

Informe: Diplomado en Ciberseguridad



Elaborado por: Servicio al Estudiante
Enero, 2022.-

CONTENIDO



- I. Objetivos.
- II. Programa.
- III. Consideraciones del Facilitador.
- IV. Calificaciones.
- V. Evaluación de la Capacitación.



Capacitación para el Ministerio de Industria Comercio y MIPYME

I. OBJETIVOS

OBJETIVO GENERAL:

Proporcionar a los alumnos herramientas teóricas y prácticas para proteger los sistemas informáticos y las informaciones que generan las organizaciones y que deben mantenerse bajo control, asegurando su confidencialidad, disponibilidad e integridad.

OBJETIVOS ESPECÍFICOS:

- Analizar la manera en que es administrada la seguridad informática.
- Aprender sobre principales técnicas preventivas ante ataques maliciosos.
- Conocer sobre el Hackeo Ético.
- Aprender sobre los estándares de seguridad de la información de la ISO27001 y NIST.
- Conocer herramientas esenciales para la defensa ante ataques cibernéticos.

II. PROGRAMA

Tema I. Administración de seguridad informática de la organización. (4hrs)

Tema II. Técnicas preventivas de ataques malintencionados. (5hrs)

Tema III. Hackeo en el marco ético, prácticas en entornos ofensivos y defensivos.
(8hrs)

Tema IV. Auditoría forense de ciberseguridad e implementación de mejores prácticas basadas en NIST e ISO 2700. (5hrs)

Tema V. Conocimiento de herramientas esenciales de Ciberseguridad. (8hrs)

III. CONSIDERACIONES DE LOS FACILITADORES

En el Diplomado en Ciberseguridad a integrantes del departamento de TI del Ministerio de Industria, Comercio y MIPYMES, los estudiantes mostraron gran interés y una muy buena participación en los temas tratados, pudieron identificar elementos importantes que podrán incorporar en sus tareas diarias dentro de la institución.

En su mayoría completaron en tiempo y en forma las asignaciones, a excepción de aquellos que en apartado de Calificaciones de más abajo se encuentran en rojo, en virtud de que no fueron entregadas las prácticas, por lo que dicho apartado aparece en cero (0). Sin embargo, se puede apreciar su buen rendimiento en aquellas que fueron completadas.

El índice general del curso fue de 89%, lo que se considera bueno. Pudimos identificar participantes de muy buen nivel de conocimiento en Ciberseguridad.

IV. CALIFICACIONES

No.	Nombre	Apellido(s)	Caso Estudio	Práctica 1	Práctica 2	Práctica 3	Práctica 4	Práctica 5	1era Prueba	Examen Final	Total del curso (Real)	Letra
1	Elvys Jose	Camacho	15	9	10	10	8	9	10	25	96	A+
2	Melida Leandra	De oleo Liriano	15	9	8	10	8	9	8	21	88	B+
3	Emil Julius	Diaz Ureña	15	9	9	10	10	9	10	25	97	A+
4	Luis Daniel	Feliz Gonzalez	15	9	9	10	10	9	10	23	95	A+
5	Rodolfo Luis	Feliz Rincon	0	9	9	10	10	9	8	25	80	B
6	Manuel	Frías Tejada	15	9	9	10	10	0	10	25	88	B+
7	Saholin Maiquer	Montilla Beriguete	15	0	0	10	10	9	10	24	78	C+
8	Moises Alberto	Ricart Paulno	15	9	9	10	10	9	10	25	97	A+
9	Julio Alexander	Rodriguez Diaz	15	9	9	10	0	0	10	25	78	C+
10	Miguel Starling	Salas	15	9	9	10	10	9	10	22	94	A
Promedio del Curso:			13.5	8.1	8.1	10	8.6	7.2	9.6	24	89.1	B+

