CONVOCATORIA PARA EMPRESAS QUE SE ENCUENTREN INTERESADAS EN SER BENEFICIARIAS DE LA ESTRATEGIA HABILIDADES DIGITALES "CIBERSEGURIDAD"

1. PRESENTACIÓN

El Ciberespacio es considerado como un nuevo campo de batalla para el que todos los países, incluyendo Colombia, deben capacitarse para defenderse de posibles ataques cibernéticos.

A medida que la pandemia evoluciona, cada vez son más las organizaciones que necesitan ajustar sus procesos para poder ejecutar la mayor parte de sus operaciones de manera virtual. En respuesta a este cambio, los controles de seguridad de la información relacionados también deben ajustarse y las configuraciones de seguridad correspondientes tendrán que actualizarse.

Durante la pandemia, por mencionar un ejemplo, se registra un acceso remoto masivo de colaboradores, para lo cual, las organizaciones necesitan contar con una mayor capacidad de procesamiento y conectividad. También, requieren abrir o expandir más "interfaces" para acceder a los servicios internos, y habilitar derechos de acceso a datos, a través de una red pública (Internet) [1].

Los ciberataques se han dirigido contra altos dirigentes de la Organización Mundial de la Salud (OMS) haciendo públicas sus contraseñas y direcciones de cuentas –aunque es posible que se hayan obtenido anteriormente– o intentando suplantar su identidad. También contra los sistemas y equipos de la OMS implicados en la gestión de la crisis desplegados en algunos Estados, según informaron a la organización las autoridades de ciberseguridad de varios países de la UE, Israel, Suiza, empresas como Microsoft u organizaciones intergubernamentales como la Interpol. [2]

La ciberseguridad es crítica para nuestra prosperidad y seguridad. Las actividades cibernéticas maliciosas no sólo amenazan las economías, sino también el funcionamiento mismo del Estado de derecho. Nuestra seguridad depende de mejorar nuestra capacidad para protegernos contra las amenazas cibernéticas: Tanto la infraestructura civil como la capacidad militar depende de sistemas digitales seguros. [3]

Colombia ha empezado a plantear una visión rectora consolidada en el documento CONPES 3701, el cual busca generar los lineamientos nacionales de política en Ciberseguridad orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país. En este marco de referencia se define la Ciberseguridad como la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética. [4]

Teniendo en cuenta esto, el Ministerio de Tecnologías de la Información y las Comunicaciones a través de la Subdirección para las Competencias Digitales, diseñó una estrategia que busca la formación en habilidades digitales que promueva el desarrollo de nuevos modelos, métodos y programas de capacitación y formación para los empleados de las empresas del país, con el fin de cerrar la brecha tecnológica y que ayude a mejorar el desarrollo y productividad de Colombia reforzando su capacidad de hacerle frente a las amenazas delictivas en el ámbito digital.

[1] Deloitte- Disponible en : https://www2.deloitte.com/content/dam/Deloitte/uy/Documents/risk/Consideraciones-ciberseguridad-ante-pandemia-global.pdf
[2] Bloomberg- Disponible en : https://www.bloomberg.com/amp/news/articles/2020-04-21/top-officials-at-world-health-organization-targeted-for-hacks
[3] Bid Reporte de Ciberseguridad 2020- Disponible en: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf
[4] MinTIC 2020- Disponible en: https://www.MinTIC.gov.co/portal/inicio/Micrositios/I+D+I/Nodos/6120:Ciberseguridad

En el marco del Contrato de Administración de Proyectos de Ciencia, Tecnología e Innovación No. 669 de 2021, en especial la línea de Competencias Digitales del MinTIC y la Fundación Tecnalia Colombia, realizan la presente convocatoria para impulsar el: **FOMENTO AL DESARROLLO DE HABILIDADES EN TALENTO DIGITAL.**

2. OBJETIVOS

2.1 GENERAL

Seleccionar personas naturales con establecimiento de comercio y personas jurídicas (empresas), de todos los sectores productivos de la economía, de carácter privado constituidas legalmente en Colombia y empresas extranjeras que tengan sucursal en Colombia y que su personal colombiano (empleados, gerentes y/o directivos) requiera formación especializada en "Ciberseguridad" con el fin de contribuir al mejoramiento de la economía del país.

2.2 ESPECÍFICOS

a) Conformar un banco de empresas elegibles que cuenten con la necesidad de formar a sus **empleados**, **gerentes y/o directivos** en Ciberseguridad.
b) Ofrecer dos (2) diplomados para la formación en habilidades especializadas (I. Diplomado en ciberseguridad para directivos o gerentes. II. Diplomado en ciberseguridad para personal técnico).
c) Facilitar a las empresas seleccionadas acompañamiento en el proceso de formación del Talento Humano en Ciberseguridad.

3. DIRIGIDO A:

Personas naturales con establecimiento de comercio y personas jurídicas (empresas) de todos los sectores productivos de la economía del sector privado con interés en mejorar su productividad mediante la formación de su Talento Humano colombiano en" Ciberseguridad" y que cuenten con las siguientes características: **a)** Empresa constituida legalmente en Colombia. **b)** Empresas extranjeras con sucursal en Colombia. **c)** Que no se encuentre en proceso de liquidación o concordato.

4. COBERTURA GEOGRÁFICA

Esta convocatoria tendrá alcance a nivel nacional.

