PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR-MATRIZ

FACULTAD DE CIENCIAS ADMINISTRATIVAS Y CONTABLES

TRABAJO DE TITULACIÓN PREVIA LA OBTENCIÓN DEL TÍTULO DE MAGÍSTER EN ADMINISTRACIÓN DE EMPRESAS CON MENCIÓN EN GERENCIA DE LA CALIDAD Y PRODUCTIVIDAD

OPTIMIZACIÓN DEL PROCESO DE ALTA Y BAJA DE USUARIOS A TRAVÉS DE LA IMPLEMENTACIÓN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, BASADO EN LA NORMA ISO 27001:2013 EN UNA EMPRESA DE CONSULTORÍA PARA LA INDUSTRIA PETROLERA

WILSON FERNANDO CHANGOLUISA CRIOLLO

DIRECTOR: MGTR. FRANCISCO VARGAS

LÍNEA DE INVESTIGACIÓN: SISTEMAS DE GESTIÓN DE PRODUCCIÓN Y OPERACIONES

QUITO, JULIO 2017

AGRADECIMIENTO

A Dios, por darme la fuerza, salud y vida para afrontar nuevos retos y superarlos con éxito, superando obstáculos y situaciones adversas pero que gracias a la fe y esperanza, no han dejado que me rinda en busca de mi superación.

A la Pontificia Universidad Católica y su Facultad de Ciencias Administrativas y Contables, por brindarme la oportunidad de formar parte de la Vigésima Segunda Promoción de Maestrantes, permitir formarme en sus aulas y ser parte del selecto grupo de profesionales que han podido cursar su carrera profesionales en tan prestigiosa institución.

Al Sr. MGTR. Francisco Vargas Carrión, por su valiosa guía y colaboración para poder culminar con éxito el presente trabajo, cuya apertura para compartir su conocimiento y experiencia, fue aporte indispensable para fortalecer y enriquecer los conocimientos adquiridos en la maestría.

DEDICATORIA

Para Luis Hernán, mi padre, quien me ha enseñado que se puede superar las más duras adversidades y cuyo ejemplo de constancia, valentía y coraje, han sido mi motivación para seguir adelante.

Para María Angelita, mi madre, cuyo amor incondicional es baluarte indispensable en mi vida, es mi fortaleza y mi energía para permitirme llegar cada vez más lejos.

Para Luis Hernán y Marco Patricio, mis hermanos, mejores amigos y ángeles de la guarda, quienes han sido los primeros en apoyarme en mis iniciativas y han estado para levantarme cada vez que la situación ha sido adversa.

Para Milton Daniel, Jonathan Alexis, Mario José y Emily Guadalupe, mis niños, por llenar de alegría mi vida con su compañía, alegría e inocencia.

Para Glenda Maricela y Diana Alexandra, por ser la motivación para culminar con éxito una etapa más de mi vida y no permitir que me rinda tras la búsqueda de mis objetivos.

Para María José y Segundo Xavier, por enseñarme a sonreír nuevamente.

Wilson Fernando.

Tabla de Contenidos

AGRADECIMIENTO ..... **I**
DEDICATORIA ..... **II**
TABLA DE CONTENIDOS ..... **III**
ÍNDICE DE FIGURAS ..... **VII**
ÍNDICE DE TABLAS ..... **XI**
INTRODUCCIÓN ..... **XV**
CAPÍTULO I: PROBLEMA DE INVESTIGACIÓN **1**
1.1 DIMENSIÓN TEMÁTICA 1
1.2 DIMENSIÓN TEMÁTICA 1
1.3 DIMENSIÓN TEMPORAL 2
1.4 PLANTEAMIENTO DEL PROBLEMA 2
1.5 FORMULACIÓN DEL PROBLEMA 9
1.6 SISTEMATIZACIÓN DEL PROBLEMA 9
1.7 GENERAL 10
1.8 ESPECÍFICOS 10
CAPÍTULO II: MARCO TEÓRICO **11**
2.1 GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EMPRESAS DE CONSULTORÍA PARA LA INDUSTRIA PETROLERA 11
2.1.1 Gestión de Seguridad de la Información para Sistemas de Administración de Usuarios. *15*
2.1.2 Gestión de Seguridad de la Información para conexión a redes inalámbricas: *20*
2.1.3 Gestión de Seguridad de la Información para Administración de Centros de Datos: *25*
2.1.4 Gestión de Seguridad de la Información para Sistemas de Control Industrial y Sistemas de Supervisión, Control y Adquisición de Datos (SCADA): *28*
2.2 MODELOS DE GESTIÓN DE SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 34
2.2.1 Familia de Normas ISO 27000. ..... *34*
2.2.2 ITIL V3 (Information Technology Infraestrucure Library - Biblioteca de Infraestructura de Tecnologías de Información) *38*
2.3 MEDICIÓN DEL TIEMPO. 41
2.3.1 Medición del Trabajo. *41*
2.3.1.1 Conceptos Básicos para la Medición del Trabajo *42*

2.3.2 Técnicas de Medición del Trabajo. *43*

2.4 NORMATIVA LEGAL VIGENTE. 46

CAPÍTULO III: DIAGNÓSTICO Y DESARROLLO..... 50

3.1 DIAGNÓSTICO DE LA SITUACIÓN ACTUAL 50

3.1.1 Levantamiento del Proceso "Alta y Baja de Usuarios" *50*

3.1.2 Aplicabilidad de los requisitos de la Norma ISO 27001:2013 al proceso de "Alta y Baja de Usuarios" *63*

3.2 DESARROLLO DE REQUERIMIENTOS APLICABLES DE LA NORMA ISO 27001:2013 AL PROCESO DE "ALTA Y BAJA DE USUARIOS" 126

3.2.1 Acciones Desarrolladas para el Cumplimiento de los requerimientos aplicables de la Norma ISO 27001:2013 al proceso de "Alta y Baja de Usuarios" *126*

3.3 MEDICIÓN DEL TIEMPO DEL PROCESO "ALTA Y BAJA DE USUARIOS"..... 149

3.3.1 Paso 1: Establecer el período de tiempo del que se desea obtener los datos históricos. *153*

3.3.2 Paso 2: Recopilar los registros de datos históricos del período de tiempo a medir. *154*

3.3.3 Paso 3: Ordenar los registros de datos históricos: *155*

3.3.4 Paso 4: Determinar si el tamaño de la muestra es significativa. *162*

3.3.5 Paso 5: Ejecutar el proceso de cálculo. *164*

3.3.6 Paso 6: Presentar y evaluar los resultados. *183*

3.4 RESULTADOS DE LA INVESTIGACIÓN 185

3.4.1 Cumplimiento de Objetivos de Control y Controles Aplicables. *185*

3.4.2 Reducción de Re-procesos por modificación de permisos de usuario. *186*

3.4.3 Mejora de Tiempos en la ejecución de cada subproceso. *186*

CAPÍTULO 4: ANÁLISIS DE RESULTADOS 188

4.1 CUMPLIMIENTO DE OBJETIVOS DE CONTROL Y CONTROLES APLICABLES RESPECTO A LA NORMA ISO 27001:2013. 188

4.2 REDUCCIÓN DE RE-PROCESOS EN LA EJECUCIÓN DE LOS SUBPROCESOS DE "ALTA DE USUARIOS" Y "BAJA DE USUARIOS". 190

4.3 MEJORA DE TIEMPOS EN LA EJECUCIÓN DE LOS SUBPROCESOS DE "ALTA DE USUARIOS" Y "BAJA DE USUARIOS". 193

CAPÍTULO 5: CONCLUSIONES Y RECOMENDACIONES 195

5.1 CONCLUSIONES. 195

5.2 RECOMENDACIONES. 197

BIBLIOGRAFÍA ..... A

ANEXOS 1

ANEXO 1: ISO 27001: 2013 – OBJETIVOS DE CONTROL Y CONTROLES. 1

ANEXO 2: EXTRACTO POLÍTICA DE SISTEMAS (MAR 17 SI PO 002) ACTUALIZADA. 16

ANEXO 3: EXTRACTO POLÍTICA SEGURIDAD DE INFORMACIÓN (MAR 17 SI PO 001) ACTUALIZADA..... 17

ANEXO 4: FLUJOGRAMA DE ESCALAMIENTO Y REPORTE DE EVENTOS QUE AFECTEN A LA SEGURIDAD DE LA INFORMACIÓN. 18

ANEXO 5: ACLARATORIA A LA NORMA UTILIZACIÓN DE DISPOSITIVOS MÓVILES - 3.4 MONITOREO Y CONTROL, CONCEPTO DE "PROPIEDAD DE LA LÍNEA". 19

ANEXO 6: EXTRACTO NORMA UTILIZACIÓN DE DISPOSITIVOS MÓVILES ACTUALIZADA A MARZO DEL 2017. 20

ANEXO 7: EXTRACTO POLÍTICA DE ALTA, BAJA Y MODIFICACIÓN DE USUARIOS, PUNTO 5.2.2, INCLUSIÓN ACTIVIDAD "ENTREGA Y RETIRO EQUIPOS". 21

ANEXO 8: EXTRACTO PROCEDIMIENTO DE GESTIÓN DE ACTIVOS DE IT, 3. RESPONSABILIDADES - RESPONSABLE DE SISTEMAS DE ÁREA: "ACTIVIDADES DE RETIRO DE EQUIPOS". 22

ANEXO 9: CAPTURA PANTALLA SISTEMA DE INVENTARIOS – REPORTE DE ACTIVOS ECUADOR. 23

ANEXO 10: PLANILLA DE ASIGNACIÓN / RETIRO DE EQUIPOS ACTUALIZADA A MARZO 2017. 24

ANEXO 11: CAPTURA PANTALLA FORMULARIO DE REGISTRO DE EQUIPOS EN INTRANET CORPORATIVA. .. 25

ANEXO 12: EXTRACTO PROCEDIMIENTO DE GESTIÓN DE ACTIVOS DENTRO DEL PUNTO QUE CITA LAS ACTIVIDADES DE COMUNICACIÓN SOBRE EL BUEN USO DE LOS ACTIVOS. 26

ANEXO 13: EXTRACTO PROCEDIMIENTO DE GESTIÓN DE ACTIVOS – ACTIVIDADES DE CONTROL SOBRE EL BUEN USO DE LOS ACTIVOS. 27

ANEXO 14: MATRIZ DE SOFTWARE ESTÁNDAR PARA ECUADOR. 28

ANEXO 15: LISTADO DE PERFILES DE USUARIO (PRIVILEGIOS) PARA ECUADOR. 29

ANEXO 16: CLASIFICACIÓN DE INFORMACIÓN. 30

ANEXO 17: CONTROLES DE SEGURIDAD. 31

ANEXO 18: ACCESO A ÁREAS RESTRINGIDAS. 32

ANEXO 19: MATRIZ DE PERFILES DE USUARIO. 33

ANEXO 20: ASIGNACIÓN DE CREDENCIALES DE ACCESO. 35

ANEXO 21: EXTRACTO PROCEDIMIENTO DE GESTIÓN DE ACTIVOS DE IT, 3. RESPONSABILIDADES - RESPONSABLE DE SISTEMAS DE ÁREA: "CONTROL DE ACTIVOS". 36

