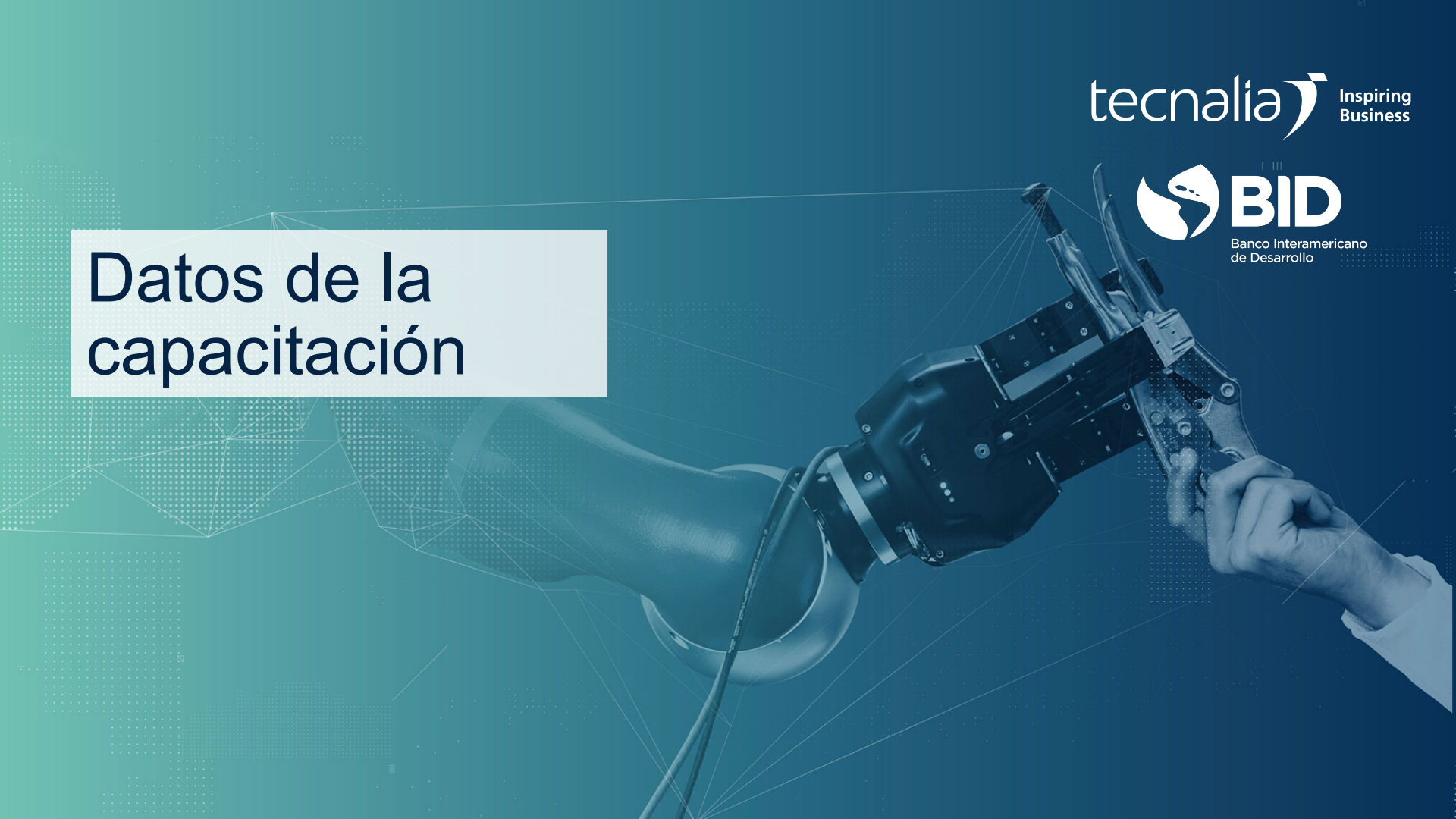
tecnalia Inspiring Business

BID Banco Interamericano de Desarrollo

CIBERSEGURIDAD EN ENERGÍA

Capacitación en Ciberseguridad para empresas de servicio eléctrico y reguladores de América Latina y Caribe

Datos de la capacitación



Objetivo

- El objetivo es dotar a los asistentes de los conocimientos fundamentales y necesarios para poder reforzar e implementar estrategias de defensa ante posibles ciberataques, y ser conscientes de las amenazas actuales y futuras a las que se enfrenta el sector.

