



PROGRAMA DE FORMACION GREMIAL EN CIBERSEGURIDAD

La Ciberseguridad o Seguridad de la Información, se ha convertido en un tema estratégico en todas las organizaciones que cuentan con datos o información crítica para su operación. El Foro Económico Mundial ha señalado que los ciberataques son parte del Top 10 de los riesgos a nivel mundial y, este riesgo estará presente en los próximos años por el avance tecnológico que hemos alcanzado. La Ciberseguridad, en este sentido, es una tarea de todos.



La Comisión de Ciberseguridad y la ABM, trabajamos de manera conjunta en la implementación de un Programa de Formación Gremial en Ciberseguridad para toda la Banca, el cual en una primera etapa constará de los siguientes cursos.

Objetivo General:



Desarrollar las habilidades y competencias de ciberseguridad que permitan establecer un estándar de conocimientos para el desarrollo de las funciones principalmente de las áreas de ciberseguridad, asegurando la gestión efectiva de riesgos de tecnologías de la información y asegurando el cumplimiento de los requerimientos regulatorios.

1. CURSO ALTA DIRECCIÓN 1.1

Dirigido a los Directivos y Consejeros de las instituciones financieras para coadyuvar en la toma de decisiones en la prevención sobre los riesgos en seguridad de la información. Trata sobre el significado de seguridad de la información, las formas en que se ve comprometida y cuáles son las funciones principales de un gobierno de seguridad.

Temas que abarca



I. Seguridad Información (SI):

- Gobierno de la SI.
- Enfoque estratégico de la SI.
- Enfoque táctico de la SI.

II. Roles de la SI.

- Entorno laboral de la SI.

**Duración
aproximada:
30 minutos.**

**Modalidad:
100% online
(e-learning).**

Contacto

Luis Antonio Ramírez Mendoza
Tel. 55 5722-4397
lramirez@abm.org.mx

Ana Lilia Ortega Angeles
Tel. 55 5722-4388
aortega@abm.org.mx



PROGRAMA DE FORMACION GREMIAL EN CIBERSEGURIDAD

2. CURSO BÁSICO 3.0

Dirigido a todos los colaboradores bancarios, clientes de los bancos y público en general, para hacer conciencia sobre los riesgos digitales y el cuidado de su información, así como de la información.

Temas que abarca



**Duración
aproximada:
6 horas.**

**Modalidad:
100% online
(e-learning).**

FASE 1

1. Seguridad de la información y ciberseguridad
2. Certificaciones y compliance

FASE 3

1. Política de seguridad
2. Gestión de riesgos
3. Control de acceso
4. Seguridad en las operaciones
5. Navegación segura
6. Seguridad en el correo electrónico
7. Seguridad en la nube

FASE 2

1. Estadísticas relacionadas a la seguridad informática
2. Hackers y crackers
3. Ingeniería social
4. Softwares maliciosos

FASE 4

1. Seguridad en redes inalámbricas
2. Seguridad en aplicaciones web
3. Seguridad en dispositivos móviles y telefonía
4. Amenazas y recomendaciones
5. Compras seguras y banca en línea
6. Uso de cajeros automáticos (ATM's)
7. Pagos usando CoDi
8. Seguridad en IOT (Internet de las cosas)

3. CURSO DE REFORZAMIENTO 2.0

Dirigido a todos los colaboradores bancarios que, el año previo, hayan tomado la versión completa o adaptativa del Curso Básico.

Temas que abarca



**Duración
aproximada:
2 horas.**

**Modalidad:
100% online
(e-learning).**

FASE 1

1. Seguridad de la información y ciberseguridad
2. Cumplimiento/compliance

FASE 3

1. Política de seguridad
2. Gestión de riesgos, amenazas y vulnerabilidades
3. Seguridad en las operaciones
4. Navegación segura

FASE 2

1. Incidentes cibernéticos
2. Hackers y crackers
3. Ingeniería social
4. Softwares maliciosos

FASE 4

1. Seguridad en redes inalámbricas
2. Seguridad en aplicaciones web
3. Seguridad en dispositivos móviles y telefonía
4. Amenazas y recomendaciones
5. Compras seguras y banca en línea
6. Uso de cajeros automáticos (ATM's)
7. Pagos usando CoDi
8. Seguridad en IOT

Contacto

Luis Antonio Ramírez Mendoza
Tel. 55 5722-4397
lramirez@abm.org.mx

Ana Lilia Ortega Angeles
Tel. 55 5722-4388
aortega@abm.org.mx



PROGRAMA DE FORMACION GREMIAL EN CIBERSEGURIDAD

A continuación, se indican las actualizaciones que se aplicaron a las versiones de los cursos Básico 3.0 y Reforzamiento 2.0:



- Cambios en la normativa de Indeval, SPEI y Swift, entre otros.
- Incidentes cibernéticos suscitados en 2021 y algunos de 2022.
- Se incluyen algunos ejemplos de las contraseñas más utilizadas por los atacantes, cuáles son las más seguras y un ejemplo de cómo integrar una contraseña segura.
- Nuevas Amenazas y Recomendaciones (Fintech, Open banking, otras derivadas del aspecto geopolítico actual, entre otros).



NUEVA MODALIDAD ADAPTATIVA

Al inicio del Curso Básico, tendrás la oportunidad de presentar una evaluación diagnóstica que te permitirá exentar los temas que ya conozcas, para que solo tomes aquellos que necesites reforzar, lo cual redundará en un menor tiempo de navegación y una mejor experiencia.



PORTAFOLIO DE SERVICIOS

- Curso con ejemplos prácticos, aplicaciones por módulo y evaluación final.
- Emisión y administración de constancias electrónicas de acreditación de los participantes.
- Gestión administrativa: registro de participantes, notificación de usuario y contraseña, seguimiento de avances y resultados por participante, reportes, etc.
- Asesoría y seguimiento a través del Centro de Atención a Usuarios (CAU) de lunes a viernes de 9:00 a 18:00 horas.
- Minería de información.



La Circular Única de Bancos (CUB) establece en los artículos 168 Bis 12 y 168 Bis 14 que se deben implementar Programas Anuales de Capacitación para concientizar en materia de seguridad de la información a todo el personal y clientes incluyendo, en su caso, a terceros que le presten servicios. Esta obligación entró en vigor desde el pasado 27 de noviembre de 2019.

Contacto

Luis Antonio Ramírez Mendoza
Tel. 55 5722-4397
lramirez@abm.org.mx

Ana Lilia Ortega Angeles
Tel. 55 5722-4388
aortega@abm.org.mx