5. PROPUESTA DE VALOR

Las empresas beneficiarias recibirán:

- La convocatoria financiará el cien por ciento (100%) de los diplomados.
- 120 horas de formación en Ciberseguridad.
- Certificación de participación emitido por la Fundación Universidad del Norte y MinTIC, siempre y cuando los participantes hayan cumplido mínimo el 80% de asistencia y hayan realizado las actividades presentadas en las modalidades sincrónicas y asincrónicas para recibir el certificado.

- Debido a la emergencia sanitaria de la Covid-19, la transferencia de conocimientos será en modalidad virtual con actividades sincrónicas y asincrónicas, por ello los beneficiarios pueden estar ubicados en cualquier región de Colombia.

6. CONTENIDO DE LA FORMACIÓN

Los diplomados serán dictados por la Fundación Universidad del Norte y los beneficiarios o postulados solo podrán optar a uno de los 2 diplomados propuestos con el fin de garantizar la equidad y participación.

Las Empresas podrán inscribir sus empleados, gerentes y directivos a alguno de los siguientes diplomados:

<table>
<tr><th colspan="2">DIPLOMADO EN CIBERSEGURIDAD PARA PERSONAL NO TÉCNICO
(no necesita conocimientos previos en ciberseguridad) – 120 horas</th></tr>
<tr><td><u>Módulo 1: Seguridad y Gestión de Riesgos</u>
Intensidad: 40 horas
Porcentaje sincrónico: 60%
Duración sesiones sincrónicas: 3 horas/sesión
Cantidad de sesiones sincrónicas: 8</td><td><u>Módulo 2: Gestión de la seguridad</u>
Intensidad: 40 horas
Porcentaje sincrónico: 60%
Duración sesiones sincrónicas: 3 horas/sesión
Cantidad de sesiones sincrónicas: 8</td></tr>
<tr><td>Contenido:
1. Conceptos básicos de la gestión del riesgo
2. Identificación de riesgos de Sistemas de Información (SI):
➢ Métodos para identificar el riesgo
➢ Cultura de riesgos y comunicación
➢ Capacidad de riesgo, apetito de riesgo y tolerancia al riesgo.
➢ Concientización del riesgo
➢ Buenas prácticas en la administración de riesgos

3. Evaluación de riesgos de SI:
➢ Identificación de riesgos vs. Evaluación de riesgos
➢ Técnicas de evaluación de riesgos
➢ Análisis de riesgo y controles
➢ Metodologías para el análisis de riesgos

4. Mitigación y respuesta a riesgos de SI:
➢ Alineando la respuesta al riesgo con los objetivos de negocio
➢ Vulnerabilidades asociadas con nuevos controles
➢ Desarrollo de un plan de acción
➢ Implementación y diseño de controles
➢ Monitoreo de controles y su efectividad</td><td>Contenido:
1. Gestión de activos:
➢ Información y clasificación de activos
➢ Concepto de Propiedad (por ejemplo, propietarios de datos, propietarios de sistemas)
➢ Concepto de Privacidad
➢ Privacidad de los datos
➢ Políticas de privacidad
➢ Control de inferencia
➢ Controles de seguridad de datos
➢ Controles de acceso
➢ Requisitos de manipulación (por ejemplo, marcas, etiquetas, almacenamiento)

2. Gestión de identidad y acceso:
➢ Control de activos físicos y lógicos
➢ Identificación, autenticación y autorización de personas y dispositivos
➢ Identidad como servicio (por ejemplo, identidad en la nube)
➢ Servicios de identidad de terceros (por ejemplo, en las instalaciones)
➢ Controles de acceso multinivel
➢ Ataques de control de acceso
➢ Ciclo de vida de aprovisionamiento de identidad y acceso (por ejemplo, revisión de aprovisionamiento.</td></tr>
</table>

➢ Documentación de procedimientos de gestión de riesgos. ➢ Respuesta al riesgo y plan de acción **5. Monitoreo y reporte de riesgos y controles de SI:** ➢ Indicadores clave de riesgos ➢ Indicadores clave de desempeño ➢ Técnicas y herramientas para la extracción y recolección de datos ➢ Resultados de evaluación de controles	
<u>Módulo 3: Operaciones de seguridad</u> **Intensidad: 40 horas** **Porcentaje sincrónico: 60%** **Duración sesiones sincrónicas: 3 horas/sesión** **Cantidad de sesiones sincrónicas: 8** **Contenido:** **1. Estándares de gestión de incidentes de seguridad de la información** **2. Esquema de incidentes de seguridad de la información** **3. Identificación de eventos de seguridad de la información** **4. Planificación de la gestión de incidentes de seguridad de la información:** ➢ Planificación y ejercicios de continuidad del negocio **5. Detección y reportes de incidentes de seguridad de la información:** ➢ Gestión de parches y vulnerabilidades ➢ Procesos de gestión de cambios **6. 6. Evaluación y categorización del evento de seguridad de la información** **7. Flujo de actividades claves de la respuesta de incidentes** **8. Gestión de aprendizaje de incidentes de seguridad de la información** **9. Estrategias de Continuidad:** ➢ Business Continuity ➢ Estrategias de recuperación ➢ Procesos y planes de recuperación ante desastres	

DIPLOMADO EN CIBERSEGURIDAD PARA PERSONAL TÉCNICO
(necesita conocimientos previos en ciberseguridad) **– 120 horas**