Revisado por:
Dirección Académica



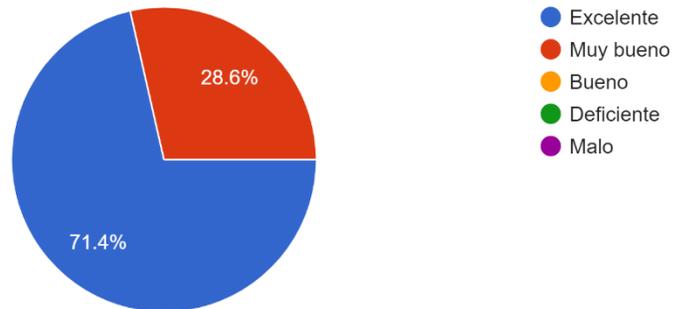
IV. EVALUACIÓN DE LA CAPACITACIÓN

Evaluación que fue aplicada a los colaboradores con fines de conocer su apreciación personal acerca de los aspectos generales del curso y elevar la calidad de este.

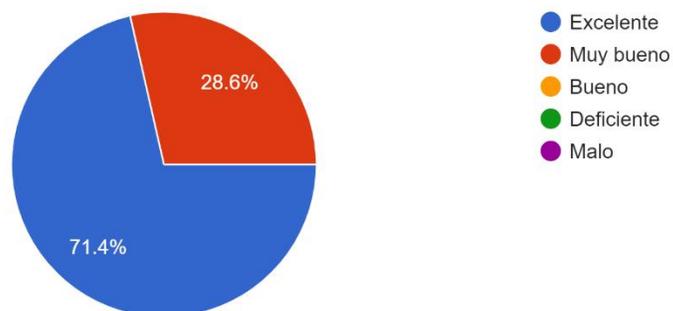
Los resultados se presentan a continuación:

VALORACIÓN DEL FACILITADOR

Puntualidad
7 respuestas

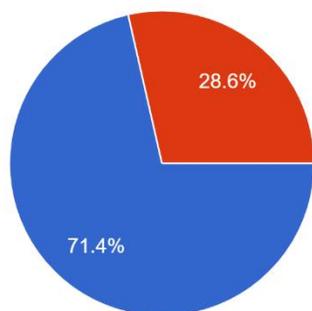


Su actitud ante el grupo
7 respuestas



Mostró dominio del tema

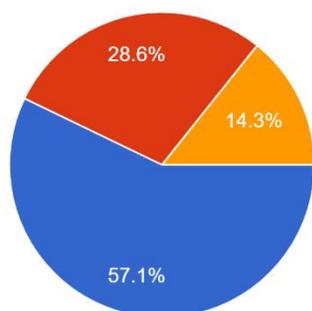
7 respuestas



- Excelente
- Muy bueno
- Bueno
- Deficiente
- Malo

Dió a conocer los objetivos del curso

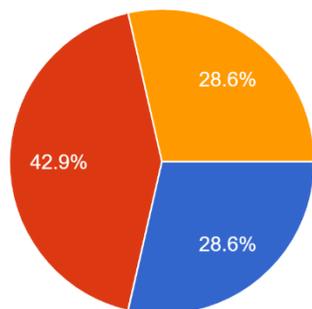
7 respuestas



- Excelente
- Muy bueno
- Bueno
- Deficiente
- Malo

Proporcionó claramente las instrucciones para las actividades

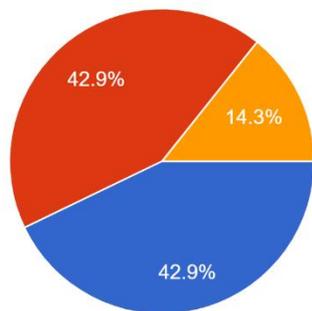
7 respuestas



- Excelente
- Muy bueno
- Bueno
- Deficiente
- Malo

Propició actividades de colaboración

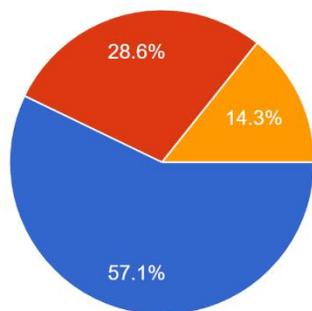
7 respuestas



- Excelente
- Muy bueno
- Bueno
- Deficiente
- Malo

Motivó la participación del grupo

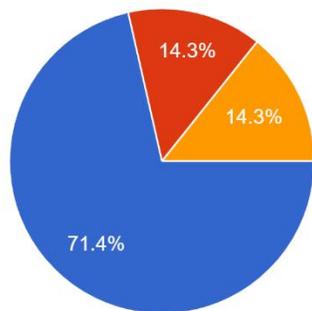
7 respuestas



- Excelente
- Muy bueno
- Bueno
- Deficiente
- Malo

Aclaró las dudas de los participantes

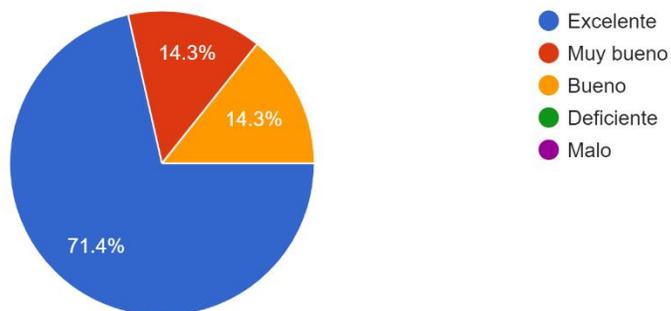
7 respuestas



- Excelente
- Muy bueno
- Bueno
- Deficiente
- Malo

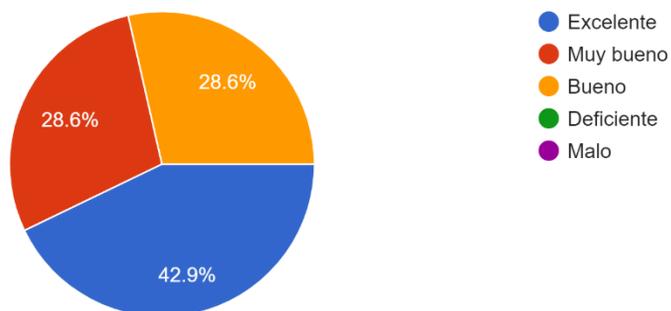
Aclaró las dudas de los participantes

7 respuestas



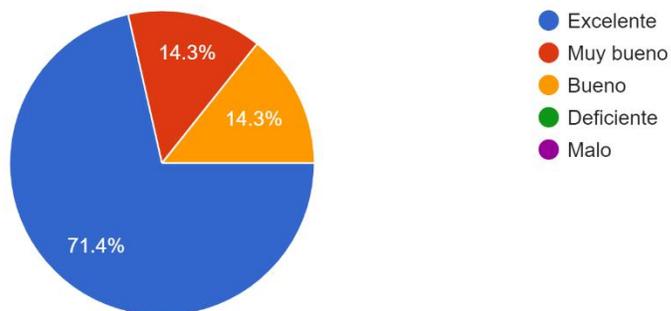
Apoyó adecuadamente su exposición con el material didáctico

