Uniempresarial
Fundación Universitaria Empresarial

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Acta No. 134 del 19 de febrero de 2021 ConsejoSuperior Universitario
Concordancia con el Acta No. 146 del 27 de enero de 2022 Consejo Superior Universitario

Uniempresarial
Fundación Universitaria Empresarial

Directivos

Presidente del Consejo Superior Universitario
Nicolás Uribe Rueda

Rector:
Carl Henrik Langebaek Rueda

Secretaria General:
Nidia Johanna Robles Villabona

Vicerrectora Académica:
Yasmín Molina Rojas

Vicerrector de Proyección Empresarial y Relacionamiento con el Entorno:
Jorge Mario Hurtado Rodríguez

Gerente de Planeación y Aseguramiento de la Calidad:
Emma Emira Carrión Rodríguez

Gerente de Talento Humano:
Luz Yazmin Lizarazo Jiménez

Gerente de Mercadeo y Admisiones:
Dorys Andrea Sotelo Carreño

Gerente Administrativo y Financiero:
Andrés Carrillo Gil

Acreditación: ACBSP GLOBAL BUSINESS ACCREDITATION

Miembro: DHLA Duale Hochschule Latinoamérica

Certificación: CERTQUA Analysieren I Zertifizieren

Política Institucional de Seguridad de la Información de la FundaciónUniversitaria Empresarial de la Cámara de Comercio de Bogotá – Uniempresarial.

1. Introducción.

La Fundación Universitaria Empresarial de la Cámara de Comercio de Bogotá - Uniempresarial (código: 2738), con domicilio en Bogotá D.C., institución de educación superior privada, de utilidad común, sin ánimo de lucro y con carácter académico deinstitución universitaria, con personería jurídica reconocida mediante resoluciónnúmero 598 de 2001-04-02, expedida por el Ministerio de Educación Nacional, desarrolla en el presente documento su Política Institucional de Seguridad de la Información.

2. Objeto.

La Política Institucional de Seguridad de la Información de Uniempresarial tiene por objeto proteger la información de amenazas, para contribuir al aseguramiento de lacontinuidad de la institución, minimizar el riesgo, reducir el impacto de incidentes de seguridad, generar oportunidades de negocio y dar cumplimiento legal, contractual yregulatorio. Además de mantener relaciones de confianza con las partes interesadasa través del cuidado en el manejo de la información que se encuentra tantoalmacenada a través de las tecnologías de información (equipos de cómputo, sistemas de información, redes (Voz y Datos), como en medios físicos y personas queinteractúan con ella.

3. Ámbito de Aplicación.

Todos los principios y disposiciones contenidas en la presente Política serán aplicables a todos los procesos, procedimientos, negocio, servicios y recursos de tecnología, lo que incluye hardware y software

de la Fundación Universitaria Empresarial de la Cámara de Comercio de Bogotá - Uniempresarial. Y su cumplimento es obligatorio por todos los miembros de Uniempresarial incluyendo, pero no limitado a los colaboradores, contratistas, proveedores, estudiantes, docentes, empresas co- formadoras y, terceros relacionados o vinculados con Uniempresarial.

4. Principios

En el desarrollo, aplicación e interpretación de la presente Política Institucional de Seguridad de la Información se aplicarán los siguientes principios:

a) Principio de Confidencialidad. Garantiza que la información será protegida para que no sea divulgada sin el debido consentimiento.
b) Principio de Integridad. Propende por la veracidad y transparencia de la información.

c) Principio de Disponibilidad. capacidad de garantizar que tanto el repositorio de la información como los datos estarán disponibles al usuario en todo momento.
d) Principio de No Repudio. Garantiza la participación de las partes en una comunicación como receptoras de la información.

5. Definiciones:

Para efectos de compresión, aplicación y de interpretación de la presente Política Institucional de Seguridad de la Información, se extraen las siguientes definiciones de la norma técnica NTC-ISO/IEC colombiana 27001 2006-03-22 para la tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).

a) **Activo:** cualquier cosa que tiene valor para la organización.

b) **Análisis de riesgo:** uso sistemático de la información para identificar las fuentes y estimar el riesgo.
c) **Confidencialidad:** propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
d) **Disponibilidad:** propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.
e) **Evaluación del riesgo:** proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.
f) **Gestión del riesgo:** actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.
g) **Incidente de seguridad de la información:** un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
h) **Integridad:** propiedad de salvaguardar la exactitud y estado completo de los activos.
i) **Seguridad de la información:** preservación de la confidencialidad, la integridad yla disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (*Accountability*), no repudio y fiabilidad.
j) **Tratamiento del riesgo:** proceso de selección e implementación de medidas paramodificar el riesgo.
k) **valoración del riesgo:** proceso global de análisis y evaluación del riesgo.

6. Información.

La información es un activo fundamental para la prestación de los servicios y la toma de decisiones eficientes de La Fundación Universitaria Empresarial de la Cámara de Comercio de Bogotá - Uniempresarial.

Uniempresarial es consciente del valor de la información,

independientemente de suforma, origen o fecha de generación, razón por la cual existe un compromiso expreso de proteger y cuidar la misma, con el fin de asegurar a sus estudiantes, egresados,

colaboradores, contratistas y proveedores, que la información se maneja en condiciones óptimas de seguridad.