ANEXO 22: EXTRACTO POLÍTICA DE ALTA, BAJA Y MODIFICACIÓN DE USUARIOS, INCLUSIÓN ACTIVIDAD "COMPROMISO DE LOS USUARIOS". 37

ANEXO 23: FORMATO DE MATRIZ DE REGISTRO DE TIEMPOS PARA EL SUBPROCESO ALTA DE USUARIOS. . 38

ANEXO 24: FORMATO DE MATRIZ DE REGISTRO DE TIEMPOS PARA EL SUBPROCESO BAJA DE USUARIOS. .. 40

ANEXO 25: TABLA DE VALORES ESTÁNDAR DE LA DISTRIBUCIÓN DE GAUSS. 42

ANEXO 26: MATRIZ CON ACTIVIDADES IDENTIFICADAS EN EL SUBPROCESO DE "ALTA DE USUARIOS". 43

ANEXO 27: MATRIZ CON ACTIVIDADES IDENTIFICADAS EN EL SUBPROCESO DE "BAJA DE USUARIOS". 44

ANEXO 28: UNIFICACIÓN REGISTROS CON MATRIZ CON ACTIVIDADES IDENTIFICADAS EN EL SUBPROCESO DE "ALTA DE USUARIOS". 45

ANEXO 29: UNIFICACIÓN REGISTROS CON MATRIZ CON ACTIVIDADES IDENTIFICADAS EN EL SUBPROCESO DE "BAJA DE USUARIOS". 48

ANEXO 30: MATRIZ DE REGISTRO DE TIEMPOS PARA EL SUBPROCESO ALTA DE USUARIOS. 52

ANEXO 31: MATRIZ DE REGISTRO DE TIEMPOS PARA EL SUBPROCESO BAJA DE USUARIOS. 57

ÍNDICE DE FIGURAS

FIGURA N° 1: ADAPTACIÓN DEL ORGANIGRAMA EMPRESARIAL 3
FIGURA N° 2: PROCESOS PRIORITARIOS ATENDIDOS POR EL ÁREA DE HELP DESK 4
FIGURA N° 3: REGISTROS DE ALTA Y BAJA DE USUARIOS (PERÍODO JULIO 2015 – JUNIO 2016) 5
FIGURA N° 4: REGISTROS DE MODIFICACIONES A USUARIOS (PERÍODO JULIO 2015 – JUNIO 2016)..... 6
FIGURA N° 5: ACCIONES PARA MITIGAR AMENAZAS 12
FIGURA N° 6: ADAPTACIÓN PROCESO ADMINISTRACIÓN DE USUARIOS (ALTA DE USUARIO) 17
FIGURA N° 7: ADAPTACIÓN NIVELES DE CLASIFICACIÓN DE LA INFORMACIÓN POR PAÍSES 19
FIGURA N° 8: ESQUEMA BÁSICO FUNCIONALIDAD DE UN FIREWALL 21
FIGURA N° 9: ADAPTACIÓN DE DIAGRAMA DE SEGMENTACIÓN DE REDES 24
FIGURA N° 10: PORCENTAJE DE DISPONIBILIDAD DE CENTRO DE DATOS APLICANDO LA NORMA TIA 942 – A 1..... 26
FIGURA N° 11: ESQUEMA DE UN SISTEMA SCADA. 29
FIGURA N° 12: PANEL VIEW SCADA EN ESTACIÓN DE PRODUCCIÓN 31
FIGURA N° 13: ADAPTACIÓN NORMA ISO 27001:2013 ENMARCADA EN EL CICLO DE DEMING (PDCA)..... 37
FIGURA N° 14: ADAPTACIÓN DEL CICLO DE VIDA DEL SERVICIO 39
FIGURA N° 15: REQUISITOS DE GESTIÓN DE SEGURIDAD DENTRO DE LA OPERACIÓN DEL SERVICIO EN ITIL V3 40
FIGURA N° 16: ADAPTACIÓN DE LA REPRESENTACIÓN ESQUEMÁTICA DE LOS ELEMENTOS DE UN PROCESO EN BASE A LA NORMA ISO 9001:2015 51
FIGURA N° 17: CARACTERIZACIÓN DEL SUBPROCESO DE ALTA DE USUARIOS 52
FIGURA N° 18: ESQUEMA DE ALTA DE USUARIO A NIVEL CORPORATIVO..... 53
FIGURA N° 19: DIAGRAMA DE FLUJO DEL SUBPROCESO DE ALTA DE USUARIOS 54
FIGURA N° 20: CARACTERIZACIÓN DEL SUBPROCESO DE BAJA DE USUARIOS 56
FIGURA N° 21: ESQUEMA DE BAJA DE USUARIO A NIVEL CORPORATIVO 57
FIGURA N° 22: DIAGRAMA DE FLUJO DEL SUBPROCESO DE BAJA DE USUARIOS 58
FIGURA N° 23: CARACTERIZACIÓN DEL SUBPROCESO DE MODIFICACIÓN DE PERMISOS DE USUARIO 60
FIGURA N° 24: DIAGRAMA DE FLUJO DEL SUBPROCESO DE MODIFICACIÓN PERMISOS DE USUARIO 61
FIGURA N° 25: RESULTADOS OBJETIVOS DE CONTROL Y CONTROLES APLICADO AL PROCESO DE ALTA Y BAJA DE USUARIOS 96

FIGURA N° 26 RESULTADOS OBJETIVOS DE CONTROL Y CONTROLES QUE CUMPLE EL PROCESO DE ALTA Y BAJA DE USUARIOS 126
FIGURA N° 27: DIAGRAMA DE FLUJO DEL PROCESO DE ALTA DE USUARIOS ACTUALIZADO LUEGO DE LA IMPLEMENTACIÓN DE LA MATRIZ DE PERFILES DE USUARIO 151
FIGURA N° 28: DIAGRAMA DE FLUJO DEL PROCESO DE BAJA DE USUARIOS ACTUALIZADO LUEGO DE LA IMPLEMENTACIÓN DE MATRIZ DE PERFILES DE USUARIO..... 152
FIGURA N° 29: PERÍODO DE MEDICIÓN DEL TRABAJO DEL PROCESO DE ALTA Y BAJA DE USUARIOS ANTES Y DESPUÉS DE APLICAR LA MATRIZ DE PERFILES DE USUARIO 153
FIGURA N° 30: PANTALLA CON DATOS HISTÓRICOS DEL SUBPROCESO DE ALTA DE USUARIOS OBTENIDOS DEL SISTEMA DE GESTIÓN DE INCIDENTES DE LA EMPRESA DE SERVICIOS DE CONSULTORÍA PARA LA INDUSTRIA PETROLERA. (CAPTURA DE PANTALLA DEL SISTEMA DE GESTIÓN DE INCIDENTES)..... 155
FIGURA N° 31: TIEMPO REGISTRADO PARA CULMINAR EL SUBPROCESO DE ALTA DE USUARIOS MEDIDO EN HORAS ANTES DE REALIZAR CAMBIOS EN EL FLUJOGRAMA..... 165
FIGURA N° 32: TIEMPO REGISTRADO PARA CULMINAR EL SUBPROCESO DE ALTA DE USUARIOS PARA USUARIOS DE TIPO 1, MEDIDO EN HORAS ANTES DE REALIZAR CAMBIOS EN EL FLUJOGRAMA 166
FIGURA N° 33: TIEMPO REGISTRADO PARA CULMINAR EL SUBPROCESO DE ALTA DE USUARIOS PARA USUARIOS DE TIPO 2, MEDIDO EN HORAS ANTES DE REALIZAR CAMBIOS EN EL FLUJOGRAMA. 166
FIGURA N° 34: TIEMPO REGISTRADO PARA CULMINAR EL SUBPROCESO DE ALTA DE USUARIOS PARA USUARIOS DE TIPO 3, MEDIDO EN HORAS ANTES DE REALIZAR CAMBIOS EN EL FLUJOGRAMA 167
FIGURA N° 35: COEFICIENTE DE VARIACIÓN DE LOS DATOS PARA LOS TRES TIPOS DE USUARIO ANTES DE APLICAR CAMBIOS EN EL FLUJOGRAMA DEL SUBPROCESO DE ALTA DE USUARIOS. 168
FIGURA N° 36: TIEMPO REGISTRADO PARA CULMINAR EL SUBPROCESO DE ALTA DE USUARIOS MEDIDO EN HORAS DESPUÉS DE REALIZAR CAMBIOS EN EL FLUJOGRAMA. 169
FIGURA N° 37: TIEMPO REGISTRADO PARA CULMINAR EL SUBPROCESO DE ALTA DE USUARIOS PARA USUARIOS DE TIPO 1, MEDIDO EN HORAS DESPUÉS DE REALIZAR CAMBIOS EN EL FLUJOGRAMA. 170
FIGURA N° 38: TIEMPO REGISTRADO PARA CULMINAR EL SUBPROCESO DE ALTA DE USUARIOS PARA USUARIOS DE TIPO 2, MEDIDO EN HORAS DESPUÉS DE REALIZAR CAMBIOS EN EL FLUJOGRAMA. 170
FIGURA N° 39: TIEMPO REGISTRADO PARA CULMINAR EL SUBPROCESO DE ALTA DE USUARIOS PARA USUARIOS DE TIPO 3, MEDIDO EN HORAS DESPUÉS DE REALIZAR CAMBIOS EN EL FLUJOGRAMA. 171
FIGURA N° 40: COEFICIENTE DE VARIACIÓN DE LOS DATOS PARA LOS TRES TIPOS DE USUARIO DESPUÉS DE APLICAR CAMBIOS EN EL FLUJOGRAMA DEL SUBPROCESO DE ALTA DE USUARIOS..... 172