Módulo 1: Ingeniería de Seguridad
Intensidad: 30 horas
Porcentaje sincrónico: 60%
Duración sesiones sincrónicas: 3 horas/sesión
Cantidad de sesiones sincrónicas: 6

Contenido:

1. Conceptos y definiciones relativos a seguridad de la información:
- Conciencia de inseguridad
- Ciberamenazas, Ciber conflictos, Cibercrimen, Ciberterrorismo y Ciberguerra
- Procesos de ingeniería que utilizan principios de diseño seguro
- Conceptos fundamentales de los modelos de seguridad
- Modelos de evaluación de seguridad

2. Metodologías y sistemas de control de acceso:
- Identificación, autenticación y autorización
- Gestión de identidades
- Modelos de control de acceso
- Tecnologías y técnicas de control de acceso

3. Amenazas y Vulnerabilidades:
- Definiciones
- Tipos de programas maligno y otras amenazas cibernéticas
- Vulnerabilidades de los sistemas basados en la web
- Vulnerabilidades de los sistemas móviles
- Amenazas emergentes

4. Criptografía:
- Criptografía simétrica
- Cifrado simétrico por bloques (e.g. AES)
- Cifrado Simétrico de flujo (e.g. Salsa y Chacha)
- Criptografía asimétrica
- Criptosistema RSA
- Firma digital
- RSA

5. Seguridad física

Módulo 2: Seguridad de la red y las comunicaciones
Intensidad: 30 horas
Porcentaje sincrónico: 60%
Duración sesiones sincrónicas: 3 horas/sesión
Cantidad de sesiones sincrónicas: 6

Contenido:

1. Diseño de arquitectura de red segura:
- Segmentación de redes.
- Redes privadas.

2. Componentes de red seguros:
- Proxies
- Firewalls: Primera, segunda y tercera generación
- Intrusion Detection Systems (IDS) e Intrusion Prevention Systems (IPS)
- Host-Based IPS
- Honeypots
- Firewall UTM.
- Next-Generation Firewalls.

3. Protocolos de comunicación seguros:
- IPsec
- SSH
- VPNs
- SSL/TLS
- Tor
- Certification Authorities and Public Key Infrastructure

4. Ataques de red:
- Ataques en protocolos de capa aplicación
- DNS Spoofing, DNS Poisoning, DNS tunneling
- Active Directory Exploitation
- Ataques a Remote Desktop Protocol (RDP)
- Ataques en protocolos de capa sesión
- Ataques a protocolo TLS
- Contra algoritmos Criptográficos.
- Uso de criptografía en Cipher suites.
- Funcionalidad.
- Ataques y otros usos del protocolo SSH
- SSH Hijacking, SSH Tunneling
- Ataques en protocolos de capa transporte
- Ataque de inundación Syn

6. Dispositivos integrados y vulnerabilidades de los sistemas ciber físicos: ➢ Ataques del canal lateral ➢ Dispositivos resistentes a manipulación	➢ TCP Hijacking ➢ Ataques de inundación UDP ➢ Ataques en protocolos de red ➢ IP Spoofing ➢ IP fragmentation attacks ➢ Ataques en redes Lan alámbricas e inalámbricas: ➢ DHCP Rogue, ARP spoofing, Mac Flooding. ➢ Password cracking WPA/WPA2
Módulo 3: Seguridad del Desarrollo de Software **Intensidad: 30 horas** **Porcentaje sincrónico: 60%** **Duración sesiones sincrónicas: 3 horas/sesión** **Cantidad de sesiones sincrónicas: 6** **Contenido:** **1. Desarrollo Seguro de Sistemas:** ➢ Gestión de Riesgos ➢ Metodologías en ingeniería de seguridad ➢ Análisis de riesgos ➢ Modelamiento de amenazas ➢ Seguridad por diseño **2. Metodologías para diseño de software Seguro:** ➢ Diseño Top-Down ➢ Diseño iterativo ➢ Ciclo de vida de desarrollo seguro ➢ Software como servicio ➢ DevOps y DevSecOps **3. Ciclo de las vulnerabilidades:** ➢ Mercado de vulnerabilidades ➢ Sistema CVE (Common Vulnerabilities and Exposures) ➢ Vulnerability disclosure ➢ Gestión de incidentes **4. Gestión del equipo de trabajo** **5. Seguridad en la Web:** ➢ Evaluación de las 10 vulnerabilidades más populares según OWASP. Ejemplos ➢ SQL Injection ➢ Broken Authentication	**Módulo 4: Evaluación y pruebas de seguridad** **Intensidad: 30 horas** **Porcentaje sincrónico: 60%** **Duración sesiones sincrónicas: 3 horas/sesión** **Cantidad de sesiones sincrónicas: 6** **Contenido:** **1. Pruebas de seguridad:** ➢ Pruebas de penetración ➢ Tipos de pruebas de penetración ➢ Metodologías para pruebas de penetración **2. Diseño de una prueba de penetración:** ➢ Recolección de información y enumeración de servicios ➢ Penetración y Escalamiento de privilegios ➢ Mantenimiento del acceso **3. Recolección de información y Enumeración de servicios. (KALI):** ➢ Recolección de información pasiva: Google Hacking, Shodan, Maltego. ➢ Enumeración DNS, SMTP, SNMP ➢ Escaneo vulnerabilidades **4. Penetración:** ➢ Fuzzing ➢ Buffer Overflows e inyección de código. ➢ Ataques del lado del cliente: Usando aplicaciones HTML y Microsoft Office ➢ Exploits públicos. ➢ Metasploit Framework **5. Escalamiento de privilegios:** ➢ Ejemplos de escalamiento de privilegios en Windows

