DESARROLLO DE SOFTWARE SEGURO

ESTRATEGIAS DE SEGURIDAD BASADAS EN ISO 27002

- Jorge Ibarra Peña
- 20310025
- 7°P
- Desarrollo de Software
- 06/09/2023
- CETI COLOMOS

Falta de Conciencia de Seguridad por parte de los Usuarios:

Campañas de Sensibilización: Realizar campañas periódicas de concienciación en seguridad de la información para educar a los empleados sobre las amenazas y las prácticas seguras.

Políticas y Directrices Claras: Establecer políticas y directrices de seguridad comprensibles que los empleados deban seguir, asegurándose de que estén bien comunicadas y entendidas.

Infraestructura de Seguridad Insuficiente:

Mantenimiento y Actualización Regular: Garantizar el mantenimiento y la actualización periódica de todos los sistemas y software críticos mediante la aplicación de parches y actualizaciones de seguridad.

Implementación de Cortafuegos y Sistemas de Detección de Intrusiones: Desplegar cortafuegos y sistemas de detección de intrusiones para proteger la red y detectar posibles amenazas.

Equipos no Seguros:

Gestión de Activos Tecnológicos: Mantener un registro actualizado de todos los equipos y dispositivos de la organización, y asegurarse de que estén configurados y protegidos adecuadamente.

Políticas de Seguridad para Dispositivos: Establecer políticas que exijan a los empleados mantener sus dispositivos seguros y actualizados, y reportar cualquier pérdida o robo de manera inmediata.

Accesos Desprotegidos:

Control de Acceso Estricto: Implementar medidas de control de acceso, como autenticación multifactor (MFA) y contraseñas robustas, para garantizar que solo personas autorizadas tengan acceso a sistemas y datos.

Gestión de Privilegios: Restringir los privilegios de acceso a sistemas y datos en función de las necesidades específicas de cada usuario o grupo de usuarios.

Falta de Procesos de Monitoreo:

Monitoreo Continuo de Sistemas: Establecer sistemas de monitoreo de seguridad que supervisen el tráfico de red, la actividad de los usuarios y los registros de eventos para detectar posibles amenazas y brechas de seguridad.

Análisis Regular de Registros y Alertas: Implementar procesos para revisar de manera periódica los registros de eventos y las alertas de seguridad, tomando medidas inmediatas ante incidentes o comportamientos sospechoso

CONCLUSIÓN

a seguridad de la información es un aspecto crucial en cualquier organización, y abordar las vulnerabilidades es esencial para proteger los activos y datos importantes. Para contrarrestar usuarios sin conciencia de seguridad, es importante educar y concientizar a los empleados. La infraestructura de seguridad debe mantenerse actualizada y protegida mediante cortafuegos y sistemas de detección de intrusiones. Los equipos deben gestionarse y configurarse de manera segura, y el acceso a sistemas y datos debe ser estrictamente controlado. Por último, la implementación de procesos de monitoreo constante es clave para detectar y responder a las amenazas. La seguridad de la información debe ser un esfuerzo continuo y adaptarse a las cambiantes amenazas cibernéticas para mantener nuestros sistemas y datos seguros.

BIBLIOGRAFÍA

Strawbridge, G. (2023, 9 marzo). Cómo promover la concienciación sobre la ciberseguridad en su organización | MetaCompliance. *MetaCompliance*. https://www.metacompliance.com/es/blog/cyber-security-awareness/how-to-promote-cyber-security-awareness-in-your-organisation

De TechTarget, C. (2021). Autenticación multifactor o MFA. *ComputerWeekly.es*. https://www.computerweekly.com/es/definicion/Autenticacion-multifactor-o-MFA