7 respuestas



Estaba realmente interesado en que aprendiera

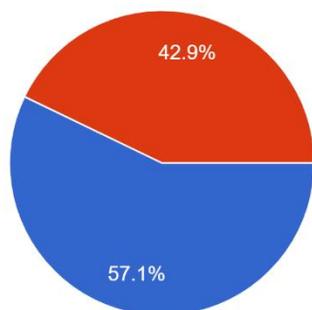
7 respuestas



LOGÍSTICA DEL EVENTO

Coordinación previa al evento

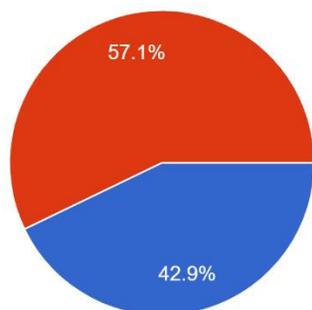
7 respuestas



- Excelente
- Muy bueno
- Bueno
- Deficiente
- Malo

Coordinación durante el evento

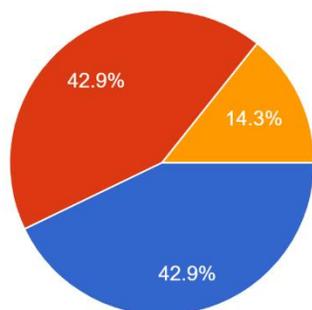
7 respuestas



- Excelente
- Muy bueno
- Bueno
- Deficiente
- Malo

La duración del evento

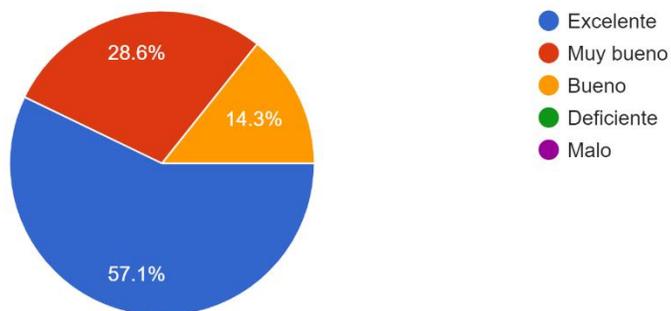
7 respuestas



- Excelente
- Muy bueno
- Bueno
- Deficiente
- Malo

Plataformas para capacitación virtual utilizadas

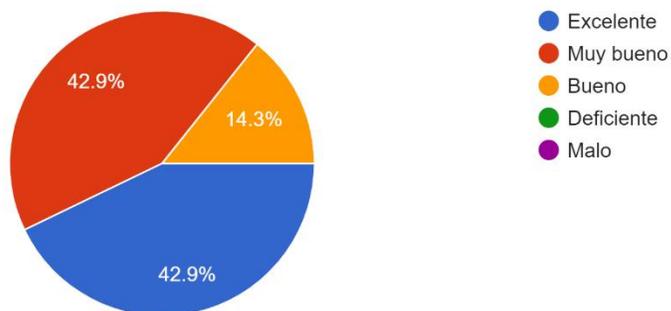
7 respuestas



PROGRAMA DEL CURSO

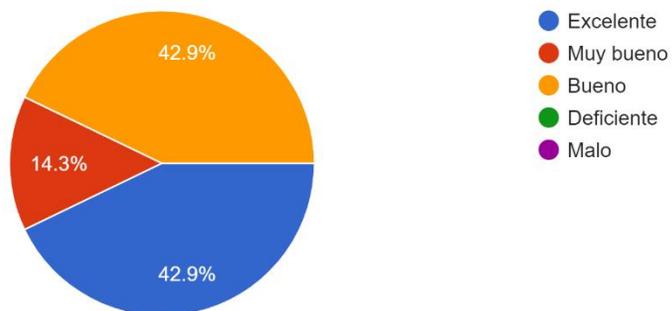
La proporción de aspectos teórico y prácticos

7 respuestas



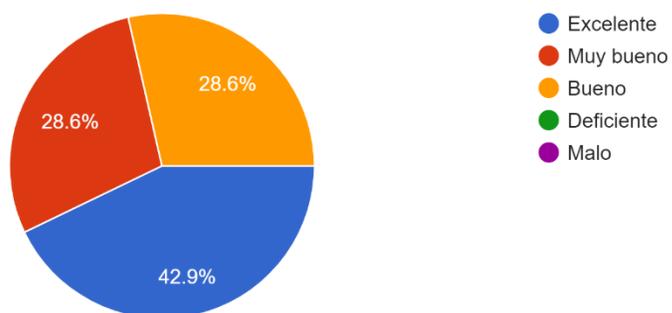
Congruencia de la información presentada y los materiales de apoyo