FIGURA N° 41: TIEMPO REGISTRADO PARA CULMINAR EL SUBPROCESO DE BAJA DE USUARIOS MEDIDO EN HORAS ANTES DE REALIZAR CAMBIOS EN EL FLUJOGRAMA..... 174
FIGURA N° 42: TIEMPO REGISTRADO PARA CULMINAR EL SUBPROCESO DE BAJA DE USUARIOS PARA USUARIOS DE TIPO 1, MEDIDO EN HORAS ANTES DE REALIZAR CAMBIOS EN EL FLUJOGRAMA. 175
FIGURA N° 43: TIEMPO REGISTRADO PARA CULMINAR EL SUBPROCESO DE BAJA DE USUARIOS PARA USUARIOS DE TIPO 2, MEDIDO EN HORAS ANTES DE REALIZAR CAMBIOS EN EL FLUJOGRAMA. 175
FIGURA N° 44: TIEMPO REGISTRADO PARA CULMINAR EL SUBPROCESO DE BAJA DE USUARIOS PARA USUARIOS DE TIPO 3, MEDIDO EN HORAS ANTES DE REALIZAR CAMBIOS EN EL FLUJOGRAMA. 176
FIGURA N° 45: COEFICIENTE DE VARIACIÓN DE LOS DATOS PARA LOS TRES TIPOS DE USUARIO ANTES DE APLICAR CAMBIOS EN EL FLUJOGRAMA DEL SUBPROCESO DE BAJA DE USUARIOS. 177
FIGURA N° 46: TIEMPO REGISTRADO PARA CULMINAR EL SUBPROCESO DE BAJA DE USUARIOS MEDIDO EN HORAS DESPUÉS DE REALIZAR CAMBIOS EN EL FLUJOGRAMA. 178
FIGURA N° 47: TIEMPO REGISTRADO PARA CULMINAR EL SUBPROCESO DE BAJA DE USUARIOS PARA USUARIOS DE TIPO 1, MEDIDO EN HORAS DESPUÉS DE REALIZAR CAMBIOS EN EL FLUJOGRAMA. 179
FIGURA N° 48: TIEMPO REGISTRADO PARA CULMINAR EL SUBPROCESO DE BAJA DE USUARIOS PARA USUARIOS DE TIPO 2, MEDIDO EN HORAS DESPUÉS DE REALIZAR CAMBIOS EN EL FLUJOGRAMA. 179
FIGURA N° 49: TIEMPO REGISTRADO PARA CULMINAR EL SUBPROCESO DE BAJA DE USUARIOS PARA USUARIOS DE TIPO 3, MEDIDO EN HORAS DESPUÉS DE REALIZAR CAMBIOS EN EL FLUJOGRAMA. 180
FIGURA N° 50: COEFICIENTE DE VARIACIÓN DE LOS DATOS PARA LOS TRES TIPOS DE USUARIO DESPUÉS DE APLICAR CAMBIOS EN EL FLUJOGRAMA DEL SUBPROCESO DE BAJA DE USUARIOS..... 181
FIGURA N° 51: PORCENTAJE DE REDUCCIÓN DE TIEMPO EN EL SUBPROCESO DE ALTA DE USUARIOS 187
FIGURA N° 52: PORCENTAJE DE REDUCCIÓN DE TIEMPO EN EL SUBPROCESO DE BAJA DE USUARIOS 187
FIGURA N°53: PORCENTAJE DE CUMPLIMIENTO DE OBJETIVOS MENSUAL (DICIEMBRE 2016 – MARZO 2017) 189
FIGURA N°54: AVANCE MENSUAL DE CUMPLIMIENTO DE OBJETIVOS DE CONTROL Y CONTROLES DE LA NORMA ISO 27001:2013 (DICIEMBRE 2016 – MARZO 2017) 189
FIGURA N° 55: NÚMERO DE ALTAS, BAJAS Y MODIFICACIÓN DE USUARIOS PARA EL PERÍODO AGOSTO 2016 – ABRIL 2017 190
FIGURA N° 56: REPROCESO EN PERMISOS DE USUARIO POR ASIGNACIÓN ERRÓNEA O PERMISOS ADICIONALES EN EL PERÍODO ENERO 2016 – ABRIL 2017 191

FIGURA N° 57: MEDIA DEL TIEMPO DE EJECUCIÓN DEL SUBPROCESO DE ALTA DE USUARIOS (TIEMPO EN HORAS)..... 193
FIGURA N° 58: MEDIA DEL TIEMPO DE EJECUCIÓN DEL SUBPROCESO DE BAJA DE USUARIOS (TIEMPO EN HORAS)..... 194

ÍNDICE DE TABLAS

Tabla N° 1: Proceso alta de usuarios versus Re procesos..... 7
Tabla N° 2: Análisis de re procesos expresado en tiempo y costo 8
Tabla N° 3: Seguridad de la información – Amenazas e Inversiones de Mitigación 11
Tabla N° 4: Actores dentro del proceso de “Alta de Usuarios”..... 55
Tabla N° 5: Actores para Ecuador dentro del proceso de “Alta de Usuarios”..... 55
Tabla N° 6: Actores y Responsabilidades dentro del proceso de “Alta de Usuarios” 59
Tabla N° 7: Actores para Ecuador dentro del proceso de “Alta de Usuarios”..... 59
Tabla N° 8: Actores y Responsabilidades dentro del proceso de “Alta de Usuarios” 62
Tabla N° 9: Actores para Ecuador dentro del proceso de “Alta de Usuarios”..... 62
Tabla N° 10: Análisis de requisitos aplicables para el proceso de “Alta y Baja de Usuarios”. 63
Tabla N° 11: Escalas de Cumplimiento de objetivos respecto a la Norma ISO 27001:2013 para el proceso de “Alta y Baja de Usuarios” 97
Tabla N° 12: A.5 Objetivo de Control - Políticas de Seguridad de la Información aplicable para el proceso de “Alta y Baja de Usuarios”. 97
Tabla N° 13: A.6 Objetivo de Control – Organización de Seguridad de la información aplicable para el proceso de “Alta y Baja de Usuarios”..... 98
Tabla N° 14: A.7 Objetivo de Control – Seguridad de los recursos humanos aplicable para el proceso de “Alta y Baja de Usuarios”..... 102
Tabla N° 15: A.8 Objetivo de Control – Gestión de Activos aplicable para el proceso de “Alta y Baja de Usuarios”..... 104
Tabla N° 16: A.9 Objetivo de Control – Control de Acceso aplicable para el proceso de “Alta y Baja de Usuarios”..... 109
Tabla N° 17: A.10 Objetivo de Control – Criptografía aplicable para el proceso de “Alta y Baja de Usuarios”. 114
Tabla N° 18: A.11 Objetivo de Control – Seguridad física y ambiental aplicable para el proceso de “Alta y Baja de Usuarios”..... 115
Tabla N° 19: A.12 Objetivo de Control – Seguridad Operacional aplicable para el proceso de “Alta y Baja de Usuarios”..... 117
Tabla N° 20: A.13 Objetivo de Control – Seguridad de las comunicaciones aplicable para el proceso de “Alta y Baja de Usuarios”..... 119
Tabla N° 21: A.15 Objetivo de Control – Relación con proveedores aplicable para el proceso de “Alta y Baja de Usuarios”. 121
Tabla N° 22: A.16 Objetivo de Control – Gestión de incidentes de Seguridad de la información aplicable para el proceso de “Alta y Baja de Usuarios”. 124
Tabla N° 23: A.18 Objetivo de Control – Cumplimiento aplicable para el proceso de “Alta y Baja de Usuarios”. 125
Tabla N° 24: Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.5.1.2 Revisión de Políticas de Seguridad de la Información, respecto a la Norma ISO 27001:2013 para el proceso de “Alta y Baja de Usuarios”. 127

Tabla N° 25: Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.6.1.3 Contacto con Autoridades, respecto a la Norma ISO 27001:2013 para el proceso de “Alta y Baja de Usuarios”. 127
Tabla N° 26: Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.6.2.1 Política para dispositivos móviles, respecto a la Norma ISO 27001:2013 para el proceso de “Alta y Baja de Usuarios”. 128
Tabla N° 27: Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.7.2.3 Procesos disciplinarios, respecto a la Norma ISO 27001:2013 para el proceso de “Alta y Baja de Usuarios”. 130
Tabla N° 28: Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.8.1.1 Inventario de activos, respecto a la Norma ISO 27001:2013 para el proceso de “Alta y Baja de Usuarios”. 130
Tabla N° 29: Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.8.1.2 Propiedad de activos, respecto a la Norma ISO 27001:2013 para el proceso de “Alta y Baja de Usuarios”. 131
Tabla N° 30: Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.8.1.3 Uso aceptable de activos, respecto a la Norma ISO 27001:2013 para el proceso de “Alta y Baja de Usuarios”. 132
Tabla N° 31: Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.8.1.4 Regreso de activos, respecto a la Norma ISO 27001:2013 para el proceso de “Alta y Baja de Usuarios”. 134
Tabla N° 32: Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.8.2.1 Clasificación de la Información, respecto a la Norma ISO 27001:2013 para el proceso de “Alta y Baja de Usuarios”. 135
Tabla N° 33: Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.8.2.1 Clasificación de la Información, respecto a la Norma ISO 27001:2013 para el proceso de “Alta y Baja de Usuarios”. 135
Tabla N° 34: Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.9.1.1 Política de Control de Acceso, respecto a la Norma ISO 27001:2013 para el proceso de “Alta y Baja de Usuarios”. ... 136
Tabla N° 35: Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.9.1.2 Acceso a redes y servicios de redes, respecto a la Norma ISO 27001:2013 para el proceso de “Alta y Baja de Usuarios”. . 137
Tabla N° 36: Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.9.2.1 Registro y cancelación de registro de usuario, respecto a la Norma ISO 27001:2013 para el proceso de “Alta y Baja de Usuarios”. 138
Tabla N° 37: Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.9.2.2 Provisión de acceso de usuario, respecto a la Norma ISO 27001:2013 para el proceso de “Alta y Baja de Usuarios”. 138
Tabla N° 38: Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.9.2.5 Revisión de los derechos de acceso de los usuarios, respecto a la Norma ISO 27001:2013 para el proceso de “Alta y Baja de Usuarios”. 139
Tabla N° 39: Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.9.2.6 Eliminación o ajuste de los derechos de acceso, respecto a la Norma ISO 27001:2013 para el proceso de “Alta y Baja de Usuarios”. 140
Tabla N° 40: Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.9.3.1 Uso de la información secreta de autenticación, respecto a la Norma ISO 27001:2013 para el proceso de “Alta y Baja de Usuarios”. 140
Tabla N° 41: Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.9.4.1 Restricción de acceso a sistemas y aplicaciones, respecto a la Norma ISO 27001:2013 para el proceso de “Alta y Baja de Usuarios”. 141

