PRÁCTICA 1.2: NORMATIVA DE SEGURIDAD DEL PUESTO DE TRABAJO

ÍNDICE

ANTECEDENTES

GameForge Entertainment reconoce la importancia de la ciberseguridad para salvaguardar nuestros activos, incluyendo propiedad intelectual y datos de usuario. La protección de los puestos de trabajo es un componente esencial de nuestra estrategia de seguridad.

OBJETIVOS

El propósito de esta política es establecer las pautas y prácticas obligatorias para proteger los puestos de trabajo de GameForge Entertainment y reducir la superficie de ataque en toda la organización. Esta política se aplica a todos los empleados.

PUNTOS CLAVE

1. Uso de contraseñas seguras:

Todos los empleados deben utilizar contraseñas robustas y únicas para acceder a sus dispositivos y cuentas. Las contraseñas deben cumplir los estándares de seguridad y deben ser actualizadas regularmente. No se deben compartir contraseñas.

- **Longitud Mínima**: Establecer una longitud mínima de contraseña de al menos 12 caracteres.
- **Complejidad**: Exigir contraseñas que incluyan una combinación de letras mayúsculas, letras minúsculas, números y caracteres especiales.
- **Evitar Información** Personal: Prohibir el uso de información personal como nombres, fechas de nacimiento, o datos fácilmente accesibles en redes sociales.
- **No Reutilizar contraseñas**: Fomentar la creación de contraseñas únicas para cada cuenta o sistema. No permitir la reutilización de contraseñas.
- **Cambios periódicos**: Exigir cambios de contraseña periódicos, cada 90 días.
- **Bloqueo de cuentas**: Implementar bloqueos de cuenta después de un número específico de intentos fallidos para prevenir ataques.

2. Actualización de Software y Sistemas Operativos:

Todos los dispositivos de la empresa, incluyendo PC de sobremesa, portátiles, dispositivos móviles y servidores, deben mantenerse actualizados con las últimas actualizaciones y parches de seguridad.

- Establecer una política de actualización automática para garantizar que todos los dispositivos reciban parches de seguridad.
- Recordar a los empleados la importancia de aceptar y aplicar actualizaciones, incluso en dispositivos personales utilizados para el trabajo.

3. Protección de Dispositivos Móviles:

Los dispositivos móviles de propiedad de la empresa deben estar protegidos con medidas de seguridad, como bloqueo de pantalla, cifrado de datos y autenticación multifactor. Los empleados deben informar la pérdida o robo de un dispositivo inmediato.

- Proporcionar instrucciones detalladas sobre cómo activar y configurar funciones de seguridad, como el bloqueo de pantalla y el cifrado de datos, en dispositivos móviles.
- Incluir un procedimiento claro para reportar la pérdida o robo de dispositivos y las acciones a seguir.

4. BYOD (Bring Your Own Device) Opcional:

El uso de dispositivos personales para el trabajo (BYOD) es opcional. Si se utiliza, se deben aplicar medidas de seguridad específicas y cumplir con las políticas de seguridad de la empresa.

5. Formación en Ciberseguridad:

Todos los empleados deben recibir formación periódica en ciberseguridad para estar al tanto de las amenazas comunes y buenas prácticas de seguridad, incluyendo la identificación de phishing y ataques de ingeniería social.

6. **Gestión de Vulnerabilidades:**

Implementar una estrategia de gestión de vulnerabilidades que incluya escaneo de seguridad, evaluación de riesgos y acciones correctivas para corregir vulnerabilidades en sistemas y aplicaciones.

7. **Gestión de Identidades y Accesos:**

Implementar un sistema de gestión de identidades y accesos que garantice que los empleados tengan acceso adecuado a los recursos y datos en función de sus roles y responsabilidades.

8. **Supervisión y Detección de Amenazas:**

Desarrollar una estrategia de supervisión y detección de amenazas que incluya la revisión constante de registros y eventos de seguridad para identificar comportamientos inusuales o actividades maliciosas.

9. **Gestión de Incidentes de Seguridad:**

Establecer un procedimiento para la gestión de incidentes de seguridad, incluyendo la notificación oportuna y la respuesta a incidentes de ciberseguridad.

10. **Auditorías y Evaluaciones Regulares:**

Realizar auditorías y evaluaciones periódicas de la seguridad de la información y la infraestructura de la tecnología para garantizar el cumplimiento de políticas y estándares de seguridad.

11. **Educación Continua en Ciberseguridad:**

Proporcionar formación continua en ciberseguridad a los empleados para mantenerlos actualizados sobre las amenazas y las mejores prácticas.

12. **Política de Copias de Seguridad y Recuperación:**

Establecer una política de copias de seguridad y recuperación de datos que asegure la disponibilidad y la integridad de la información crítica.

13. Evaluación de Terceros:

Evaluar y establecer estándares de seguridad para terceros y proveedores de servicios que tengan acceso a los sistemas o datos de la empresa.

REFERENCIAS

INCIBE - Instituto Nacional de Ciberseguridad (https://www.incibe.es/)