Políticas de Protección de Datos y Seguridad

El material expone un marco integral de cumplimiento normativo y seguridad de la información (Alineado con la Ley Orgánica de Protección de Datos Personales - LOPDP de Ecuador). Se divide en las siguientes áreas clave:

1. Evaluación de Riesgos y Brechas: Se identifica un nivel de riesgo "Alto" y "Muy Alto" con prioridad de acción "Inmediata" en diversas áreas, destacando la falta de consentimientos (empleados, clientes, datos de salud, biometría), transferencias internacionales no formalizadas, y deficiencias en políticas de contraseñas, BYOD y retención de datos.

2. Controles de Acceso (Lógico y Físico):

- **Gestión de Cuentas:** Prohibición de cuentas compartidas. Se aplica el principio de menor privilegio con revisiones semestrales.
- **Autenticación:** Contraseñas de mínimo 8 caracteres complejos. Uso obligatorio de Autenticación Multifactor (MFA) para accesos remotos y sistemas críticos (ODOO, Alfresco). Las contraseñas caducan cada 3 meses para administradores y cada 6 meses para usuarios finales.
- **Redes:** Implementación de VLANs para segregar redes críticas y creación de redes de invitados.

3. Protección de Datos Específicos:

- **Biometría:** Alta restricción. No se almacenan imágenes (JPEG/PNG), únicamente plantillas numéricas (hash). Las bases de datos deben estar cifradas (AES-256 o superior). Al desvincular a un empleado, la plantilla se elimina de forma segura.
- **Videovigilancia:** Las grabaciones se conservan por 30 días, salvo investigaciones en curso.

4. Gestión de la Información y Dispositivos:

- **Respaldos:** Automatizados en la nube y manuales semanalmente en Google Drive. Se exige doble copia (nube/local), cifrado para datos sensibles y pruebas de restauración cada 6 meses.
- **Dispositivos Móviles (BYOD):** Obligatoriedad de MDM para dispositivos con la app corporativa (FALCO), permitiendo borrado remoto y cifrado. El rastreo GPS se limita estrictamente al horario laboral.

5. Gestión de Incidentes y Terceros:

- **Incidentes:** Reporte inmediato. Si hay riesgo, se debe notificar a la Superintendencia de Protección de Datos en un máximo de **5 días**, y al titular afectado en **3 días** si el riesgo para sus derechos es alto.

- **Encargados (Proveedores):** Es obligatorio firmar un Acuerdo de Encargo de Tratamiento (DPA) que garantice confidencialidad, medidas de seguridad y prohibición de uso de datos para fines propios. No pueden subcontratar sin autorización previa.