Tabla N° 42: Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.10.1.1 Política sobre el uso de controles criptográficos, respecto a la Norma ISO 27001:2013 para el proceso de “Alta y Baja de Usuarios”. 142
Tabla N° 43: Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.10.1.2 Gestión de claves, respecto a la Norma ISO 27001:2013 para el proceso de “Alta y Baja de Usuarios”. 142
Tabla N° 44: Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones, respecto a la Norma ISO 27001:2013 para el proceso de “Alta y Baja de Usuarios”. 143
Tabla N° 45: Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.11.2.7 Eliminación segura o reutilización del equipo, respecto a la Norma ISO 27001:2013 para el proceso de “Alta y Baja de Usuarios”. 143
Tabla N° 46: Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.12.2.1 Controles contra el malware, respecto a la Norma ISO 27001:2013 para el proceso de “Alta y Baja de Usuarios”. 144
Tabla N° 47: Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.12.5.1 Instalación de software en sistemas operativos, respecto a la Norma ISO 27001:2013 para el proceso de “Alta y Baja de Usuarios”. 145
Tabla N° 48: Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.12.6.2 Restricción en la instalación del software, respecto a la Norma ISO 27001:2013 para el proceso de “Alta y Baja de Usuarios”. 145
Tabla N° 49: Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.13.2.4 Acuerdos de confidencialidad o no divulgación, respecto a la Norma ISO 27001:2013 para el proceso de “Alta y Baja de Usuarios”. 146
Tabla N° 50: Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.16.1.1 Responsabilidades y procedimientos, respecto a la Norma ISO 27001:2013 para el proceso de “Alta y Baja de Usuarios”. 147
Tabla N° 51: Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.16.1.2 Reporte de eventos de seguridad de la información, respecto a la Norma ISO 27001:2013 para el proceso de “Alta y Baja de Usuarios”. 148
Tabla N° 52: Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.16.1.2 Informar sobre las debilidades en la seguridad de la información, respecto a la Norma ISO 27001:2013 para el proceso de “Alta y Baja de Usuarios”. 148
Tabla N° 53: Objetivos de Control y Controles donde la “Matriz de Perfiles de Usuario” cubrió los requisitos especificados. 149
Tabla N° 54: Extracto de registros históricos con datos relevantes obtenidos del Sistema de Gestión de Incidentes. 156
Tabla N° 55: Codificación para el perfil de usuario acorde a su complejidad de permisos de acceso y aplicaciones. 157
Tabla N° 56: Extracto de la unificación registros históricos con clasificación tipo de perfil de usuario. 158
Tabla N° 57: Extracto de actividades identificadas para el subproceso de “Alta de Usuarios”. 159

Tabla N° 58: Extracto de unificación de registros y actividades identificadas para el subproceso de “Alta de Usuarios”. 161
Tabla N° 59: Cálculo de muestra de población significativa para los subprocesos de “Alta de Usuarios” y “Baja de Usuarios”. 163
Tabla N° 60: Identificación de actividades de mayor duración para cada tipo de usuario antes de aplicar cambios en el flujograma del Subproceso de “Alta de Usuarios”..... 167
Tabla N° 61: Identificación de actividades de mayor duración para cada tipo de usuario después de aplicar cambios en el flujograma del Subproceso de “Alta de Usuarios”. 171
Tabla N° 62: Comparación de actividades de mayor duración para cada tipo de usuario antes y después de aplicar cambios en el flujograma del subproceso “Alta de Usuarios”. 173
Tabla N° 63: Identificación de actividades de mayor duración para cada tipo de usuario antes de aplicar cambios en el flujograma del Subproceso de “Baja de Usuarios”. 176
Tabla N° 64: Identificación de actividades de mayor duración para cada tipo de usuario después de aplicar cambios en el flujograma del Subproceso de “Baja de Usuarios”. 180
Tabla N° 65: Comparación de actividades de mayor duración para cada tipo de usuario antes y después de aplicar cambios en el flujograma del subproceso “Baja de Usuarios”. 182
Tabla N° 66: Presentación de resultados y variación en los indicadores del subproceso de “Alta de Usuario”. 183
Tabla N° 67: Presentación de resultados y variación en los indicadores del subproceso de “Baja de Usuario” 184
Tabla N° 68: Porcentaje de cumplimiento de objetivos de control y controles para el proceso de “Alta y Baja de Usuarios” 185
Tabla N° 69: Altas, bajas y modificaciones (reproceso) de usuario para el periodo Enero 2016 Abril 2017.186
Tabla N° 70: Análisis de re procesos expresado en tiempo y costo para el período Enero 2016 – Abril 2017. 192

INTRODUCCIÓN

El presente estudio se enfoca en la optimización del proceso de “Alta y Baja de Usuarios” con el objetivo de reducir el número de re procesos que se presentan en el mismo.

Para ello se aplica los ciento catorce objetivos de control y controles que dicta la Norma ISO 27001:2013, levantamiento del proceso de “Alta y Baja de Usuarios” y sus respectivos subprocesos para poder entender a detalle cada uno de ellos y aplicar sobre los mismos las acciones de mejora que cita la Norma.

Adicional, se realiza el Estudio de Tiempo, desglosando cada subproceso en las actividades que lo componen, para identificar las actividades que mayor tiempo demandan dentro del ciclo del proceso y una vez aplicados los objetivos de control y controles de la Norma ISO 27001:2013 comprobar que la implementación de estos controles aportó a la optimización del tiempo de cada subproceso y por ende del proceso en general.

Todo este estudio está enfocado a una Empresa Multinacional cuya actividad es la Consultoría para la Industria Petrolera y que aplica normativas, políticas y reglamentos que vienen regidos desde su casa matriz para todas sus filiales.

CAPÍTULO I: PROBLEMA DE INVESTIGACIÓN

1.1 Dimensión Temática

En la actualidad existe variedad de políticas, procedimientos y herramientas que permiten salvaguardar la integridad de la información de las empresas, siendo uno de los puntos más vulnerable en esta gestión, la persona quien tiene acceso o administra esta información y la responsable de autorizar el acceso a esta información.

Para mitigar estas vulnerabilidades existen normativas que presentan un compilado de buenas prácticas y requisitos, que pueden aplicarse en cualquier tipo de empresa y que aportan a salvaguardar la información de las mismas, entre ellas se encuentran modelos para la creación de Sistemas de Gestión de Seguridad de la Información como la Norma ISO 27001:2013.

1.2 Dimensión Temática

La investigación se realizará en el proceso de “alta y baja de usuarios” del área de Sistemas de una Empresa, que brinda servicios de consultoría para la industria Petrolera con sede en la ciudad de Quito y que forma parte de un grupo multinacional.

1.3 Dimensión temporal

La investigación se llevará a cabo tomando como referencia los registros estadísticos desde julio del 2015 hasta junio del 2016 y su aplicación para el período del segundo semestre del 2016.

1.4 Planteamiento del Problema

La empresa en la cual se realizará la investigación, es una organización creada en el año 2014, que nace de la necesidad de centralizar los procesos administrativos y de consultoría de tres empresas, cuyas actividades principales son las de: exploración, explotación y desarrollo de yacimientos de petróleo y cuyas actividades iniciaron en el año de 1998.

La centralización y unificación de los procesos administrativos donde se incluye el área de Sistemas de las tres empresas, obligó a que se optimice la administración de todos los procesos asignados a esta área, con el fin de eliminar duplicidad en puestos de trabajo como: jefaturas, supervisiones y coordinaciones, alineando procesos operativos en una sola estructura.

El Departamento de Sistemas está incluido dentro de la Gerencia de Administración y Finanzas de Ecuador y cuya estructura se detalla en la Figura N° 1.

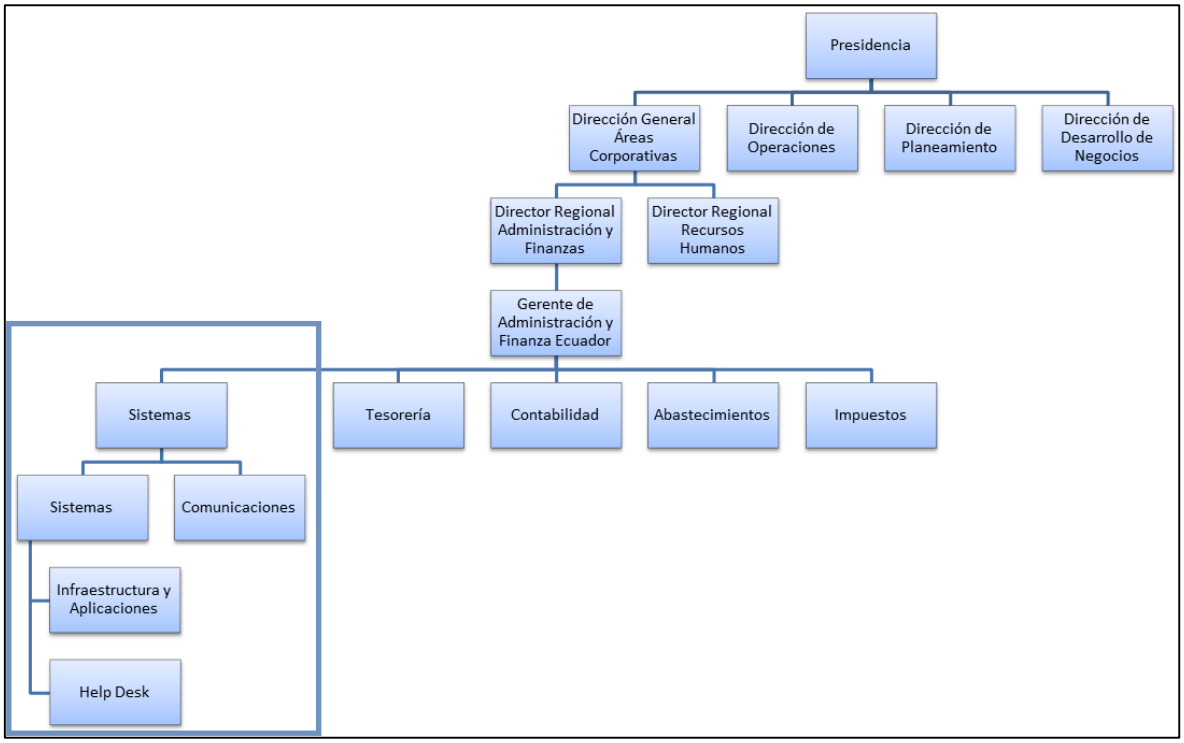


Figura N° 1: Adaptación del Organigrama Empresarial.
Fuente: (Empresa de Consultoría para la Industria Petrolera, 2016).

Como se muestra en la Figura N°1, el Departamento de Sistemas se divide en dos áreas: Sistemas y Comunicaciones. El área de Comunicaciones se dedica exclusivamente a la administración de los enlaces de datos y todo medio de transmisión que utilicen las empresas (telefonía fija, telefonía celular, Internet, red local, red nacional, red internacional).

El área de Sistemas abarca dos sub-áreas que son: Infraestructura y Aplicaciones, que se encarga de velar por el buen funcionamiento de la infraestructura física y aplicaciones de software que dispone la empresa y la sub-área de Help Desk que se encarga del soporte a los usuarios mediante la atención de incidentes de trabajo o tickets (como se los denomina), para que los usuarios puedan realizar sus tareas diarias sin problemas; este servicio es brindado por una tercera empresa externa al grupo, mediante un contrato de

prestación de servicios el cual provee de cuatro ingenieros de soporte para la atención de los usuarios a nivel de Ecuador.

Las tareas del equipo de soporte del área de Help Desk se registran mediante una herramienta de software de control de incidentes o tickets, en el cual mensualmente se obtienen los reportes de las trabajos realizados y tiempo utilizado para la resolución de dicha tarea; el mismo que es evaluado por la Coordinación del área de Sistemas con frecuencia mensual, para conocer si los parámetros de "atención" descritos en el contrato se alcanzaron.

Este parámetro de "atención" es el tiempo que el Ingeniero de Soporte le dedicó a la actividad, siendo su estándar mínimo de 90%, si el parámetro está por debajo, se aplican penalidades a la empresa prestadora del servicio.

En la Figura N° 2 se muestran los procesos que desarrollan los ingenieros de soporte y que se consideran los más prioritarios (catalogados así por la Coordinación del Departamento de Sistemas en base al tiempo que afectaría a un usuario no completarlas en el tiempo establecido):



Figura N° 2: Procesos Prioritarios atendidos por el área de Help Desk.
Fuente: (Empresa de Consultoría para la Industria Petrolera, 2016).

Se cataloga al proceso de “alta y baja de usuarios” como la más crítica y prioritaria, ya que la misma es el inicio de un flujo que permite la creación del usuario para el ingreso a los sistemas de la empresa, asignación de casilla de correo, asignación de equipos, permisos de acceso a repositorios de información, claves para conexión a sistemas de comunicación (telefonía fija, red inalámbrica), activación de tarjetas para ingreso a oficinas.

El no brindar estos accesos al usuario, representa que el mismo no podrá desempeñar sus funciones efectivamente desde la fecha que ingresa a la empresa.

En la Figura N° 3, se detallan las altas y bajas de usuarios registrados desde julio 2015 hasta junio 2016, las mismas corresponden a altas y bajas de personal contratado directamente para la empresa, personal externo a la empresa, personal de organismos de control y pasantes.

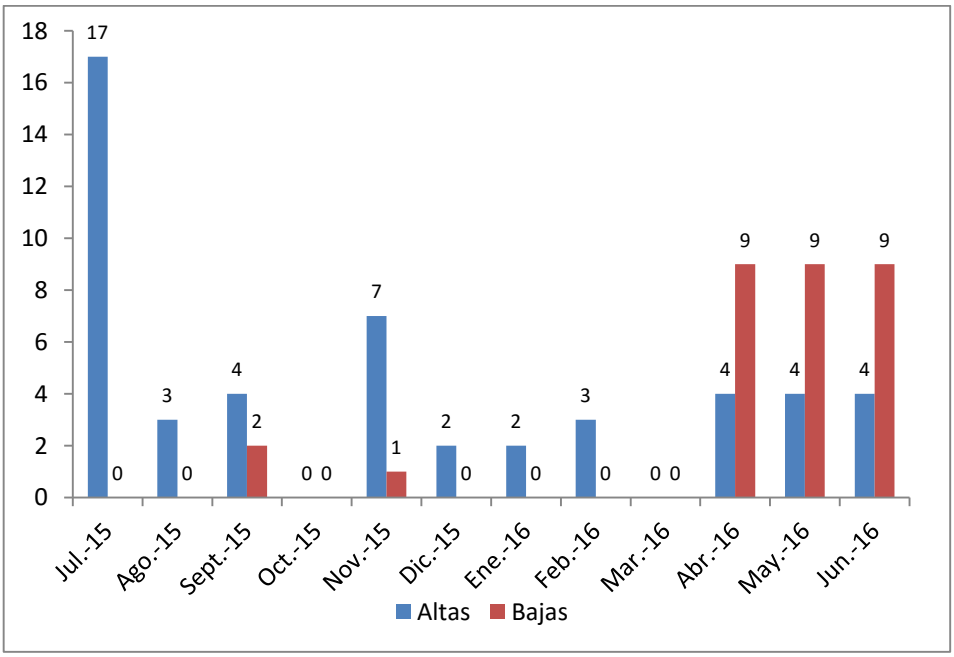


Figura N° 3: Registros de Alta y Baja de Usuarios (Período Julio 2015 – Junio 2016).
Fuente: (Empresa de Consultoría para la Industria Petrolera, 2016).

La Figura N° 4 muestra la cantidad de incidentes resueltos por el área de sistemas (barra verde) para el período de julio 2015 hasta junio 2016, referente a la reasignación de permisos a usuarios para acceder a carpetas compartidas, bloques de información en la intranet o enlaces en la plataforma de SharePoint que maneja la empresa, es decir, re-procesos en la asignación de permisos.

También se muestra las bajas completas para su posterior re-proceso y creación de nuevo usuario (barra azul).

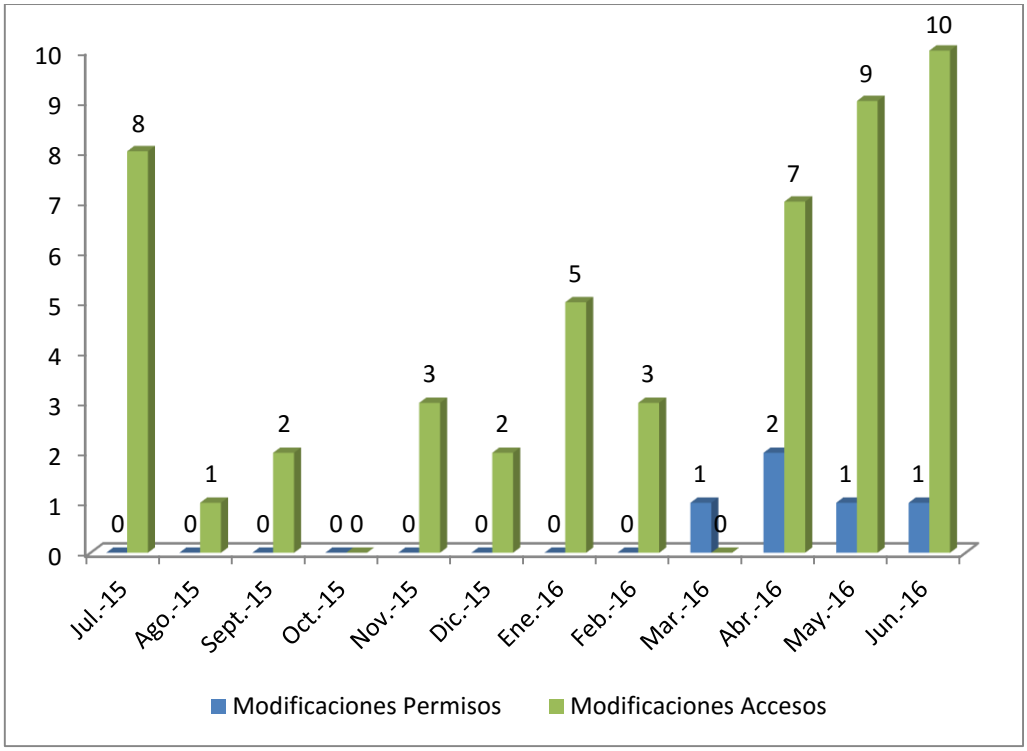


Figura N° 4: Registros de modificaciones a usuarios (Período Julio 2015 – Junio 2016).
Fuente: (Empresa de Consultoría para la Industria Petrolera, 2016).

En la Tabla N° 1, se presentan los niveles de re-procesos de pedidos de alta de usuarios expresados en porcentaje (incluye casos de bajas para reasignación completa de permisos de usuarios)

Tabla N° 1.

Proceso alta de usuarios versus Re procesos

Mes	*Altas*	*Reprocesos*	*Porcentaje*	*Reproceso / Altas*
Jul-15	17	8	47%	0,47
Ago-15	3	1	33%	0,33
Sept-15	4	2	50%	0,50
Oct-15	0	0	0%	0,00
Nov-15	7	3	43%	0,43
Dic-15	2	2	100%	1,00
Ene-16	2	5	250%	2,50
Feb-16	3	3	100%	1,00
Mar-16	0	1	100%	1,00
Abr-16	4	9	225%	2,25
May-16	4	10	250%	2,50
Jun-16	4	11	275%	2,75
Total	50	55	110%	1,10

Nota. Re procesos y ejecución de nuevas altas expresado en escala de 0 a 1. Informes de Gestión de Incidentes de Help Desk. (2016). Registros de Alta y Baja de Usuarios. Ecuador: Empresa de Consultoría para la Industria Petrolera.

Los valores presentados en la Tabla N°1 demuestran un nivel de fallas no aceptable para este proceso (Promedio 110%); estos niveles de re procesos constituyen el problema de estudio y generan los siguientes riesgos:

- Administración de información restringida por usuarios con accesos incorrectos.
- Modificación, eliminación y/o distribución errónea de información sensible.
- Aumento de la carga operativa del personal de sistemas que atiende estos requerimientos.

El aumento en la carga operativa del personal de sistemas y el aumento de frecuencia de revisiones de cumplimiento por parte del área de “Compliance”, que es uno de los efectos de los re procesos y se ejecutan para validar que los usuarios tienen acceso a la

información y aplicaciones que les corresponde, no será objeto de análisis del presente estudio.

En la Tabla N° 2, se realiza el análisis del tiempo y costo invertido en los re procesos de alta de usuarios del período Julio 2015 – Junio 2016; para este cálculo se utilizó el valor hora – técnico contractual de $ 19,50 (USD).

Tabla N° 2:
Análisis de re procesos expresado en tiempo y costo

Mes	*# Altas*	*# Bajas para nuevo permiso*	*Tiempo baja (horas)*	*# Asignación nuevos permisos*	*Tiempo permisos (horas)*	*# Modificación Accesos*	*Tiempo accesos (horas)*	*Esfuerzo total en horas por re proceso*	*Esfuerzo total en USD*
Jul-15	17	0	0	0	0	8	4	4	$ 78,00
Ago-15	3	0	0	0	0	1	0,5	0,5	$ 9,75
Sept-15	4	0	0	0	0	2	1	1	$ 19,50
Oct-15	0	0	0	0	0	0	0	0	-
Nov-15	7	0	0	0	0	3	1,5	1,5	$ 29,25
Dic-15	2	0	0	0	0	2	1	1	$ 19,50
Ene-16	2	0	0	0	0	5	2,5	2,5	$ 48,75
Feb-16	3	0	0	0	0	3	1,5	1,5	$ 29,25
Mar-16	0	1	1	1	2	0	0	3	$ 58,50
Abr-16	4	2	2	2	4	7	3,5	9,5	$ 185,25
May-16	4	1	1	1	2	9	4,5	7,5	$ 146,25
Jun-16	4	1	1	1	2	10	5	8	$ 156,00
Total	83	**5**	**5**	**5**	**10**	**50**	**25**	**40**	**$ 780,00**
Promedio mensual	4,2	0,4		0,4		4,2			$ 65,00

Nota. Esfuerzo total calculado por re procesos y expresado en horas y dólares. Informes de Gestión de Incidentes de Help Desk. (2016). Registros de Alta y Baja de Usuarios. Ecuador: Empresa de Consultoría para la Industria Petrolera.

La empresa considera la necesidad de enfocar una optimización de su proceso de “alta y baja de usuarios” por su impacto interno.