7 respuestas



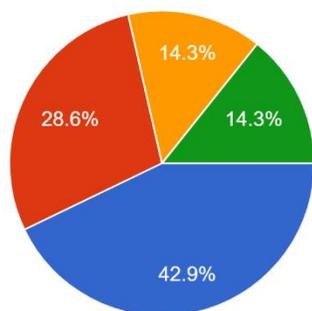
El nivel de profundidad con que se abordaron los temas

7 respuestas



El curso cumplió con sus expectativas

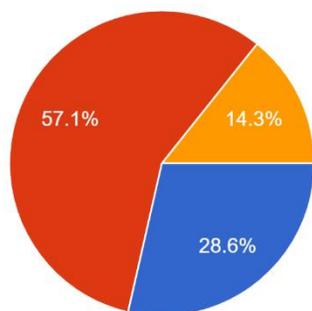
7 respuestas



- Excelente
- Muy bueno
- Bueno
- Deficiente
- Malo

El contenido aprendido es aplicable para su desempeño

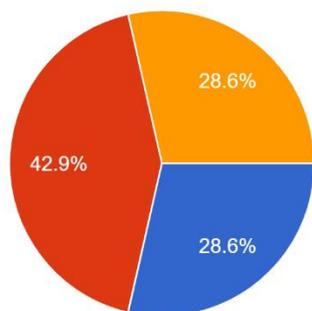
7 respuestas



- Excelente
- Muy bueno
- Bueno
- Deficiente
- Malo

Material de apoyo

7 respuestas



- Excelente
- Muy bueno
- Bueno
- Deficiente
- Malo

Aprendizajes personales más significativos mencionados por los participantes del diplomado.7 respuestas

- ❖ Criptografía, la importancia de segregar la infraestructura, como verificar un correo electrónico sospechoso.
- ❖ Prevención de ataques Almacenamiento en la nube, El uso de herramientas necesarias para las implementar en seguridad TIC
- ❖ La herramienta Maltego, identificación de cuentas vulnerables y la herramienta redline.
- ❖ Casos de estudios, herramientas de escaneo de vulnerabilidades y normativas y marco de ciberseguridad.
- ❖ Herramientas de implementación para el pentesting, temas de ransomware y la herramienta maltego
- ❖ La aplicación Maltego, La auditoría Forense, La criptografía
- ❖ Una buena orientación de como promovemos la seguridad de la información puede permitirnos que nos vean como entes de apoyo fundamentales para el cumplimiento de las metas de la institución. Es importante conocer nuestras operaciones e infraestructura a totalidad, para así tomar buenas

En qué actividades considera que puedes aplicar lo aprendido7 respuestas

- ❖ En mi trabajo diario
- ❖ En el ámbito laboral
- ❖ Tanto en mis actividades de seguridad defensiva como en la creación de políticas, procedimientos y aplicación de buenas prácticas basado en normativas.
- ❖ En el trabajo y futuros estudios
- ❖ En mi labor diaria.
- ❖ En mis labores profesionales y mi pasatiempo en cuanto a la seguridad ofensiva.

CONCLUSIÓN

Basandonos en la evaluación de los aspectos generales de la capacitación, se presentan muy buenos indicadores de aprendizaje e interpretamos que hemos alcanzado los objetivos propuestos.

La gran mayoría de los participantes tuvo muy buen desempeño y quedó satisfecho con la metodología de los facilitadores, la logística del evento y el contenido del programa de clases.

Aprendieron sobre la protección de los sistemas informáticos, sobre importancia de la información controlada que generan las organizaciones y como asegurar la confidencialidad e integridad de la misma. También , como mitigar los riesgos de los ciberataques y las herramientas necesarias para la seguridad TIC.

Además, algo muy importante y positivo es que los participantes lograron identificar esas areas donde pueden aplicar esos conocimientos adquiridos y enriquecer sus actividades laborales.