➢ Cross-Site Scripting (XSS) ➢ Insecure Deserialization. **6. Análisis de programas:** ➢ Revisión de código ➢ Análisis estático ➢ Análisis dinámico ➢ Ingeniería inversa.	➢ Ataques de diccionarios **6. Mantenimiento del acceso:** ➢ Port forwarding ➢ DNS, HTTP y SSH tunneling ➢ Movimiento lateral con RDP ➢ Movimiento lateral con SSH

a. METODOLOGÍA PARA APLICAR EN LAS SESIONES SINCRÓNICAS

El enfoque será netamente teórico-práctico. Se privilegiará las estrategias de aprendizaje activo y las estrategias usadas estarán enmarcadas en la metodología del aprendizaje en línea (Aprendizaje Colaborativo, Aprendizaje basado en retos y en casos). Ahora bien, desde la interacción entre alumnos y docente se fortalecerá la colaboración, modelado y apropiación de las TIC, donde es importante el acompañamiento no solo sincrónico, sino también garantizando estrategias para la autorregulación del trabajo asincrónico, logrando consigo el andamiaje de consejos, conceptos, estrategias y aplicabilidad de las prácticas eficaces de Ciberseguridad. Cabe mencionar que, desde esta perspectiva, el estudiante tendrá un rol que cumplir: Antes, durante y después de la sesión sincrónica.

b. MEDIACIÓN ASINCRÓNICA

La presentación de contenidos educativos por medio de entornos multimodales (presentaciones digitales, videos instruccionales, entre otros) y videoconferencias contará con elementos que favorezcan una fácil comprensión por parte de la audiencia a la que está dirigido el material (Atkinson y Mayer, 2004), quienes proponen cinco principios: Señalización, Segmentación, Modalidad, Multimedia, y Coherencia.

El desarrollo de este DIPLOMADO se realizará a través de una plataforma virtual LMS, con características planteadas de aprendizaje autónomo para los momentos asincrónicos, y todas las actividades se alinearán al cumplimiento de los resultados de aprendizaje.

Los diplomados incluirán vídeo-lecciones, instrucciones guía, y materiales de estudio en distintos formatos (HTML, Genially, PDF, etc), así como también ejercicios modelados, ejemplos y todo tipo recursos relacionados a Ciberseguridad.

c. MATERIALES DE APRENDIZAJE

Evaluación:
Para el desarrollo y evaluación de los cursos de formación, se contemplarán los siguientes principios y las mismas metodologías de formación:

a. **Igualdad:** los cursos se desarrollarán en contextos de igualdad, es decir, los participantes se regirán por los mismos deberes, derechos y oportunidades.
b. **Coherencia:** Se conservará la misma metodología de evaluación para las pruebas parciales como para la evaluación final.
c. **Reserva de la prueba:** Se implementarán los mecanismos necesarios para salvaguardar la confidencialidad de la información y la protección de datos.

d. **Práctico:** Retos adaptativos a las demandas laborales y situacionales que conlleva la aplicación de la formación.

Criterios de evaluación:
Para esta formación virtual, se tendrán en cuenta dos factores o tipos de evaluación:

Formativa: Entendiendo como evaluación formativa, toda participación, trabajo independiente en foros y consulta de material. Cabe apreciar que, el estudiante deberá asistir en un 80% a las clases sincrónicas para la aprobación del curso.

Evaluación sumativa y académica: toda actividad o ejercicio de simulación, actividad con evidencias, solución de casos (Actividades académicas) deberán cumplirse en un 100%.
La evaluación integral del curso tendrá los siguientes criterios:
- Pertinencia en los resultados de aprendizaje y contexto del estudiante.
- Factores situacionales y de experiencias en el aprendizaje.
- Retroalimentación y evaluación formativa.

7. REQUISITOS MÍNIMOS HABILITANTES PARA EMPRESAS INTERESADAS EN HABILIDADES DIGITALES

Las empresas interesadas en participar en esta convocatoria deberán cumplir con los siguientes requisitos:

- Requisitos Jurídicos.

N.	REQUISITO	DOCUMENTACIÓN REQUERIDA
7.1	Empresas legalmente constituidas en Colombia.	Certificado de Existencia y Representación Legal expedido por la entidad o autoridad competente, cuya vigencia no supere los treinta (30) días calendario, con respecto a la fecha de cierre de la convocatoria. La matrícula mercantil deberá estar renovada dentro del último año.
7.2	Personas jurídicas extranjeras con sucursal en Colombia.	Las personas jurídicas extranjeras deberán demostrar que tienen domicilio en Colombia a través de sucursal, para lo cual deberán aportar certificado existencia y representación legal expedido por la Cámara de Comercio de la ciudad respectiva en la República de Colombia, en la cual se compruebe su existencia y representación legal, cuya fecha de expedición deberá ser dentro de los 30 días calendario anteriores a la fecha de cierre de la convocatoria. En dicho documento deberá constar quién ejerce la representación legal y las facultades del mismo, se deberá acreditar su duración la cual no será inferior a la vigencia del convenio (plazo de ejecución y liquidación) y un (1) año más.
7.3	Empresa que no se encuentren en proceso de Liquidación o concordato	Certificación del Representante Legal en el que conste que no se encuentra incursa en un proceso liquidatario o concordato, de igual forma en la misma comunicación se realizará manifestación bajo la gravedad de juramento de no estar en una causal de inhabilidad o incompatibilidad.
7.4	Identificación Tributaria	Todos los participantes deberán adjuntar su identificación tributaria, allegando para tal efecto, copia del Registro Único Tributario – RUT, debidamente actualizado.

