ID	Nombre del Caso de Prueba	Tipo de Prueba	Categoría	Descripción/Resultado Esperado			
F-001	Login Exitoso	Funcional	Acceso	El usuario con rol "Funcionario" ingresa sus credenciales válidas y es redirigido a la pantalla principal de la Intranet.			
F-002	Búsqueda Documental	Funcional	Gestión Documental	Al buscar un término ("Protocolo COVID") en el repositorio, se muestra el documento relevante en menos de 2 segundos.			
F-003	Publicación de Comunicado	Funcional	Comunicados	El usuario con rol "Directivo" publica un comunicado; este aparece inmediatamente en la pantalla principal de todos los usuarios.			
F-004	Acceso Restringido	Funcional	Roles	Un usuario con rol "Funcionario" intenta acceder a la funcionalidad de "Carga Masiva de Documentos Internos" (solo para Subdirección). El sistema debe denegar el acceso con un mensaje de error.			
F-005	Visualización de Calendario	Funcional	Calendarización	El funcionario verifica que el calendario institucional muestra la vista mensual por defecto y refleja una reunión reciente.			
F-006	Revisión de Días Restantes	Funcional	Perfil de Usuario	El usuario ingresa a su perfil y verifica que los datos de "Días Administrativos y Vacaciones" son personalizados y están actualizados.			
F-007	Carga Individual de Documento	Funcional	Carga de Documentos	El usuario con rol "Subdirección" carga un archivo PDF de menos de 5MB. El documento debe aparecer en el repositorio con la fecha y el nombre del autor registrados.			
F-008	Eliminación de Documento	Funcional	Carga de Documentos	El usuario autorizado elimina un documento obsoleto. El documento desaparece del repositorio y se registra el evento en el log de auditoría.			
F-009	Acceso a Manual de Usuario	Funcional	Usabilidad	El usuario hace clic en el enlace del manual de usuario digital desde la pantalla principal, y este se abre correctamente en versión Web o PDF.			
F-010	Logout del Sistema	Funcional	Acceso	El usuario hace clic en "Cerrar Sesión". El sistema lo desconecta y lo devuelve a la pantalla de login.			

ID	Nombre del Caso de Prueba	Tipo de Prueba	Categoría	Descripción/Resultado Esperado			
U-001	Validación de Credenciales	Unitaria	Login	El método `validarCredenciales(usuario, clave)` debe retornar `true` solo para la combinación usuario/clave correcta en la base de datos.			
U-002	Formato de Fecha	Unitaria	Calendario	El método `formatearFecha(timestamp)` debe convertir un timestamp a formato DD-MM-AAAA.			
U-003	Cálculo de Días Restantes	Unitaria	Vacaciones	La función `calcularDias(tomados, totales)` con entrada (5, 15) debe retornar el valor 10.			
U-004	Permiso de Rol	Unitaria	Roles	El método `verificarPermiso(rol_id, funcion_id)` para "Funcionario" y "EliminarDoc" debe retornar `false`.			

ID	Nombre del Caso de Prueba	Tipo de Prueba	Categoría	Descripción/Resultado Esperado
U-005	URL de Búsqueda	Unitaria	Documental (API)	El *endpoint* de búsqueda \`/api/documentos?query=x\` debe retornar una respuesta HTTP 200 si la búsqueda es exitosa.
U-006	Notificación de Comunicado	Unitaria	Comunicación	El método `generarNotificacion(comunicado)` debe crear un registro en la tabla de notificaciones para todos los usuarios activos.
U-007	Tamaño Máximo Archivo	Unitaria	Carga	La función de validación `verificarTamano(archivo)` debe retornar un error si el archivo excede los 10MB (ejemplo de restricción).
U-008	Validación de Email	Unitaria	Usuario	El método `validarEmail(email)` debe retornar `false` para un email sin "@" (ej. "usuario.cesfam.cl").
U-009	Serialización de Datos	Unitaria	API (Mapeo de Datos)	Un objeto JSON de un documento debe serializarse correctamente al formato de la base de datos (Ej. `fechaCarga` como DateTime).
U-010	Conexión a BD	Unitaria	Configuración (Startup)	El método de inicio de la aplicación `iniciarConexionBD()` debe establecer la conexión y retornar un objeto de conexión válido.

ID Prueba	Nombre del Caso de Prueba	Tipo de prueba	Categoría	Columna 1
S-001	**Inyección SQL (OWASP A03)**	Seguridad (Validación de en	OWASP Top 10	Al intentar ingresar ' OR '1'='1 en el campo de cont
S-002	**XSS Reflejado (OWASP A07)**	Seguridad (Validación de sa	OWASP Top 10	Al ingresar un script malicioso (Ej: <script>alert('X
S-003	**Contraseña Segura**	Seguridad (Autenticación)	ISO 27001 (A.9.2)	El sistema debe rechazar una contraseña de menc
S-004	**Control de Acceso Básico**	Seguridad (Autorización)	ISO 27001 (A.9.4)	Un usuario "Funcionario" intenta acceder a una UI
S-005	**Cifrado en Tránsito**	Seguridad (Confidencialidac	ISO 27001 (A.13.2)	Verificar que todas las comunicaciones de la Intra
S-006	**Manejo de Sesiones**	Seguridad (OWASP A04)	OWASP Top 10	Tras 5 minutos de inactividad, la sesión del usuari
S-007	**Carga de Archivos Maliciosos**	Seguridad (Integridad)	OWASP A01 (Broken Access Cor	Intentar subir un archivo con extensión peligrosa (
S-008	**Exposición de Datos (OWASP A01**	Seguridad (API)	OWASP Top 10	Intentar obtener datos de otro usuario (Ej: días de
S-009	**Fuerza Bruta en Login**	Seguridad (Autenticación)	ISO 27001 (A.9.2)	Intentar 5 inicios de sesión fallidos en 60 segundo
S-010	**Registro de Eventos (Logging)**	Seguridad (Trazabilidad)	ISO 27001 (A.12.4)	Verificar que un evento crítico (Ej: cambio de rol d

Resultado esperado