7. **Elementos de la Seguridad de la Información:** Son elementos de la seguridad de lainformación:

   a) Confidencialidad
   b) Disponibilidad
   c) Integridad
   d) Preservación

8. **Gestión de Activos de Información.**

   A cada dependencia, corresponde realizar un inventario de los activos de información que poseen, para así asegurar su Confidencialidad, Disponibilidad, Integridad y Preservación. Para ello deberán:

   a) Identificarla.
   b) Valorarla.
   c) Clasificarla.
   d) Organizarla.

9. **Uso de servicios y recursos de tecnología.**

   Cualquiera que haga uso de los servicios y de los recursos de tecnología de Uniempresarial acepta explícitamente todo el contenido de la presente Política de Seguridad de la Información y por ende su cumplimiento es obligatorio.

10. **Acceso a los Servidores.**

Acceso a los sitios destinados para albergar los servidores principales y auxiliaresdeberá ser controlado y restringido.

11. Acceso a los Recursos de Tecnologías de Información.

El acceso a los recursos de tecnologías de información de Uniempresarial deberá serrestringido, por lo que los equipos, correos institucionales deben tener claves.

12. Gestión del riesgo.

La protección de la información requiere un proceso integral de gestión del riesgoque:

a) Identifique, clasifique y defina los propietarios de los activos de información deacuerdo con su sensibilidad y criticidad

b) Liste y analice las amenazas y vulnerabilidades de los activos y evalúe la probabilidad de ocurrencia e impacto en términos de la pérdida de la confidencialidad, integridad y disponibilidad de ocurrencia e impacto en términos de la pérdida de la confidencialidad, integralidad y disponibilidad, paradeterminar el nivel de riesgo existente.

c) Permita el tratamiento del riesgo (mitigar, transferir, aceptar, evitar), con el fin de llevar el riesgo a un nivel aceptable.

d) Implemente actividades de monitoreo que permitan medir la eficacia de los controles implementados para generar oportunidades de mejora.

13. Procedimiento para reporte de incidentes de seguridad.

El Comité de Seguridad de la Información establecerá y será el encargado de dar cumplimiento del procedimiento para reporte de incidentes de seguridad. Para ello deberá tener en cuenta:

a) Establecer etapas con su correspondiente responsable.
b) Señalar los términos para cada una de las etapas.
c) Categorizar los incidentes.
d) Señalar las respuestas para cada uno de los posibles incidentes.

14. Malware y accesos no autorizados.

Se deben implementar controles multinivel para proteger los sistemas informáticos, para ello El Comité de Seguridad de la Información elaborará y mantendrá, reglas con estándares y procedimientos que mitiguen los riesgos asociados a amenazas de malware y accesos no autorizados.

15. Estrategias.

Uniempresarial asignará lo recursos necesarios para implementar un gobierno de seguridad de la información alineado con los requisitos de ley, contractuales y reglamentarios, y a las necesidades de las distintas áreas de la institución. Así mismo,facilitará los medios para la educación, formación y concientización en materia de seguridad de la información.

16. Comité de Seguridad de la Información:

El Comité de Seguridad de la Información, estará integrado por el Secretario General, quien lo presidirá, el Director Administrativo y Financiero o quien haga sus veces, el Director de Planeación y Aseguramiento de la Calidad o quien haga sus veces y el Director de Tecnologías o quien haga sus veces, quien actuará como secretario. Tendrá como funciones:

a) Verificar el cumplimiento de la Política Institucional de Seguridad de la Información.

b) Asignar los roles y responsabilidades de cada uno de sus miembros.

c) Levantar actas de cada una de sus sesiones.
d) Liderar la implementación de los controles exigidos por la ley y la normatividadvigente.
e) Crear e implementar un plan estratégico de seguridad de la información todos los sistemas que soportan los procesos de Uniempresarial.
f) Asegurar que los responsables del plan estratégico de seguridad de laInformación tienen la autoridad necesaria para llevar a cabo su implementación y mejora continua.
g) Hacer la evaluación de la efectividad del plan implementado y su nivel decumplimiento anualmente.

17. Responsables.

A. **Consejo Superior Universitario:** El Consejo Superior Universitario es responsablede:

i. Aprobar los recursos requeridos para la Gestión de la Seguridad de la Información en la Uniempresarial.
ii. Velar por las respectivas actualizaciones de esta política, los procesos, procedimientos, instructivos y formatos específicos. Uniempresarial se reserva el derecho a modificar el presente documento sin previo aviso y a su entera discreción.
iii. Aprobar la Política Institucional de Seguridad de la Información de Uniempresarial.

B. **Rector:** El Rector es responsable de:

i. Supervisar el cumplimiento de la Política Institucional de Seguridad de laInformación de Uniempresarial.

C. **Jefes de las dependencias:** Los jefes de las dependencias son responsables de aplicar y seguir todos los lineamientos de gestión contenidos en la política.

D. Colaboradores de Uniempresarial: Todos los colaboradores de Uniempresarial serán responsables del manejo de la información, el cumplimiento de las políticasy de los controles implementados por la institución, así como reportar los incidentes de seguridad e implementar acciones correctivas o preventivas a que haya lugar según sus competencias, para asegurar un proceso permanente de mejora en la gestión de la seguridad de la información.

E. Estudiantes: Todos los estudiantes tienen el deber de acatar la presente políticacuando haga uso de los recursos de tecnología de la información de Uniempresarial

F. Usuarios: Los usuarios son responsables proteger y garantizar el debido tratamiento de la información propia o de terceros. Además de propender por evitar accesos no autorizados, sustracción, pérdida, modificación y uso indebido de la información de Uniempresarial.

18. Vigencia

La presente Política Institucional de Seguridad de la Información de Uniempresarialentrarán en vigencia a partir del 19 de febrero de 2021.