N.	REQUISITO	DOCUMENTACIÓN REQUERIDA
7.5	Certificado de pagos al sistema de seguridad social y aportes parafiscales	Certificación en la cual acredite el pago de los aportes al sistema de seguridad social realizados durante los seis (6) meses anteriores a la fecha de cierre de la convocatoria, a los sistemas de salud, pensiones, riesgos laborales, cajas de compensación familiar, ICBF y SENA de conformidad con lo establecido en el artículo 50 de la Ley 789 de 2002 y la Ley 1607 de 2012. Dicha certificación debe estar suscrita por el revisor fiscal si la empresa de acuerdo con la ley lo requiere, o en caso contrario, la certificación debe estar suscrita por el representante legal de la misma. **NOTA 1:** Este requisito aplica para todas las empresas así sea presentada por intermedio de clúster o cámara de comercio en tal caso deberá aportar la respectiva certificación. **NOTA 2:** No se deben adjuntar planillas de pago sino la certificación de que trata la Ley.
7.6	Documento de identificación del representante legal	Fotocopia de la cédula de ciudadanía o documento de la identificación del representante legal de la empresa por ambas caras.
7.7	Antecedentes disciplinarios del interesado y su representante legal	Deberá aportar la consulta o certificación de si la entidad interesada individual y su representante legal, registran sanciones y/o inhabilidades de tipo disciplinario en la página de Procuraduría General de la Nación. De encontrarse reportado será causal de RECHAZO de la postulación. En todo caso será consultado por la entidad.
7.8	Antecedentes fiscales del interesado y su representante legal	Deberá aportar la consulta o certificación que la entidad interesada y su representante legal no aparezcan reportados en el boletín de responsables fiscales CGR, ingresando para el efecto a la página www.contraloriagen.gov.comódulo de responsabilidad fiscal/temas relacionados/boletín de responsables fiscales. De encontrarse reportado será causal de RECHAZO de la postulación. En todo caso será consultado por la entidad.
7.9	Registro Nacional de Medidas Correctivas	Deberá aportar el certificado de consulta del representante legal de la empresa, a fin de constatar que no registre anotaciones de medidas correctivas, por lo cual se deberá allegar fotocopia legible de la cédula. En caso de que hayan transcurrido seis (6) meses desde la imposición de la multa y esta no haya sido pagada con sus debidos intereses, será causal de RECHAZO de la postulación. En todo caso será consultado por la entidad.
7.10	Antecedentes judiciales	Deberá aportar la consulta o certificación de si el representante legal, registran sanciones y/o inhabilidades de tipo judicial en la página de Policía Nacional. De encontrarse reportado será causal de RECHAZO de la postulación. En todo caso será consultado por la entidad.

CLÚSTER Y CÁMARAS DE COMERCIO

La convocatoria está dirigida a establecimientos de comercio y empresas, por lo cual, en caso de presentarse bajo la representación de clúster o cámara de comercio, estos solo podrán realizar la postulación de las empresas y cargar la información respectiva, toda vez que no se suscribirá convenio o contrato para la ejecución de la formación, ya que la

capacitación se pagará de manera directa a la institución de educación superior que adelantará la formación.

Adicional a la información anterior deberán considerarse que la figura asociativa de clúster o la cámaras de comercio se desarrolla bajo la representación de otras empresas por lo cual deberá acreditar:

N.	REQUISITO	DOCUMENTACIÓN REQUERIDA
7.11	Asociación o afiliación de las empresas que lo conforman.	El clúster o cámara de comercio deberá aportar el acta o documento de afiliación o autorización con la que cuenta para representar a la empresa que postula bajo su asociación.

8. REQUISITOS FINANCIEROS

N.	REQUISITO	DOCUMENTACIÓN REQUERIDA
8.1	La empresa interesada deberá demostrar un índice de liquidez mayor o igual a 1.0, un capital de trabajo igual o mayor a $5.000.000 y un índice de endeudamiento inferior o igual al 70%, índices calculados de acuerdo con las siguientes fórmulas: a) **Índice de liquidez** Se determina la liquidez, medida como activo corriente sobre pasivo corriente reflejado en el balance general con corte al último periodo fiscal, así: IL = Activo Corriente / Pasivo Corriente se determina así: **Donde:** AC: es igual a activo corriente de cada participante PC: es igual a pasivo corriente de cada participante b) **Capital de Trabajo** Se determina restando al activo corriente menos el pasivo corriente, así: CT = Activo Corriente - Pasivo Corriente **Donde:** AC: es igual a activo corriente de cada participante PC: es igual a pasivo corriente de cada participante **c) índice de Endeudamiento** Se obtiene el porcentaje de endeudamiento al dividir el pasivo total por el activo total que se reflejen Estados de la Situación Financiera con	La empresa podrá acreditar registro único de proponentes RUP, cuya información financiera deberá corresponder a la última anualidad y no tener una fecha de expedición mayor a 30 días calendario a la fecha de cierre de la convocatoria, o podrán aportar los Estados de la Situación Financiera de los años 2019 o en su defecto 2020 si lo tienen a la fecha, con las notas respectivas bajo la estructura de las NIIF. Se deberá adjuntar de manera obligatoria la fotocopia de la tarjeta profesional del contador y del revisor fiscal y la certificación de la junta central de contadores con vigencia menor a tres meses que estén suscribiendo los estados financieros de situación financiera. Notas: 1. Adjuntar los anteriores documentos en el espacio del formulario denominado Estados de la Situación Financiera. 2. Los interesados deben cumplir con los tres indicadores financieros. El incumplimiento de uno o más de ellos, será causal de RECHAZO DE LA POSTULACIÓN.