- Dadas las circunstancias provocadas por la COVID-19, los cursos se desarrollarán en remoto, y en directo.

- Dos modalidades de cursos: para gestores y para técnicos.

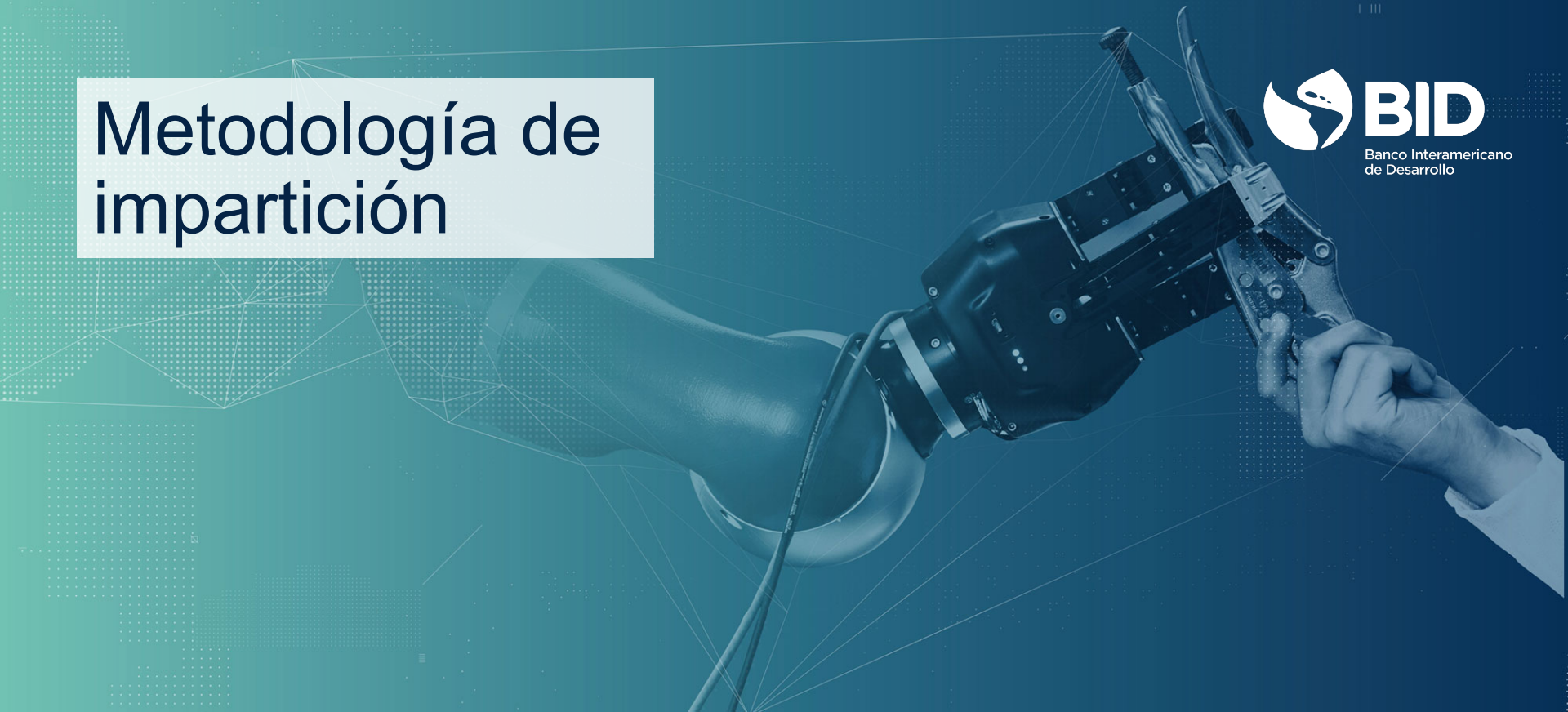
Curso para gestores

- Orientado a gerentes, directivos y reguladores.
- El **objetivo** es ofrecer ciertas pautas de ciberseguridad que deben ser conocidas por parte de los gestores, para entender las necesidades de protección, las amenazas pasadas y futuras a las que se pueden enfrentar y que mecanismos de protección se pueden desplegar en sus organizaciones.
- **Perfil de los asistentes**: profesionales del sector energético que están en puestos de dirección o de decisión, no siendo necesario tener conocimientos específicos técnicos.

Curso para técnicos

- Dirigido a aquellos **perfiles técnicos** que operan en alguna parte del ciclo de vida de la energía, para que por una parte sean conscientes de las amenazas a las que se pueden enfrentar, y por otra que puedan ejercitar mediante ejercicios prácticos los conocimientos adquiridos.
- Está compuesto por dos partes, una parte **teórica** con ejercicios teóricos y una segunda parte **práctica** en la que se ejercitarán los conocimientos adquiridos.
- **Perfil de los asistentes**: profesionales del sector energético que están en puestos de supervisión, mantenimiento y configuración de los elementos que conforman la Smart Grid. Adicionalmente al conocimiento que tengan de equipos de subestaciones, protocolos, PLCs, y otros elementos del sector, se recomienda que tengan conocimientos básicos de Linux.

Metodología de impartición



Curso para Gestores

- La duración del curso para gestores es de **10 horas**
- Se propone que se realice en **2 semanas**, de tal forma que se impartan **5 horas por semana**
- La duración de cada sesión sería de **2,5 horas**
- Asistencia: **20 participantes**

Curso para Técnicos

- La duración del curso para técnicos es de **40 horas**
- Se propone realizarlo a lo largo de **9-10 semanas**, impartiendo **6 horas semanales** en días diferentes
