CASO PRÁCTICO 1 – REDACCIÓN DE UNA POLÍTICA DE SEGURIDAD

CONTEXTO

Imagina que redactas estas políticas desde el equipo de seguridad de la universidad, así que por lo menos tienes que distinguir tres roles: estudiantes, personal docente e investigador (PDI) y personal de administración y servicios (PAS).

Supón que parte de las infraestructuras y sistemas de información están en un centro de datos local (la plataforma de Aula Virtual, MyApps y el directorio de usuarios) y que lo demás se consume a proveedores en la nube (a través de O365: correo electrónico, Teams u otros como sistemas para matriculación, nóminas, etc.). Además, la universidad proporciona portátiles al PAS y permite al profesorado y al PAS trabajar con sus propios teléfonos móviles ya que no se les proporciona ninguno corporativo.

FORMA DE TRABAJAR

En equipos de cuatro personas (dos parejas de prácticas, por ejemplo), yo os asigno la política que tenéis que redactar y entregarme.

Alternativas para realizar el caso

P.1.1 Formación y concienciación

Esta política necesita establecer, como mínimo:

Estándares

a. Objetivos del programa de formación y concienciación por rol/responsabilidad y áreas de contenido mínimas por rol/responsabilidad que deben tratarse (matriz de formación y concienciación).
b. Necesidades adicionales de formación y concienciación para ciertos roles específicos.
c. Involucración esperada del personal en las actividades de formación y concienciación (son obligatorias, optativas, hay diferentes oportunidades para realizarlas, etc.); recompensas y política de reconocimiento o sanciones.
d. Involucración esperada de los empleados subcontratados y de otros socios y terceras partes en actividades de formación y concienciación específicas.
e. Temporización recomendada para ciertas actividades (por ejemplo, cuando se contrata a un nuevo empleado, cuando se le promociona, cuando se adquiere un nuevo recurso, cuando se modifica una política importante del modelo de control, etc.).
f. Instrucciones detallas sobre cómo proceder para obtener consejo en materia de ciberseguridad o para notificar necesidades de formación y concienciación específicas que se detecten.

P.1.2 Gestión de recursos humanos y seguridad del personal

Esta política necesita establecer, como mínimo:

Estándares

a. Condiciones de no divulgación para cada nivel de riesgo del personal.
b. Acceptable Use Policy (AUP) o reglas de comportamiento para cada nivel de riesgo del personal (reglas que describen las responsabilidades de los individuos y el comportamiento que se espera de ellos con respecto a los activos y datos de la organización).
c. Lista de conflictos de interés identificados.
d. Si los procesos no están automatizados, pasos necesarios para notificar a las instancias interesadas la terminación de contratos, trasferencia o re-asignación del personal y para devolver llaves, tokens, medios de almacenamiento, terminales móviles, etc.

P.1.3 Protección del entorno físico y ambiental

Esta política debe establecer, como mínimo:

Estándares

a. Lista de roles y responsabilidades que deben ocuparse para poder acceder a los diferentes activos físicos (recursos)
b. Pasos necesarios para solicitar, de manera individual, acceso a activos físicos de manera temporal o permanente.
c. Instrucciones detalladas acerca de cómo y cuándo traspasar los perímetros físicos.
d. Pasos necesarios para entregar, mover y retirar activos físicos de la infraestructura cuando estos procesos requieren traspasar perímetros de seguridad. Será necesario un conjunto específico de instrucciones para los terminales móviles.
e. Pasos necesarios para transportar, manejar y borrar medios de almacenamiento.
f. Instrucciones detalladas acerca de cómo obtener, guardar y gestionar (para renovar o cambiar periódicamente si es necesario) llaves, contraseñas, combinaciones o cualquier otro tipo de credencial física.
g. Pasos necesarios para notificar la pérdida/compromiso/daño de llaves, contraseñas, combinaciones o cualquier otro tipo de credencial física.
h. Instrucciones detalladas acerca de cómo comportarse cuando se activan alarmas relacionadas con la seguridad física.
i. Instrucciones detalladas acerca de cuándo y cómo personas externas y visitantes pueden obtener acceso físico a los diferentes recursos y cuándo y cómo deben ser escoltados para realizar sus labores.
j. Instrucciones detalladas acerca de cómo los diferentes recursos deben estar protegidos ambientalmente (temperatura, humedad, vibraciones, polvo, etc.).