Para esto se implementará los requisitos aplicables que dicta la Norma ISO 27001:2013 al proceso de “alta y baja de usuarios” que administra la empresa en estudio.

Por último, una vez implementados los requisitos aplicables de la Norma ISO 27001:2013, se procederá a medir la variable en estudio en el proceso de “Alta y Baja de Usuarios” cuyo valor actual es del 110% de re procesos y el objetivo de la propuesta sería el de reducir este porcentaje.

1.5 Formulación del Problema

¿La implementación de Gestión de Seguridad de la Información basado en la Norma ISO 27001:2013, permitirá optimizar el desempeño del proceso de “alta y baja de usuarios” de una empresa de consultoría para la industria petrolera?

1.6 Sistematización del Problema

- ¿El aplicar un diagnóstico de la gestión actual del proceso comparados con los requisitos aplicables de la Norma ISO 27001:2013, permitirá identificar los controles de gestión para la mejora del desempeño del proceso?
- ¿El desarrollo e implementación de controles de gestión basada en requerimientos aplicables de la norma ISO 27001:2013, permitirá optimizar el desempeño del proceso de seguridad de la información de “alta y baja de usuarios”?
- ¿La aplicación de controles de gestión basado en requerimientos aplicables de la Norma ISO 27001:2013 mediante el control de la cantidad de re procesos que se realicen en un proceso de “alta y baja de usuarios”, logrará optimizar su desempeño?

1.7 General

Optimizar la Gestión de Seguridad de la Información para el Proceso de “Alta y Baja de Usuarios” en una empresa de Consultoría para la Industria Petrolera basado en la Norma ISO 27001, para reducir el porcentaje de re procesos que actualmente se presentan.

1.8 Específicos

- Diagnosticar la situación actual del proceso de “Alta y Baja de Usuarios” respecto a requisitos aplicables de la norma ISO 27001:2013.
- Optimizar el desempeño del proceso de “Alta y Baja de Usuarios” mediante el desarrollo e implementación de requisitos aplicables de la norma ISO 27001:2013.
- Evaluar la optimización de desempeño del proceso de “Alta y Baja de Usuarios” en base al control de re procesos efectuados, implementados los requisitos aplicables de gestión de seguridad de la información basado en la norma ISO 27001:2013

CAPÍTULO II: MARCO TEÓRICO

2.1 Gestión de Seguridad de la información en empresas de consultoría para la industria petrolera

La gestión de la seguridad de la información dentro de las empresas y específicamente en las empresas relacionadas a la industria petrolera por su nivel de competitividad es un punto muy importante para este tipo de organizaciones, considerando que existen varias aristas en las cuales se aplica está gestión.

La gestión de la seguridad de la información ha tomado gran relevancia considerando las últimas estadísticas de ataques informáticos que se han presentado a nivel mundial, a continuación se resumen los puntos más relevantes sobre esta situación (ver Tabla N° 3):

Tabla N° 3:
Seguridad de la información – Amenazas e Inversiones de Mitigación

Unidades	Detalle
1800	Millones de Virus en la red mundial
180	Mil Programas con Software Malicioso
244	Mil Programas Malware
10	Millones de Paquetes nocivos
8%	De los celulares a nivel mundial están infectados
USD 3500 MM	Se invierten para mitigar las amenazas de seguridad al año en USA
USD 700 M	Se invierten para mitigar las amenazas de seguridad en Latinoamérica

Nota. Cantidades expresadas en miles y millones de dólares.
Fuente: (Level 3, 2016).

Las empresas invierten recursos económicos, humanos y técnicos para contrarrestar estas amenazas que pueden ser: desarrollos tecnológicos en base a hardware o software,

desarrollos procedimentales u organizacionales que abarquen creación o mejora de guías, manuales, reorganización y/o creación de áreas (por ejemplo: áreas dedicadas exclusivamente a la seguridad como Compliance o un área exclusiva de Seguridad de la Información ligada a Tecnología). Estas acciones tienen como fin plantear planes dirigidos a la mitigación de amenazas (ver Figura N° 5).

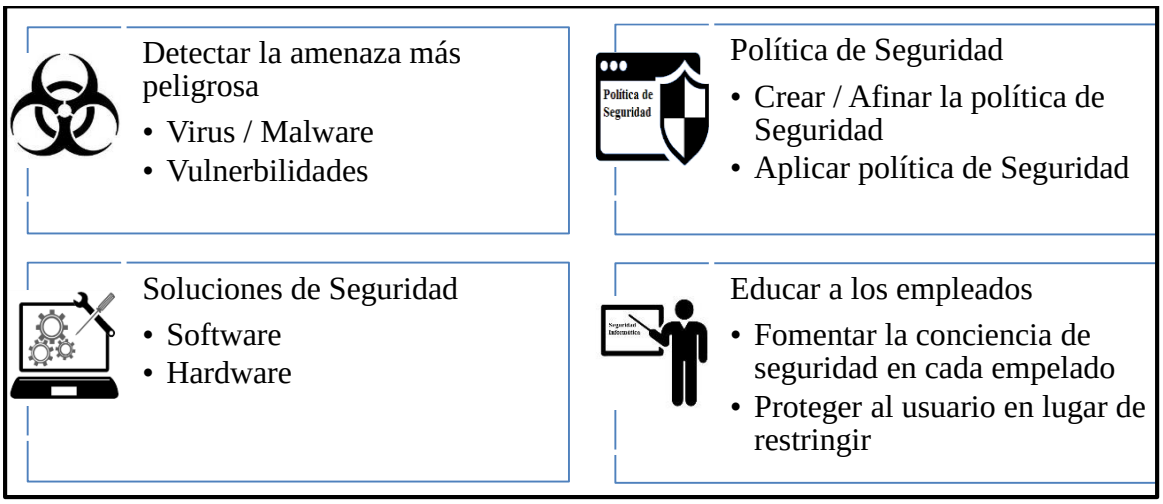


Figura N° 5: Acciones para mitigar amenazas.
Fuente: (Level 3, 2016).

Estas acciones tratan de impedir ataques informáticos que pueden provocar pérdidas económicas, de información, o ambas. Además permiten cerrar brechas y vulnerabilidades que pueden presentarse ya que el 40% de las amenazas causan mayor daño en el día cero (Level 3, 2016).

Se debe considerar que a pesar de que existan controles de seguridad procedimentales, herramientas de hardware y/o software que protegen la infraestructura y seguridad de una empresa y/o áreas enfocadas en la gestión de la seguridad de la información, el punto más vulnerable es el usuario final que accede a la información y puede difundir o publicar en medios no seguros la misma.

Hay que considerar que el 67% de la información empresarial que se filtra hacia la red es realizada por el mismo usuario (PGP Corporation, 2016) de forma accidental en la mayoría de casos, así también existen otros riesgos como:

- Inseguridad en el envío de información.
- Robo (Hacking) de información.
- Bajos niveles de seguridad en políticas de administración de información y comunicaciones.
- Errores humanos.

Por ello, la gestión de usuarios, donde se determinan los permisos, accesos a repositorios de información y a medios de comunicación como: Internet, correo electrónico personal y redes sociales, es primordial al momento de tratar sobre la administración de la seguridad de la información. También se consideran los siguientes lineamientos de seguridad al momento de asignar permisos a un usuario (Level 3, 2016):

- Privacidad del Correo electrónico del usuario con sus requerimientos regulatorios: Asegura que el usuario mientras brinde sus servicios en determinada empresa, tendrá absoluta confidencialidad sobre los datos que él administra, por ejemplo: listado de proveedores, secretos comerciales, entre otros.
- Niveles de acceso autorizados a información crítica del negocio: Sin importar el nivel de jerarquía del usuario, dentro de una organización deben cumplirse políticas de acceso, en especial para los repositorios con información crítica del negocio que estarán restringidos para la mayoría de usuarios.

- Sitio de almacenamiento de la información de un usuario (computador asignado / servidor de archivos / Herramientas en la nube): Dependiendo de la locación donde se encuentre el usuario puede definirse donde almacenará la información correspondiente a sus actividades, por ejemplo: si está en un lugar remoto sin acceso a la red empresarial podrá almacenar localmente en su computador.
- Niveles de Información compartida con terceros: Lo cual define hasta qué punto puede un usuario compartir la información con partes interesadas.

En este escenario, el sector petrolero no es la excepción, considerando el nivel de criticidad e importancia de la información que maneja el mismo como son: datos de exploración, producción y operación, talento humano, datos de proveedores y partes interesadas, datos comerciales y datos legales. Una vulnerabilidad en la Administración de Seguridad de la Información de una empresa, puede convertirse en una potencial fortaleza de otra e incidir incluso en niveles de competitividad.

Los principales campos de Gestión en Administración de Seguridad de la Información para la industria de Producción (donde se enmarca el Sector Petrolero) son:

- Gestión de Seguridad de la Información para Sistemas de Administración de Usuarios.
- Gestión de Seguridad de la Información para conexión a redes inalámbricas.
- Gestión de Seguridad de la Información para Administración de Centros de Datos.
- Gestión de Seguridad de la Información para Sistemas de Control Industrial y Sistemas de Supervisión, Control y Adquisición de Datos (SCADA).

A continuación se detallan los campos de gestión mencionados para la industria de Producción:

2.1.1 Gestión de Seguridad de la Información para Sistemas de Administración de Usuarios.

Permite administrar toda la información referente al personal que brinda sus servicios a una organización. Esto incluye datos personales, profesionales y números de contacto. La divulgación de estos datos puede representar una fuga de información del talento humano que tiene la organización, números de contacto que pueden pasar a formar parte de listados masivos de envío de correo basura (Spam), suplantación de identidad (Phishing), desfalcos, secuestros a aparatos electrónicos y/o pago por rescate (EDIWORLD, 2016).

Mediante un sistema de gestión de seguridad se pueden implementar acciones de control como:

- Administración centralizada y encriptado de la información: Esto permite contar con un único repositorio de información, en el cual se puede controlar el acceso al mismo, otorgar permisos para ver y/o modificar la información que dentro del mismo se almacena, así como llevar un control de cambios (con el registro del usuario que realizo el cambio) de la información.

También permite que la información que puede ser descargada del repositorio, cumpla parámetros de seguridad para su portabilidad y almacenamiento externo, como lo es la encriptación y/o cifrado de datos para hacer frente a un eventual robo, plagio y/o distribución no autorizada de esta información. Con ello, se controla que la información que se descarga no pueda ser abierta en equipos que no pertenecen a la empresa, adjuntada en correos personales o subida a medios de almacenamiento externo o en la nube.