N.	REQUISITO	DOCUMENTACIÓN REQUERIDA
	corte al último periodo fiscal y el resultado se multiplica por 100: IE = (Total Deudas o Pasivo Total / Activo Total o Patrimonio Bruto) x 100 **Donde:** PT: es igual a pasivo total de cada participante AT: es igual a activo total de cada participante.	

Nota 1: Para la verificación de requisitos financieros en caso de presentación de clúster o por cámaras de comercio, se aplicarán los siguientes indicadores:

INDICADOR	FORMULA	MARGEN SOLICITADO
Rentabilidad del Patrimonio	Utilidad Operacional sobre Patrimonio	Igual o Mayor a 0.0
Rentabilidad del Activo	Utilidad Operacional sobre Activo Total	Igual o Mayor a 0.0
Capital de Trabajo (Solo ESAL con Utilidad operacional negativa)	Activo Corriente menos Pasivo Corriente	Positivo
Patrimonio (Solo ESAL con Utilidad Operacional negativa)	Activo Total menos Pasivo Total	Positivo

- **RENTABILIDAD DEL PATRIMONIO**

Se determina la Rentabilidad del Patrimonio, tomando **Utilidad Operacional sobre Patrimonio**.

RENTABILIDAD DEL PATRIMONIO = $\frac{\text{\$ UTILIDAD OPERACIONAL}}{\text{\$ PATRIMONIO}}$ = $\frac{\$}{\$}$ = $\$$ **(Indique la cifra con máximo 2 decimales)**

Una vez aplicada la formula anterior, la cifra resultante deberá ser **Igual o Mayor a (0.0) cero**.

- **RENTABILIDAD DEL ACTIVO**

Se determina la Rentabilidad del Activo, tomando **Utilidad Operacional sobre Activo Total.**

RENTABILIDAD DEL ACTIVO = $\frac{\text{\$ UTILIDAD OPERACIONAL}}{\text{\$ ACTIVO TOTAL}}$ = $\frac{\$}{\$}$ = $\$$ **(Indique la cifra con máximo 2 decimales)**

Una vez aplicada la formula anterior, la cifra resultante deberá ser **Igual o Mayor a (0.0) cero.**

Tratándose de Entidades Sin Ánimo de Lucro (ESAL), que a 31 de diciembre 2020, para todos aquellos inscritos que hayan renovado el RUP, o a corte diciembre 2019 para aquellos inscritos que no hayan renovado aún el RUP, presenten Utilidad Operacional **negativa** afectando el cálculo de los indicadores de Capacidad Organizacional con un resultado negativo, se considera que cumplen con el requisito y se habilitan dentro del proceso de verificación de requisitos habilitantes, toda vez que la ausencia de lucro es una de sus características fundamentales. En el caso de que la Entidad Sin Ánimo de Lucro (ESAL) presente Utilidad Operacional **Negativa**, deberá cumplir con un indicador adicional de Capital de Trabajo (Activo Corriente menos Pasivo Corriente), cuyo resultado debe ser positivo, con el fin de evaluar si la

empresa inscrita cuenta con los recursos que le permita llevar a cabo la ejecución de la formación y el de Patrimonio (Activo Total menos Pasivo Total), cuyo resultado debe ser positivo, con el fin de evaluar la cantidad de recursos propios en relación al proceso de formación, para asegurar la continuidad del proponente en el tiempo.

- **CAPITAL DE TRABAJO (Solo ESAL con Utilidad Operacional Negativa)**

Se determina tomar el Activo Corriente menos el Pasivo Corriente, datos obtenidos del Registro Único de Proponentes con información financiera a treinta y uno (31) de diciembre 2020, para todos aquellos inscritos que hayan renovado el RUP, o a corte diciembre 2019 para aquellos inscritos que no hayan renovado aún el RUP, y el

CAPITAL DE TRABAJO = $_____ -- $_____ = $_____

ACTIVO CORRIENTE PASIVO CORRIENTE

(Indique la cifra con máximo 2 decimales)

- **PATRIMONIO (Solo ESAL con Utilidad Operacional Negativa)**

Se determina restando al Activo Total el Pasivo Total, datos obtenidos del Registro Único de Proponentes con información financiera a treinta y uno (31) de diciembre 2020, para todos aquellos inscritos que hayan renovado el RUP, o a corte diciembre 2019 para aquellos inscritos que no hayan renovado aún el RUP, y el valor obtenido deberá ser **Positivo.**

PATRIMONIO = $_____ -- $_____ = $_____

ACTIVO TOTAL PASIVO TOTAL

(Indique la cifra con máximo 2 decimales)

9. REQUISITOS TÉCNICOS

Se requerirá aportar la siguiente documentación técnica a fin de participar en la convocatoria:

N.	REQUISITO	DOCUMENTACIÓN REQUERIDA
9.1	La empresa realizará la designación de una persona responsable del proyecto, quien estará a cargo de coordinar y dar respuesta al desarrollo de este y que tenga la capacidad de toma de decisiones frente al mismo.	Diligenciar en la solicitud de inscripción (anexo N°1), los datos de la persona designada como responsable del proyecto en la empresa adjuntando la copia del documento de identificación.
9.2	Postulación de las personas a formar	Se deben diligenciar los anexos solicitados, haciendo la salvedad que la única lista a considerar será la que se adjunte a través del link y una vez enviada no podrá ser remplazada o modificada salvo para aclarar nombres o números de cédula del personal propuesto previo requerimiento de la Entidad. **En el anexo 2, deben diligenciar los nombres de todas las personas postuladas por la organización para formarse en ciberseguridad, así mismo se debe especificar cual va a ser el programa del cual será beneficiario el empleado o**

		directivo (Diplomado para Técnicos / Diplomado para directivos)

Nota 1: El número de empleados, gerentes y/o directivos por empresas a beneficiar se dará a conocer una vez sean evaluadas las propuestas presentadas en esta convocatoria, teniendo en cuenta que los recursos destinados desde el Fondo Único de Tecnologías de la Información y las Comunicaciones – FONTIC del MinTIC son limitados.

Nota 2: Las empresas deberán suscribir los compromisos y garantías que la universidad requiera para adelantar la formación.

Para asignar los cupos, primero se evaluarán todos los aspirantes y se calculará para cada empresa el porcentaje de empleados que participan dentro del total de aspirantes habilitados, ese mismo porcentaje será el que se les asignará los cupos disponibles, así será proporcional la repartición de cupos

10. CAUSALES DE RECHAZO DE LAS POSTULACIONES

Serán causales de rechazo de las postulaciones cuando: **a)** Su objeto y/o producto digital posean contenido sexual explícito, explotación infantil o que fomenten la violencia en cualquiera de sus expresiones o géneros o promuevan el uso de sustancias psicoactivas. **b)** Que la empresa postulante se encuentre en proceso de liquidación, concordato o reestructuración. **c)** No alleguen en debida forma los documentos requeridos en esta convocatoria dentro de los términos perentorios otorgados por la entidad. **d)** Se postulen después de vencido el plazo establecido para el efecto de esta convocatoria. **e)** Cuando en el formulario de postulación de la empresa no se evidencie la finalización de la inscripción. **f)** Se encuentren incursas en alguna de las causales de inhabilidad e incompatibilidad establecidas en la Constitución o la ley. Esta misma causal es aplicable a sus representantes legales.

Nota 3: MINTIC podrá verificar en cualquier momento la información de existencia y representación legal de las empresas que se postulen. Así mismo podrá solicitar en cualquier momento, información y documentación adicional o aclaraciones de estas. En el evento de encontrarse irregularidades, inconsistencias o incongruencias en la información suministrada en la postulación, MinTIC se reserva el derecho de rechazar la postulación de la empresa y de adelantar ante las autoridades competentes las acciones a que hubiere lugar.

Nota 4: No obstante, lo anterior, los requerimientos o aclaraciones no significarán compromisos por parte de MinTIC, para la aprobación, inclusión y/o aceptación o habilitación de las postulaciones como beneficiarias en el proceso de la presente convocatoria.

11. PROCEDIMIENTO DE POSTULACIÓN

Las empresas interesadas en postularse a la presente convocatoria deberán:

a. Ingresar al enlace habilitado para la inscripción a la Convocatoria publicada en la página web http://www.talentodigital.gov.co
b. Diligenciar en su totalidad el formulario disponible, incluido el enlace a la carpeta con los anexos y soportes requeridos en un servicio de almacenamiento en la nube. Las empresas interesadas deben considerar las fechas de caducidad de dichos enlaces generados en estas plataformas para evitar inconvenientes debido a que la documentación no se encuentre disponible a la fecha de postulación.
c. Validar que toda la información suministrada corresponda a la solicitada en el formulario y los requisitos

descritos del presente documento.

d. Hacer clic en el botón "Finalizar", si la postulación no se finaliza su estado es "incompleto" y la empresa no se considera postulada.

Nota 5: La selección se realiza a través MinTIC y con su postulación, la empresa interesada autoriza que sus datos de contacto sean compartidos para la ejecución de este proyecto con la Institución de Educación Superior (Fundación Universidad del Norte) que desarrollara los diplomados.

Nota 6: Las aclaraciones y subsanaciones deben allegarse única y exclusivamente a través del correo electrónico info.talentodigital@mintic.gov.co

Nota 7: Toda modificación o alteración a la información presentada por la empresa (incluidos los anexos y soportes requeridos cargados en el enlace compartido en la plataforma de la subdirección de competencias digitales), luego de finalizar su postulación, no será tenida en cuenta ni será válida para la evaluación de la empresa.

Adicionalmente se debe tener en cuenta que:

a. La fecha de postulación de la empresa corresponderá a la fecha de la última vez que finalice su postulación en la plataforma de Talento Digital.
b. Se aceptarán únicamente las postulaciones que se presenten a través del formulario electrónico habilitado, debidamente finalizado y con toda la información y documentación solicitada en la presente convocatoria.
c. La postulación de la empresa y participación en el proceso de selección no generan obligación de MinTIC – Fondo Único de TIC, para otorgar cualquier clase de beneficio económico.
d. La información presentada por cada empresa postulada será revisada por parte de MinTIC.
e. El otorgamiento de los cupos se realizará hasta agotar el presupuesto en estricto orden cronológico (incluyendo la hora) de postulación y se asignará el cupo de beneficiarios a cada empresa.

