Checklist Onboarding / Offboarding Seguro

Control de accesos para ingreso y salida de personal

DATOS DEL PROCESO

Empleado / Contratista: _____ **Cargo:** _____

Área: _____ **Fecha efectiva:** _____

Responsable TI: _____ **Tipo:** [ ] Ingreso [ ] Salida [ ] Cambio de cargo

ONBOARDING — ACCESOS A CREAR (día de ingreso)

Sistemas y accesos:

- [ ] Crear cuenta de correo corporativo con nombre estándar
- [ ] Agregar a grupos de distribución y calendarios del área
- [ ] Activar MFA en cuenta de correo desde el primer día
- [ ] Crear cuenta en gestor de contraseñas corporativo
- [ ] Provisionar acceso al ERP/CRM con perfil adecuado al cargo
- [ ] Acceso a VPN si trabaja remoto — entregar credenciales y guía de uso
- [ ] Acceso a repositorios de código (si aplica) con permisos específicos al rol
- [ ] Acceso a herramientas de colaboración (Teams / Slack / Drive)
- [ ] Registrar en inventario: equipo asignado, número de serie, IP, fecha de entrega

Capacitación obligatoria el primer día:

- [ ] Entregar y firmar Política de Uso Aceptable de TI
- [ ] Entregar y firmar Política de Contraseñas corporativas
- [ ] Capacitación antiphishing básica (mínimo 15 minutos)
- [ ] Informar quién y cómo reportar incidentes de seguridad
- [ ] Firma de Acuerdo de Confidencialidad (NDA)

OFFBOARDING — REVOCAR EL MISMO DÍA DE LA SALIDA

CRÍTICO: La revocación debe hacerse el mismo día, idealmente antes de que el empleado salga. Accesos no revocados son uno de los vectores de ataque más frecuentes en PYMEs.

Accesos a revocar:

- [ ] Deshabilitar cuenta de correo corporativo (conservar 90 días antes de eliminar)
- [ ] Forzar cierre de sesión en todos los dispositivos (forced sign-out)
- [ ] Eliminar del gestor de contraseñas corporativo
- [ ] Revocar acceso a VPN
- [ ] Revocar acceso a ERP/CRM y sistemas internos
- [ ] Revocar acceso a repositorios de código y pipelines CI/CD
- [ ] Revocar acceso a herramientas de colaboración y drives compartidos
- [ ] Eliminar tokens de API, claves SSH y certificados personales del empleado
- [ ] Revocar acceso físico: tarjeta, código de alarma
- [ ] Cambiar contraseñas de cuentas compartidas que el empleado conocía

Gestión de activos y datos:

- [ ] Recuperar equipo, teclado, mouse, monitor y accesorios corporativos
- [ ] Hacer imagen/backup del equipo antes de borrar
- [ ]

Borrar datos personales del equipo y restablecer a estado de fábrica

- [ ] Transferir archivos de trabajo a reemplazante o supervisor
- [ ] Archivar o redirigir el correo según política interna (mínimo 30 días)
- [ ] Actualizar inventario de activos con la devolución

VALIDACIÓN FINAL

Responsable TI (firma): _____ **Jefatura directa (V°B°):** _____

Fecha de completación: _____

Observaciones: