EJERCICIO 1

Políticas de seguridad informática de los usuarios

Capacitación continua: Realizar sesiones de capacitación periódicas para mantener a los empleados actualizados sobre las últimas amenazas y mejores prácticas de seguridad.

Uso adecuado: Implementar políticas claras sobre el uso adecuado de los recursos tecnológicos, incluyendo la prohibición de actividades personales en dispositivos de la empresa.

Actualizaciones y parches: Asegurarse de que todos los dispositivos y software estén actualizados con los últimos parches de seguridad para prevenir vulnerabilidades.

Sistema de seguridad informática

Antivirus y antimalware: Implementar soluciones de antivirus y antimalware en todos los dispositivos y realizar análisis regulares para detectar y eliminar amenazas.

Firewall: Configurar firewalls en todos los puntos de entrada y salida de la red para proteger contra accesos no autorizados y ataques externos.

Cifrado: Utilizar cifrado de extremo a extremo para proteger datos sensibles tanto en tránsito como en reposo. Esto incluye el uso de protocolos seguros como HTTPS y VPNs para conexiones remotas.

Apertura y cierre de las salas

Horarios específicos: Establecer horarios específicos para la apertura y cierre de las salas de computadores, asegurando que solo el personal autorizado tenga acceso durante estos tiempos.

Supervisión y registro: Implementar un sistema de registro para monitorear quién entra y sale de las salas, y asegurar que siempre haya personal autorizado supervisando la apertura y cierre.

Consideraciones al operar con el equipamiento

Mantenimiento preventivo: Realizar mantenimiento preventivo regular de los equipos para asegurar su correcto funcionamiento y prolongar su vida útil.

Manipulación segura: Establecer procedimientos adecuados para la manipulación segura de equipos y dispositivos, incluyendo el uso de equipos de protección personal cuando sea necesario.

Control de acceso, identificación de los usuarios y requisitos de las contraseñas

Acceso restringido: Limitar el acceso a las salas de computadores y a la información sensible solo a personal autorizado mediante el uso de sistemas de control de acceso.

Identificación y autenticación: Implementar sistemas de identificación y autenticación robustos, como tarjetas de acceso, biometría y autenticación de dos factores.

Políticas de contraseñas: Establecer políticas de contraseñas seguras, incluyendo requisitos de longitud, complejidad y cambios periódicos. Además, fomentar el uso de gestores de contraseñas para almacenar y gestionar contraseñas de manera segura.

Prohibiciones en el uso de aplicaciones

Aplicaciones no autorizadas: Prohibir el uso de aplicaciones no autorizadas en los dispositivos de la empresa y realizar auditorías periódicas para asegurar el cumplimiento.

Descargas restringidas: Restringir la descarga de software y archivos desde fuentes no confiables para prevenir la instalación de malware y otras amenazas.