12. PLAZO DE EJECUCIÓN

El plazo de ejecución del presente programa será de 5 meses para adelantar el proceso de formación del diplomado, los cuales se comenzarán a contar a partir del inicio de la formación del diplomado.

13. BANCO DE ELEGIBLES

a. Los resultados del proceso de selección se publicarán en la página web de Talento TI http://www.talentodigital.gov.co.
b. Las empresas evaluadas se organizarán en un listado en estricto orden de inscripción por fecha y hora.
c. En caso de que alguna de las empresas seleccionadas se retire o desista y aún haya presupuesto disponible, se procederá a elegir a la siguiente empresa en orden descendente de la lista del banco de elegibles, según inscripción y selección en caso de que así lo decida MinTIC.

Nota 8: Las empresas que sean seleccionadas para participar en este proyecto, deberán suscribir los documentos que establezca la **Institución de Educación Superior (Fundación Universidad del Norte)** que desarrollará los diplomados.

Nota 9: En caso de que la empresa seleccionada no remita los documentos exigidos por la **Institución de Educación Superior (Fundación Universidad del Norte)** que desarrollará los diplomados para el inicio de la formación del personal, en el término de cinco (5) días hábiles después de notificada su selección se entenderá que la empresa desiste tácitamente de su interés en el programa y se procederá a seleccionar a la siguiente

empresa en el orden descendente de la lista de elegibles, según el orden de registro en la plataforma.

Nota 10: Una vez publicados los resultados preliminares de las empresas habilitadas, los interesados podrán presentar solicitudes de aclaraciones y comentarios hasta las 16:00 horas de los siguientes dos (2) días hábiles a la fecha de publicación. Por fuera de este término se considera que las reclamaciones son extemporáneas y por tal razón no serán aceptadas.

Nota 11: Las peticiones y reclamaciones se deben presentar exclusivamente a través del correo electrónico info.talentodigital@mintic.gov.co con el asunto "Convocatoria Habilidades Digitales".

14. ACEPTACIÓN DE TÉRMINOS Y VERACIDAD

Con la inscripción, las empresas postuladas aceptan las características, requisitos y condiciones de la presente convocatoria, para el desarrollo de esta y para ser beneficiarios, en caso de ser seleccionados, del apoyo en la formación requerida por la empresa en Ciberseguridad. De igual forma, declaran que la información suministrada es veraz y corresponde a la realidad. En caso de encontrarse alguna incoherencia, falsedad y/o inconsistencia en la información o documentación suministrada, MinTIC, podrá en cualquier momento rechazar la postulación o si es del caso declarar la pérdida del beneficio, sin perjuicio de las acciones legales correspondientes en especial por la información suministrada para la formación.

15. CAMBIOS E INTERPRETACIÓN DE LA CONVOCATORIA

MinTIC y la línea de Competencias Digitales, podrán en cualquier momento, realizar cambios en los términos de la presente convocatoria, para lo cual se publicarán las diferentes adendas.

Es obligación de los interesados, consultar de manera constante la página web en la que se informarán dichos cambios. En todo caso los datos que se publiquen en la página web de la Entidad serán vinculantes para la convocatoria y sus participantes. Si llegare a existir contradicción entre lo publicado y los términos de esta convocatoria, tendrá prevalencia este documento.

Para el proceso de verificación y evaluación se considerarán los documentos de justificación realizados, así como los límites y datos proporcionados por el mismo.

16. CRONOGRAMA

Ítem	Fecha
Apertura de la Convocatoria	5 de mayo de 2021
Presentación de observaciones referente a la convocatoria Email: info.talentodigital@mintic.gov.co con asunto convocatoria Habilidades Digitales – Ciberseguridad	del 5 al 11 de mayo de 2021 hasta las 16:00
Respuesta consolidada a las observaciones	12 de mayo de 2021
Cierre de la convocatoria	18 de mayo del 2021 hasta las 23:59
Publicación de resultados empresas habilitadas	25 de mayo de 2021
Solicitudes de aclaración	27 de mayo de 2021

17. PROTECCIÓN DE DATOS PERSONALES

MinTIC y la **Institución de Educación Superior (Fundación Universidad del Norte) que desarrollara los diplomados** actuarán como responsables del tratamiento de los datos personales que lleguen a ser tratados en el marco de la formación, de conformidad con las políticas de privacidad establecidas en este sentido y cumplirá con todas las disposiciones previstas en la Ley 1581 de 2012 su decreto reglamentario 1377 de 2013 y demás normas que regulen la materia.

Cada empresa con la aceptación de la participación en el presente proceso, de acuerdo con lo establecido en la Ley 1581 de 2012, autoriza a MinTIC, y la **Institución de Educación Superior (Fundación Universidad del Norte) que desarrollara los diplomados** al tratamiento de datos personales.

18. FORMULARIO DE INSCRIPCIÓN

Los interesados en participar en la convocatoria deberán completar y finalizar formulario ubicado en el siguiente link y acompañado de los documentos solicitados en el mismo: https://mintic.gov.co/micrositios/convocatoria-habilidades-digitales/775/w3-channel.html