- Procesos de creación, baja y modificación de usuarios: Permite asignar y diferenciar los permisos que tendría un usuario acorde a las funciones, responsabilidades y hasta el área a la cual estará asignado. Esto controla:

    - El nivel de acceso que tiene el mismo (acceso a repositorios de información por área, acceso a información empresarial considerada sensible solo bajo responsabilidad del dueño del repositorio y por un período de tiempo determinado).
    - Aplicaciones a las que tendrá acceso (correo electrónico empresarial, medios de comunicación instantánea empresarial como Microsoft Lync o Skype Empresarial y permisos para conexión a Internet).
    - Equipos que le serán asignados (computador portátil o de escritorio, extensiones telefónicas, equipos de telefonía celular, claves de marcación telefónica: local, nacional, internacional y celulares).
    - Permisos sobre la información a la que podría acceder (ver, modificar o ambos).

- Permite obtener una descripción detallada de la cuenta de usuario, registro de actividades, control del nivel de seguridad de contraseña, control de horas de inicio de sesión de un usuario, habilitar o deshabilitar temporal / definitivamente una cuenta de usuario (Microsoft, 2016).

En la Figura N°6 se muestra una adaptación del Proceso de Administración de Usuarios enfocado específicamente al alta de un usuario que: crea, asigna permisos de acceso y aplicaciones acorde a su perfil.

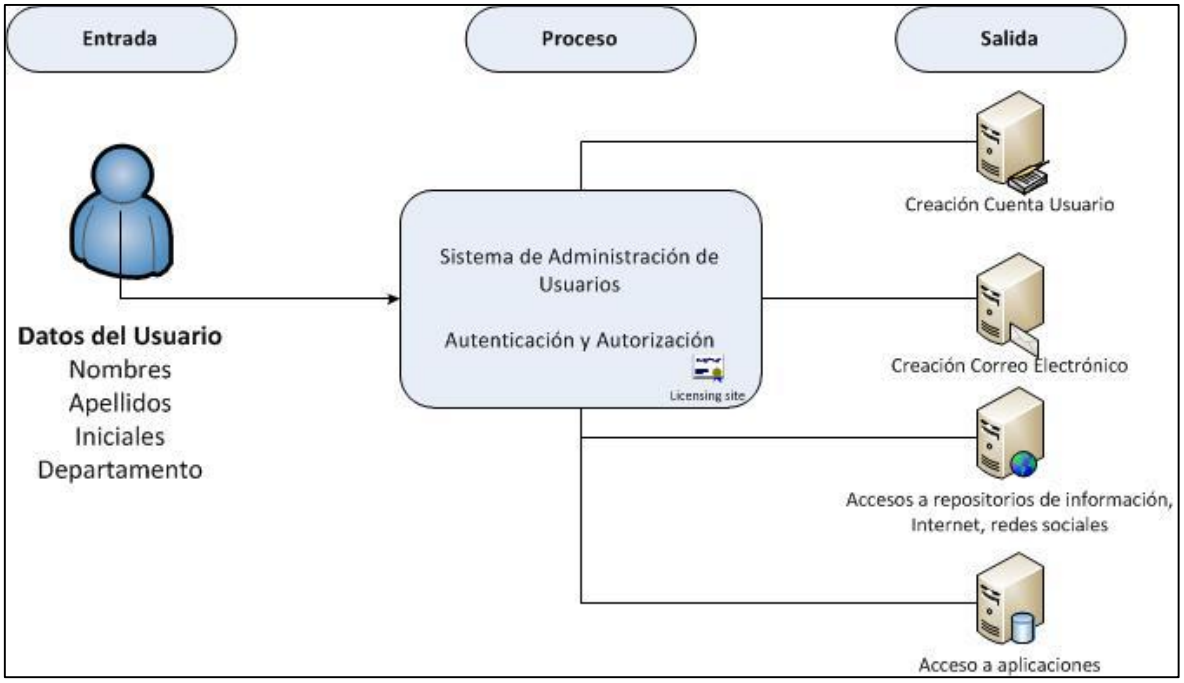


Figura N° 6: Adaptación Proceso Administración de Usuarios (Alta de usuario)
Fuente: (Ingeniería Dric - IDRIC, 2016)

- Flujos de aprobación para asignación y delegación de permisos: Acorde a las funciones que un usuario desempeña dentro de una empresa, el mismo puede interactuar en flujos de aprobación o firma (ejemplo: aprobación de solicitudes de compra, aprobación de planificación de cronogramas de trabajo y/o aprobación de días libres a su equipo de trabajo) y a la par puede ser delegado para actuar en cadenas de aprobación de otras áreas de forma temporal (por

vacaciones o reemplazo) o de forma definitiva (por cambio de funciones o asensos). El no tener delimitado correctamente los permisos puede provocar que un usuario actúe dentro de una cadena de aprobación lo cual puede generar retrasos en su flujo.

- Políticas de seguridad de la información: Esto permite fijar niveles de seguridad a la información que está disponible para los usuarios, la misma puede clasificarse acorde a cada país o empresa. Para el Ecuador la clasificación de la información está definida de la siguiente manera (ver Figura N° 7):

    - Secretísimo.
    - Secreto.
    - Confidencial.
    - Reservado.

Con ello además de restringir los medios por los cuales los usuarios pueden acceder y distribuir la información, también enseña mediante íconos el nivel de importancia que tiene dicha información, además del daño y repercusión que puede tener la divulgación de la misma.

Por último, se incluyen los niveles de autorización que se debe cumplir para que el usuario pueda acceder a la información, así como a los privilegios que tendrá para la misma:

- Lectura.

- Escritura.
- Lectura y Escritura.

País	"Top Secret"	"Secret"	"Confidential"	"Restricted"
Argentina	Estrictamente Secreto y Confidencial	Secreto	Confidencial	Reservado
Australia	Top Secret	Secret	Confidential	Restricted
Bolivia	Supersecreto o Muy Secreto	Secreto	Confidencial	Reservado
Brasil	Ultra Secreto	Secreto	Confidencial	Reservado
Canadá	Top Secret/Très secret défense	Secret/Secret défense	Confidential/ Confidentiel défense	
Chile	Secreto	Secreto	Confidencial	Reservado
Colombia	Ultrasecreto	Secreto	Confidencial	Reservado
Costa Rica	Alto Secreto	Secreto	Confidencial	
Ecuador	Secretisimo	Secreto	Confidencial	Reservado
El Salvador	Ultra Secreto	Secreto	Confidencial	Reservado
España	Secreto	Reservado	Confidencial	Difusión Limitada

Figura N° 7: Adaptación Niveles de Clasificación de la información por países
Fuente: (Departamento de Defensa de los Estados Unidos, 2016)

Además dentro del manejo de información se utilizan normas sobre la difusión de la misma, no solo en el contexto de confidencialidad y seguridad de la información sino también considerando aquella que puede catalogarse como ofensiva, racista, sin base o justificativo que la sustente o que no aporte al desarrollo de sus actividades laborales.

Por último, la administración de seguridad de la información busca restringir los medios no establecidos por la empresa para compartir información, por ello se bloquea el acceso a redes sociales, correos electrónicos no empresariales y medios de almacenamiento en la nube.

También se restringe el uso de las herramientas de hardware o software proporcionados por la empresa para actividades de uso personal, (ejemplos: registrar correos empresariales en redes sociales o suscripciones a páginas de interés personal) bloqueando así el ingreso de software y/o correo malicioso a los servidores empresariales.

2.1.2 Gestión de Seguridad de la Información para conexión a redes inalámbricas:

Este campo busca definir un estándar para la instalación y uso de una solución de conectividad inalámbrica (Wireless - WIFI), con ello propone un esquema que debe contemplar un método de autenticación de usuarios a la red inalámbrica, además de un método de encriptación seguro y eficiente, cuyo algoritmo proporcione la integridad de datos (Cisco Systems, 2016). Para ello existen soluciones de hardware y software que permiten implementar este tipo de controles, entre los más importantes están:

- Administradores de contenido.
- Centros de monitoreo de intrusos.
- Cortafuegos (Firewalls).

La Figura N° 8 muestra un esquema lógico de un equipo Firewall cuyo propósito es bloquear el acceso no autorizado a la red, permitiendo únicamente la entrada y salida de tráfico autorizado.

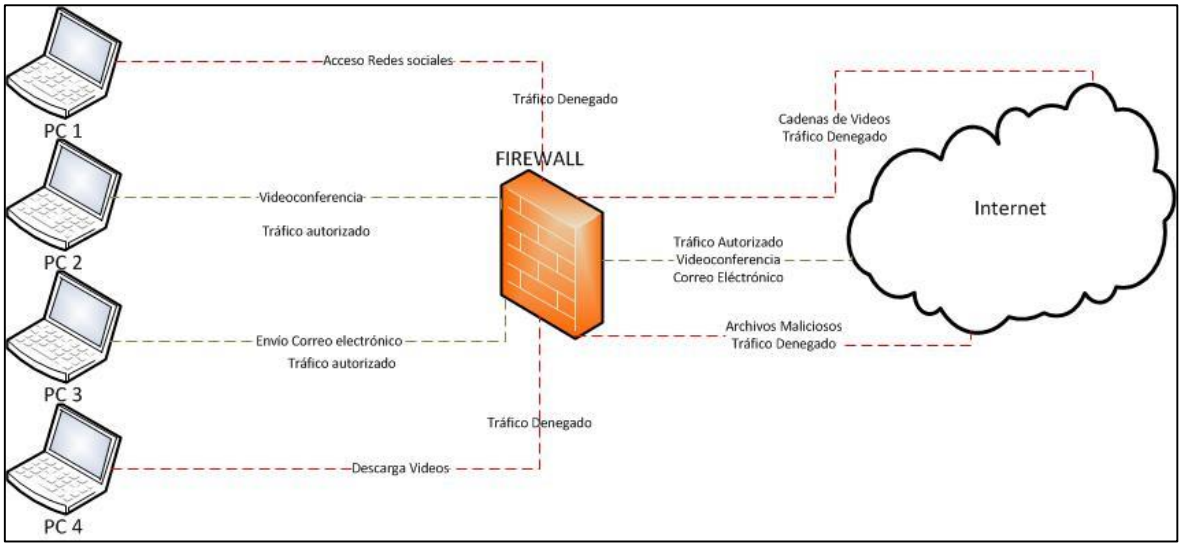


Figura N° 8: Esquema básico funcionalidad de un Firewall
Fuente: (Check Point Software Technologies Ltd., 2016)

Para cumplir con políticas de seguridad de la información en conexiones inalámbricas se deben cubrir los siguientes requisitos:

- Establecer la infraestructura que administrará las conexiones inalámbricas (estándares de hardware y software): Lo cual permite establecer un estándar corporativo en lo que se refiere a infraestructura, software, protocolos de comunicación, protocolos de seguridad, encriptación y cifrado de la comunicación, entre los principales.

  Estas herramientas permiten controlar de manera adecuada y segura la forma de conexión de los usuarios a la red, llevar un registro de conexiones y de intentos de vulnerar la red y la correcta autenticación de los usuarios a la red empresarial. Esto garantiza la integridad de la información que se maneja en la red.