- La duración de las sesiones podrá ser o de **2 horas** o **4 horas** dependiendo del módulo a impartir
- Asistencia: **12 participantes**

Módulos	Enunciado	Semanas									
		1	2	3	4	5	6	7	8	9	10
Modulo 1	Conceptos base de ciberseguridad	4h									
Modulo 2	Situación y retos en materia de ciberseguridad del sector eléctrico	2h									
Módulo 3	Normativas y estándares de ciberseguridad aplicables		4h								
Módulo 4	Análisis de Riesgos de ciberseguridad		2h	2h							
Módulo 5	Clasificación de contramedidas y controles de seguridad en función del elemento a proteger				4h						
Módulo 6	Respuesta ante incidentes				2h						
Módulo 7	Cyber-Range					2h					
Módulo 8	Retos Futuros de Ciberseguridad en la Smart Grid					1h					
Módulo 9	Tecnologías emergentes					1h					
Prueba de conocimiento y certificado:						1h					
Módulo 10 Práctica	Prácticas de Cyber-Range y Ciberseguridad							6h	6h	3h	
Reunión de cierre y lecciones aprendidas											2h

Impartición de los cursos

- Para las sesiones teóricas se contempla la utilización de **herramientas de comunicación online** (Teams, Webex, Zoom, o Google Meet).
- Para las sesiones prácticas, se deberá tener en cuenta las **características de los PCs** que los participantes van a tener que utilizar, ya que se prevé la utilización de máquinas virtuales, conexiones VPN, y utilización de herramientas de monitoreo de los avances como puede ser FBCTF (Facebook capture the flag).
- Se recomienda, tener la posibilidad de realizar una **prueba de conexión** unos días antes del comienzo del curso para asegurar que las conexiones funcionan correctamente.

Impartición de los cursos

- Se establecerá un **punto de comunicación** entre participantes y TECNALIA, ya sea a través de un foro, o utilización de herramientas para tal fin, con el fin de poder resolver dudas e inquietudes.
- Si los participantes, el BID y los instructores acceden, se recomienda **grabar las sesiones**, con el único objetivo de que los participantes que no puedan atender a los cursos por problemas de comunicación puedan posteriormente reproducir el contenido de los mismos.

