# Universidad Tecnológica de Cancún

Ingeniería de desarrollo y gestión de software.

Seguridad en el desarrollo de aplicaciones

Profesora:
Bravo Calderon Erika Alejandra

Actividad:
Actividad 2 U1

Grupo:
IDYGS83

Nombre(s):
Perez Couoh Jose Angel
21393149

Tarea: Ciberataque y Prevención de Apagones en Ucrania (2015)

**Introducción:**

El ciberataque que resultó en el apagón masivo en Ucrania en 2015 destaca la importancia de la ciberseguridad en infraestructuras críticas. En este documento, analizaré posibles medidas que podrían haberse tomado para prevenir este incidente y propondré acciones que hubiera considerado adecuadas en mi rol como estudiante de desarrollo de software.

**Medidas de Prevención:**

Mejora de la Ciberseguridad:

Implementar medidas avanzadas de seguridad cibernética, como firewalls, sistemas de detección de intrusiones y sistemas de monitoreo continuo.

Actualizar regularmente los sistemas operativos y software para corregir vulnerabilidades conocidas.

Concientización y Capacitación:

Proporcionar programas de concientización sobre seguridad cibernética para los empleados de las compañías de energía, destacando las amenazas potenciales y las mejores prácticas de seguridad.

Ofrecer capacitación específica en ciberseguridad para el personal encargado de la gestión y supervisión de sistemas de control industrial.

Implementación de Segmentación de Redes:

Separar las redes de control industrial de las redes corporativas para limitar la propagación de malware y reducir la superficie de ataque.

Utilizar firewalls y políticas de segmentación para restringir el acceso no autorizado a sistemas críticos.

Respuesta y Recuperación:

Desarrollar planes de respuesta a incidentes para abordar rápidamente los ciberataques, minimizando el tiempo de inactividad.

Realizar simulacros periódicos para garantizar una respuesta eficiente y mejorar la capacidad de recuperación.

**Acciones Personales:**

En mi rol como estudiante de desarrollo de software, habría abogado por la promoción de la ciberseguridad como una prioridad estratégica. Además, habría propuesto realizar evaluaciones regulares de vulnerabilidades y auditorías de seguridad para identificar y abordar posibles debilidades en la infraestructura.
Además, abogaría por la colaboración entre el gobierno, la industria y expertos en ciberseguridad para compartir información sobre amenazas y desarrollar medidas de defensa colectivas.

**Conclusión:**
La prevención de ciberataques en infraestructuras críticas implica una combinación de tecnologías avanzadas, concientización del personal y una respuesta rápida y eficaz ante incidentes. La implementación de estas medidas puede reducir significativamente el riesgo de ataques similares en el futuro.

referencias
[1] El papel de la ciberseguridad en el conflicto entre Rusia y Ucrania .... https://conecta.tec.mx/es/noticias/santa-fe/educacion/el-papel-de-la-ciberseguridad-en-el-conflicto-entre-rusia-y-ucrania.
[2] Rusia invade Ucrania: cómo los ciberataques se convirtieron en otra .... https://www.bbc.com/mundo/noticias-internacional-60508957.
[3] Rusia y Ucrania: los 3 ciberataques rusos que más teme Occidente. https://www.bbc.com/mundo/noticias-60850173.
[4] La ciberguerra de Rusia contra Ucrania nunca ha acabado. https://elpais.com/tecnologia/2022-02-26/la-ciberguerra-de-rusia-contra-ucrania-nunca-ha-acabado.html.