Base de conocimiento para atención de incidentes

Tipo	Escenario	Fecha	Justificación	Solicitó	Descripción de actividad	Resultado	Observaciones o acciones de mejora
Correctivo	Cambio de Credenciales en Directorio Activo Acceso a VPN	21/11/2024	Robo de equipo	Belén Cruz	Cambiar contraseñas de los sistemas a los que tenía acceso el equipo robado, revocando certificados y accesos a redes del corporativas o VPN	Se protegieron los accesos externos del usuario de esa laptop.	Configurar sincronización automática para evitar perdida de datos. Implementar cifrado completo del disco duro.
Preventivo	Cifrado de Disco	25/02/2025	Evitar sustracción de datos	Alonso Sánchez	Procedimiento de Cifrado de Disco	Implementada como configuración estándar	Ninguna. Acción efectiva al momento.
Preventivo	Sincronización de OneDrive	25/02/2025	Evitar sustracción de datos	Alonso Sánchez	Procedimiento de Sincronización de OneDrive	Implementada como configuración estándar	Ninguna. Acción efectiva al momento.
Preventivos	Instalación de un cable acerado	25/02/2025	Evitar sustracción de datos	Alonso Sánchez	Procedimiento de Instalación de un cable acerado	En progreso	Pendiente de concluir.
Preventivo	Simulación de Phishing	05/12/2024	Un empleado recibió correo aparentemente legítimo, solicitando actualizar contraseña a través de un enlace	Angelica Andrade	Revocar y restablecer credenciales comprometidas	Mitigación de brecha de seguridad por suplantación de identidad.	Capacitar a los empleados en identificar phishing. Evaluación de capacitación de códigos maliciosos