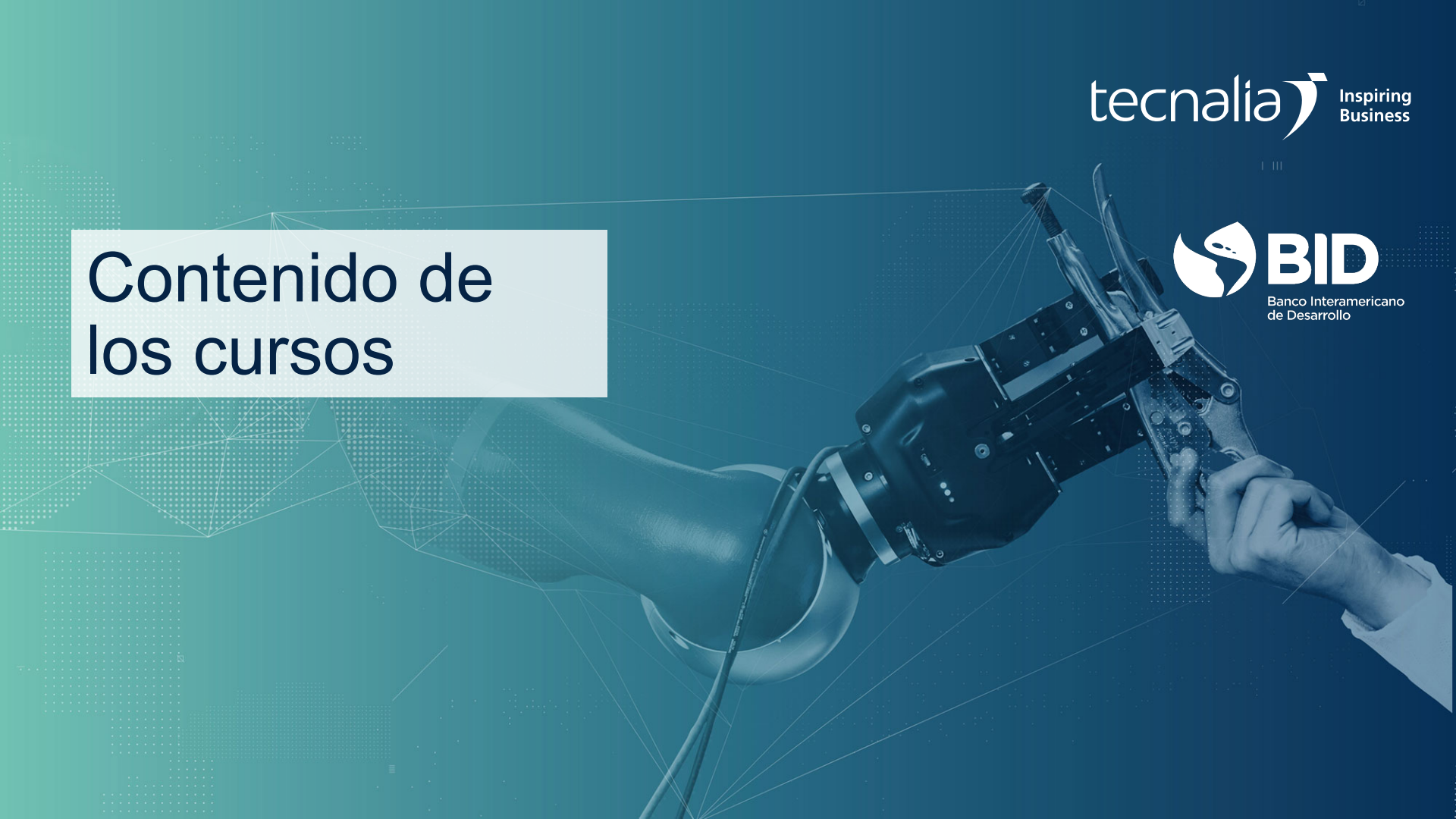
Materiales de Capacitación

- El material de las presentaciones de todos los cursos se entregará tanto a los participantes como al BID
- También se entregarán todas las máquinas virtuales que puedan ser utilizadas para la realización de las prácticas

tecnalia Inspiring Business

BID Banco Interamericano de Desarrollo

Contenido de los cursos



Módulos de capacitación

	Horas Perfil Gestión	Horas Perfil Técnico
1. Conceptos base de ciberseguridad	2	4
2. Situación y retos en materia de ciberseguridad del sector eléctrico	2	2
3. Normativas y estándares de ciberseguridad aplicables	1	4
4. Análisis de Riesgos de ciberseguridad	0,5	4
5. Clasificación de contramedidas y controles de seguridad en función del elemento a proteger	0,5	4
6. Respuesta ante incidentes	1,0	2
7. Ciber-Range	1	2
8. Retos Futuros de Ciberseguridad en la Smart Grid	1	1
9. Tecnologías emergentes	1	1
10. Prácticas (10-15 horas)		15
Prueba de conocimiento y certificado:		1
	10	40

Módulo 1: Conceptos básicos de ciberseguridad

Objetivos: Exponer conceptos generales y buenas prácticas en ciberseguridad, así como una primera aproximación de las estrategias a seguir en entornos industriales en general.
a) Administración de la seguridad: i. Conceptos básicos: Vulnerabilidad, amenaza, riesgo, contramedida. ii. Propiedades de los sistemas ciberseguros: confidencialidad, integridad, disponibilidad, privacidad. iii. Tipología de adversarios y motivaciones. Malware, ingeniería social.
b) Ciberseguridad Industrial, estrategias, amenazas.
c) Respuesta ante incidentes de ciberseguridad.
d) Conceptos básicos de Criptografía y esteganografía.

Módulo 2: Situación y retos en materia de ciberseguridad del sector eléctrico

Objetivos: Exponer la situación del sector con respecto a la ciberseguridad, tanto en Latinoamérica como en Europa y Norteamérica, y los retos a los que se enfrenta el sector a la hora de definir y desplegar mecanismos de protección.
a) Situación actual del sector tanto en LATAM y otras regiones (Europa y Norteamérica).
b) Incidentes de ciberseguridad en sector energético, ejemplos basados en referencias de ECSO, EU y NIST.
c) Retos actuales del sector a la hora de implementar soluciones de ciberseguridad en sector eléctrico.

Módulo 3: Normativas y estándares de ciberseguridad aplicables

Objetivos: Presentar las principales normativas y estándares de ciberseguridad que tienen que ser tenidos en cuenta en el sector energético, haciendo mayor énfasis en las normas IEC-62443 e IEC-62351.
a) Directiva NIS, y marco de ciberseguridad del NIST (Europa y USA).
b) IEC-62351. (estructura, utilización y consecuencias operativas).
c) IEC-62443. (estructura y utilización y consecuencias operativas).
d) Otros estándares de interés: IEEE 1686, ISO/IEC 27019.
e) Ejercicio práctico de interpretación de normas 62351 y 62443.

Módulo 4: Análisis de Riesgos de ciberseguridad

Objetivos: Presentar las pautas necesarias para realizar análisis de riesgos de ciberseguridad en sector energético, y realización de un plan director de ciberseguridad.
a) Pautas de realización de un análisis de riesgos de ciberseguridad.
b) Fuentes de riesgos.
c) Identificación de activos.
d) Identificación de posibles amenazas
e) Recomendaciones de fuentes de información de ataques, ejemplo de Mitre.
f) Realización de un Plan director de ciberseguridad.

