FACULTAD DE INGENIERÍA

Carrera Profesional de Ingeniería de Sistemas e Informática

Tarea 2

Amenazas de Red

Curso:

Seguridad Informática

Sección:

31437

Docente:

ENZO RUBEN HEREDIA MELENDEZ

Presentado por:

Cutimbo Jibaja, Daniel Alberto

Arequipa – Perú

2022

¿Que controles de seguridad implementarías en una organización o en la organización en la que laboras?

A nivel administrativo:

- **Crear y aplicar políticas de seguridad de la información:** Crear normas sobre el acceso y uso de los dispositivos de la empresa, sobretodo los dispositivos que tienen acceso a información sensible. Evitando así que puedan ser usados para motivos personales pudiendo descargar archivos o accediendo a páginas web que puedan contener código malicioso.
- **Concientización de la seguridad de la información:** Capacitar al personal de la organización sobre los métodos de hacking y sus riesgos no solo contra la información de la organización sino también contra su información personal.
- **Comunicación efectiva:** Fomentar la comunicación efectiva entre las distintas áreas que tienen acceso a la información con el departamento de ciberseguridad para prevenir, y proteger la información frente a incursiones no autorizadas.

A nivel de hardware:

- **Ofrecer hardware dedicado de uso śolo laboral y bloquear los puertos de acceso físicos:** Bloquear los pueros de acceso (USB, microUSB, USB-C, etc) de los ordenadores y dispositivos que utilice el personal de la organización de uso exclusivo para laborar, acceder a la información o enviar correos, mensajes a distintas áreas.

A nivel de software:

- **Cambio de las contraseñas de acceso de los dispositivos:** Los dispositivos de red, bases de datos y cualquier dispositivo dentro de la organización debe estar protegido con contraseña distinta a la establecida por defecto y sobretodo cambiar las contraseñas cada cierto periodo de tiempo.
- **Monitorear constantemente el registro de eventos:** Establecer horarios y cuentas de acceso autorizado a la información para así detectar incursiones por parte de terceros, además de identificar los dispositivos por dirección MAC e IP.
- **Sistema de cierre de sesión automático:** Implementar en los dispositivos y sistemas un sistema de *Automatic Log-Out* para delimitar el tiempo de inactividad de los usuarios y por seguridad cerrar su acceso a la información.

Bibliografía:

- ISO/IEC 27002:2013, Information technology — Security Techniques — Code of practice for information security controls (Tecnología de la información – Técnicas de seguridad – Código de práctica para controles de seguridad de la información)
- ISO/IEC 27003, Information technology — Security techniques — Information security management system implementation guidance (Tecnología de la información – Técnicas de seguridad – Guía de implementación del sistema de gestión de seguridad de la información)
- ISO/IEC 27004, Information technology — Security techniques — Information security management — Measurement (Tecnología de la información – Técnicas de seguridad – Gestión de seguridad de la información – Medición)
- ISO/IEC 27005, Information technology — Security techniques — Information security risk management (Tecnología de la información – Técnicas de seguridad – Gestión de riesgos de seguridad de la información)