P.1.4 IAAA y control de accesos

Esta política debería establecer, como mínimo:

Estándares

a. Instrucciones detalladas acerca de cuándo y cómo bloquear y cerrar sesión en diferentes activos.
b. Pasos necesarios para establecer y mantener una contraseña fuerte.
c. Instrucciones detalladas acerca de cuándo es necesario establecer y mantener contraseñas diferentes para entornos seguros e inseguros.
d. Pasos necesarios para obtener, mantener, refrescar, etc. otros tipos de autenticadores.
e. Prácticas específicas para acceder a activos utilizando terminales móviles (criptografía, conexión de red, etc.).
f. Pasos necesarios para notificar contraseñas y/o autenticadores perdidos, comprometidos o dañados.
g. Pasos necesarios para solicitar modificaciones en cuentas, usuarios, roles, privilegios, permisos y capacidades.

P.1.5 Protección de datos y seguridad de la información

Esta política debe establecer, como mínimo:

Estándares

a. Categorías de datos.
b. Lista de roles y responsabilidades que pueden acceder a las diferentes categorías de datos
c. Pasos necesarios para solicitar, individualmente, permisos adicionales tanto temporales como permanentes.
d. Instrucciones detalladas acerca de cuándo, dónde y cómo deben cifrarse/descifrarse los datos.
e. Cuando se requiere intervención del usuario (idealmente, esto debería ser automático), instrucciones detalladas sobre los mecanismos criptográficos que se aceptan dependiendo de la categoría de los datos: función hash, algoritmo, longitud de clave etc.
f. Prácticas específicas de “mesa limpia”.
g. Prácticas específicas para evitar que se espíe a los empleados por encima del hombro (recomendaciones para la ubicación de los monitores y teclados, para utilizar terminales móviles, etc.).
h. Prácticas específicas para destruir documentos impresos.
i. Medios y servicios de almacenamiento autorizados/prohibidos y prácticas específicas para almacenar datos en ellos, para transportarlos y para utilizarlos.
j. Cuando se requiera la intervención del usuario (idealmente, esto debería esta automatizado), instrucciones detalladas para evitar o eliminar metadatos de distintos tipos de documentos, imágenes y ficheros.

P.1.6 Respuesta ante incidentes

Esta política necesita establecer:

Estándares

a. Actividades de respuesta a incidentes por rol/responsabilidad y por tipo de incidente.
b. Formación en respuesta a incidentes necesaria para cada rol/responsabilidad.
c. Temporización recomendada (o plazos) u obligatoria para ciertas actividades específicas.
d. Procedimientos para operar ciertos activos específicos en modelo manual, con todas sus conexiones con el exterior interrumpidas, hasta que se puedan recuperar condiciones de operación seguras en todos los aspectos.

e. Instrucciones detalladas acerca de cómo proceder para obtener consejo acerca de la respuesta a incidentes o para notificar aspectos relacionados con incidentes (que estén ocurriendo en el presente o ya pasados).
f. Procedimiento de comunicación y listado de personal con el que contactar en el caso de un incidente incluyendo fabricantes, administradores, personal de soporte, etc.

P.1.7 Bring Your Own Device (BYOD)

Esta política necesita establecer:

Estándares

a. Formas de solicitar el uso de BYOD, de ponerlo en marcha y de informar cuándo un dispositivo se ha perdido, robado o ha sido comprometido.
b. Lista de escenarios en los que el dispositivo del usuario podría ser borrado de manera remota.
c. Soporte por parte del departamento TI.
d. Lista de aplicaciones obligatorias: navegador, gestor de email, mensajería instantánea, anti-malware, firewall personal, etc.
e. Lista de aplicaciones y prácticas prohibidas (por ejemplo, jailbreak o root).
f. Lista de app stores permitidas.
g. Instrucciones para configurar las aplicaciones de manera segura.
h. Instrucciones para limitar el acceso al dispositivo (PIN, biometría, etc.).
i. Instrucciones para bloquear el dispositivo tras un tiempo de inactividad.
j. Instrucciones de conectividad (configuración de WiFi, Bluetooth).
k. Instrucciones sobre actualización de SO y aplicaciones.
l. Lista de formas de acceso permitidas a los datos de la organización (cifrado, almacenamiento).