Módulo 5: Clasificación de contramedidas y controles de seguridad en función del elemento a proteger

Objetivos: Definir elementos a proteger dependiendo de la fase del ciclo de vida energético (generación, distribución, transporte y última milla), así como presentación de diferentes controles de seguridad de ciertos elementos de la Smart Grid.
a) Elementos a tener en cuenta en todo el ciclo de vida de fuentes de energía tradicionales y renovables: Generación, Distribución, Transporte y Ultima Milla.
b) Subestación/utilities.
c) Smart meters.
d) RTUs.
e) IED.
f) Scada.
g) Protocolos.
h) Elementos de comunicación Switches/routers (orientado a switches industriales).
i) Ejercicio de discusión y de aplicación concreta de contramedidas en una Smart Grid.

Módulo 6: Respuesta ante incidentes

Objetivos: Entender en que consiste un sistema de respuesta ante incidentes con respecto a incidentes de ciberseguridad, y como se podría implementar, identificando los actores involucrados, y adicionalmente entender los conceptos de CERT, CSIRT y CNPIC e identificar los principales de la región Latinoaméricana.
a) Conceptos base de gestión de incidencias. Qué es, actores, niveles.
b) Frameworks de actuación ante incidencias: i. Framework de actuación de ENISA. ii. Smart grid task force – Europa, junio de 2019, ámbitos diferentes y requisitos. iii. Energy cybersecurity capability maturity framework del departamento de energía de USA y del Homeland Security.
c) Gestión de amenazas/incidentes Infraestructuras críticas en LATAM (México, Colombia, Argentina, Brasil, Centroamérica).
d) Conceptos de CERTs, CSIRTs y CNPIC.
e) Ejercicio de respuesta ante incidentes.

Módulo 7: Cyber-Range

Objetivos: Presentación de lo que es un Cyber-Range, para que sirve y como podría ser utilizado en el sector energético para ejercitar a los técnicos.
a) Qué son, conceptos clave, tipos de ejercicios, utilidad en el sector eléctrico qué es federación de Cyber-Ranges.
b) Tipos de ejercicios de Cyber-Range que se pueden realizar.

Módulo 8: Retos Futuros de Ciberseguridad en la Smart Grid

Objetivos: Exponer diferentes retos futuros en ciberseguridad en el sector, y como se han de tener en cuenta dentro de la estrategia de ciberseguridad de cada uno de los actores de la Smart Grid
a) Retos futuros de ciberseguridad en la Smart Grid (prosumer, energías renovables, vehículo eléctrico).

Módulo 9: Tecnologías emergentes

Objetivos: Presentar como se espera que las nuevas tecnologías puedan afectar al sector energético y que posibilidades abren al sector.
a) Inteligencia artificial aplicada a la ciberseguridad.
b) Aplicación de Blockchain en sector energía. Casos de usos para carga de coche eléctrico, origen de energía renovable, IDs (desde el punto de vista de ciberseguridad).
c) Criptografía Cuántica y Post-cuántica.
d) Edge computing/5G.

Módulo 10: Prácticas de Cyber-Range y Ciberseguridad

Objetivos: Realizar diferentes ejercicios prácticos en los que se comprometan equipos de una red IT y posteriormente realizar el salto a la red OT, realizando diferentes ataques. Asimismo, se realizarán ejercicios de Cyber-Range de defensa de red team y blue team.
a) Fases de un ataque, y realización de prácticas de pentesting usando las herramientas de Kalilinux (fuerza bruta, man in the middle….)
b) Ataques a Infraestructura de Laboratorio: i. Denegación de Servicio DoS. ii. Man in the middle. iii. Fuerza bruta. iv. Acceso a control de Scada. v. Otros
c) Cyber-Range: Ejercicios de ataque
d) Demo de certificación de Smart meters (únicamente la parte de ciberseguridad).

Prueba de conocimiento y certificado

Objetivos: Realizar una prueba conjunta entre los alumnos y los profesores, para comprobar que los conocimientos se han adquirido y despejar posibles dudas y reforzar conceptos que no hayan sido entendidos
a) Prueba conjunta entre alumnos e instructores

Por cualquier duda o consulta por favor contactar a:

Virginia Snyder
Especialista Senior Energía
División de Energía
Sector de Infraestructura y Energía
(202)215-3471
https://blogs.iadb.org/energia/es/
https://hubenergia.org/