- Vulneración de los datos personales por parte de empresas y estados.
- Firma Electrónica simple copiada.
- Malware firmado digitalmente.
- Aumento en el Spam.
- Virus inteligentes.

Lección 10: El futuro de la protección de los datos digitales.

- Perspectiva y futuro de la regulación de las firmas electrónicas y digitales.
- El futuro del documento electrónico: seis propuestas para el siglo XXI.
- Inteligencia Artificial.
- Criptomonedas.
- Blockchain.
- Computación cuántica: Beneficios y amenazas.