- Establecer los roles y responsabilidades para la administración de las redes inalámbricas (Administrador y operadores): Permitiendo definir un rol único que

administre y otorgue los permisos para que un usuario se conecte a la red corporativa, evitando que la red quede abierta para un ataque o que cualquier usuario pueda acceder a la red corporativa y por ende a sus repositorios de información en línea.

- Definir los perfiles de los usuarios que se conectarán a la red y los permisos que tendrá cada uno: Con esto el administrador de la red, en base al perfil que se le asignó al usuario puede asignar o restringir el acceso a páginas de contenido social, por ejemplo, un administrador de Marketing o Publicidad debería tener acceso a redes sociales con el fin de publicitar la empresa o marca por este medio o con el fin de descargar o subir contenido multimedia (audio, videos, animaciones, entre otros) con el fin de publicitar o promocionar un tema referente a la empresa.

  Por ello, es de vital importancia que los roles de usuarios sean asignados correctamente, evitando brindar acceso no adecuado a usuarios de áreas que no deben interactuar más que con el contenido interno y permitido de la empresa.

- Establecer el protocolo o protocolos de seguridad que debe cumplir la red inalámbrica: Esta medida logra definir los protocolos de red y seguridad que deben utilizarse para la conexión a redes inalámbricas, para lo cual se usan únicamente protocolos certificados y aprobados por entes de control de seguridad. Esto disminuye el riesgo de ingreso se software malicioso a la red empresarial, filtración en la red de usuarios ajenos a la misma, conexión

únicamente de dispositivos calificados y que se cumpla el estándar de comunicaciones.

Adicionalmente, estos protocolos permiten controlar el flujo de información en la red evitando el envío de video, audio, archivos ejecutables y otro software o elementos que representen una amenaza para la red y el contenido de la misma.

- Definir el número exacto de redes que deben implementarse: Lo cual delimita los puntos de acceso que se dispondrá para acceder a la red. Es muy común hoy en día que exista delimitación o segmentación en las redes empresariales, para lo cual de manera general se define una red de uso interno, y una red para invitados. Esta práctica no es del todo segura, ya que al habilitar una red de invitados dentro de la red global se genera el riesgo de que un dispositivo que no cumple el estándar o protocolos pueda acceder a la misma y mediante software especializado pueda infiltrarse a la red empresarial y a la información que se transmite en la misma.

  Para evitar estas amenazas se debe definir el número de redes, los permisos, acceso y niveles de seguridad que manejarán; así como segmentar adecuadamente las mismas. Por ejemplo: la red de datos puede distribuirse en dos subredes: computadores e impresoras, puede crearse una red para invitados y cuya conexión se limite únicamente a dispositivos específicos como computadores y bajo ningún motivo las red de Automatización o Control de acceso debe compartir el segmento de alguna de las redes mencionadas.

En la Figura N° 9, se muestra un ejemplo de la segmentación de redes y el control que existe sobre las mismas, con esta segmentación se define claramente el rango de cada una, qué tipos de equipos se conectan a la misma e inclusive la prioridad individual que se le debe dar para definir su ancho de banda.

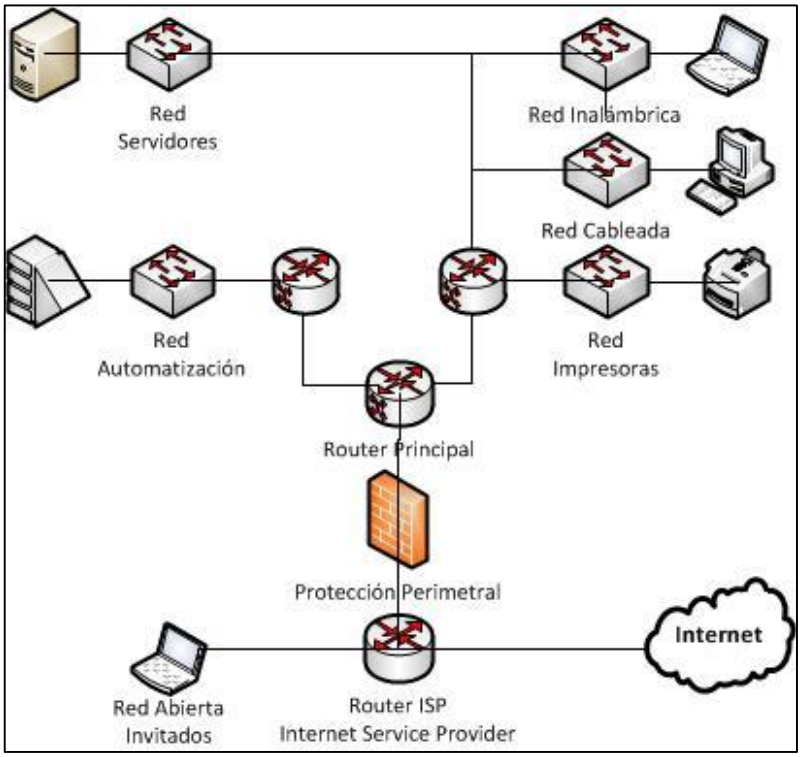


Figura N° 9: Adaptación de Diagrama de Segmentación de Redes
Fuente: (Cisco Systems, 2004)

- Establecer los equipos (tipos y modelos) que pueden conectarse a la red inalámbrica: Además de definir qué tipos de equipos (computadores, equipos celulares, entre otros), se pueden definir los modelos que accederán a la red. Por ejemplo, se puede dejar por fuera equipos celulares de determinada marca cuyos protocolos de seguridad no cumplen los estándares recomendados o simplemente denegar el acceso a la red a cualquier dispositivo móvil (equipos celulares, Tablet, entre otros) los cuales son más vulnerables y mediante los cuales podría producirse una intrusión a la red.

2.1.3 Gestión de Seguridad de la Información para Administración de Centros de Datos:

Estos sistemas e infraestructura contienen equipos y aplicaciones que cumplen funciones clave para el suministro de servicios esenciales para una organización (comunicaciones, almacenamiento de información, sistemas de control perimetral y vigilancia, entre otros). Si bien, para ello existen medios físicos y lógicos para proteger esta infraestructura (Firewall, Antivirus, Servidores de Filtro y Contenido, entre otros), se deben cubrir requisitos que van desde el ámbito físico hasta de proceso como por ejemplo:

- Requisitos para instalaciones físicas de Centros de Datos aplicables al país como lo requiere la "Norma TIA 942 – A 1" (Asociación de la Industria de las Telecomunicaciones, 2013) como: estructura básica del Centro de Datos (resistencia de materiales, instalaciones y suministro de energía eléctrica, sistema de aire acondicionado, sistema contra incendios, etc.), estudio sísmico, capacidad de redundancia y factibilidad de mantenimiento simultáneo.

  El aplicar el estándar TIA 942 – A 1 proporciona una base para el desarrollo e implementación de centros de datos, permitiendo que los mismos cuenten con las facilidades y seguridades estándar para ser catalogados como seguros y con base en ello definir su nivel de disponibilidad.

La siguiente figura (Figura N° 10) muestra el porcentaje de disponibilidad que asegura el aplicar los estándares TIA 942 – A 1, indicando el número total de horas de parada que podría sufrir un centro de datos.

TIER	% Disponibilidad	% Parada	Tiempo anual de parada
TIER I	99,67%	0,33%	28,82 horas
TIER II	99,74%	0,25%	22,68 horas
TIER III	99,98%	0,02%	1,57 horas
TIER IV	100,00%	0,01%	52,56 minutos

Figura N° 10: Porcentaje de disponibilidad de Centro de Datos aplicando la norma TIA 942 – A 1
Fuente: (Asociación de la Industria de las Telecomunicaciones, 2013)

En el Ecuador, existen Centros de Datos certificados como Capa 4 (Tier 4), lo cual asegura que cumple: infraestructura antisísmica, que esté construido con materiales calificados y que la zona donde se encuentre no sea calificada como "de riesgo" y si es "de riesgo" que pueda mitigar las amenazas correspondientes; también esta certificación incluye que cumpla estándares en lo referente a sistema eléctrico redundante, infraestructura intrínsecamente segura, sistema de refrigeración y aire acondicionado redundante y con norma ecológica.

- Planes de recuperación y contingencia ante desastres naturales o fallas: Esto desarrolla planes de contingencia ante eventos o desastres naturales que pueden afectar al funcionamiento y/o infraestructura que aloja el centro de datos.

  También permite contar con planes de respuesta ante desastres provocados de forma accidental o maliciosa que pueden afectar a la infraestructura y funcionamiento del centro de datos, como por ejemplo: un incendio o conato de

incendio que puede comprometer la integridad de la infraestructura y poner en riesgo la vida de las personas que desempeñan sus labores dentro del mismo.

Estos planes deben estar avalados por las respectivas autoridades, ser publicados en un lugar visible y difundidos a todo el personal.

- Procesos operativos, delegación de responsabilidades, roles y funciones: Todo centro de datos debe contener planes operativos y de mantenimiento que no afecten al funcionamiento del mismo, realizarse por personal calificado y que las actividades que realiza este personal no impacte o deteriore la infraestructura que se almacena en el Centro de Datos.

  Además, debe incluirse a detalle: los roles y responsabilidades del personal que brinda sus servicios en el centro de datos, así como la cadena de escalamiento y decisión ante posibles problemas o amenazas. Al ser un sitio que almacena información crítica de la empresa y está en funcionamiento ininterrumpidamente en todo momento, es necesario que se defina: el personal responsable para monitorear el funcionamiento, rendimiento y posibles alarmas, el personal responsable de ejecutar acciones o cambios ante posibles alarmas, el cronograma de mantenimiento de los sistemas que apoyan al correcto funcionamiento del centro de datos (sistema eléctrico, de refrigeración, control de acceso, etc.) y delegar al personal responsable y adecuado para esa tarea, así como, el respectivo cronograma de ejecución y solo en casos de emergencia solicitar el ingreso del mismo fuera de cronograma.

Por último, el mantenimiento del espacio físico del Centro de Datos también debe planificarse, determinando qué materiales se utilizarán para ello, así como los equipos de seguridad que debe utilizar el personal para evitar accidentes o lesiones, considerando que se trata de un espacio confinado, donde existe carga eléctrica y una señal externa (como un equipo celular) puede provocar una interferencia o daño en determinado equipo de comunicación.

2.1.4 Gestión de Seguridad de la Información para Sistemas de Control Industrial y Sistemas de Supervisión, Control y Adquisición de Datos (SCADA):

La seguridad en los Sistemas SCADA tiene gran importancia, ya que dentro de los mismos interactúan equipos, software, dispositivos de monitoreo y Control de Producción, los cuales controlan varios parámetros operacionales como: temperatura, presión, gestión de alarmas, tratamiento de datos y control de procesos, entre los más importantes (Automatas ORG, 2006). En la Figura N° 11 se muestra un esquema del modelo de un sistema SCADA, donde el sistema lee el flujo y nivel medido para posterior enviar los valores de ajuste a los PLC.

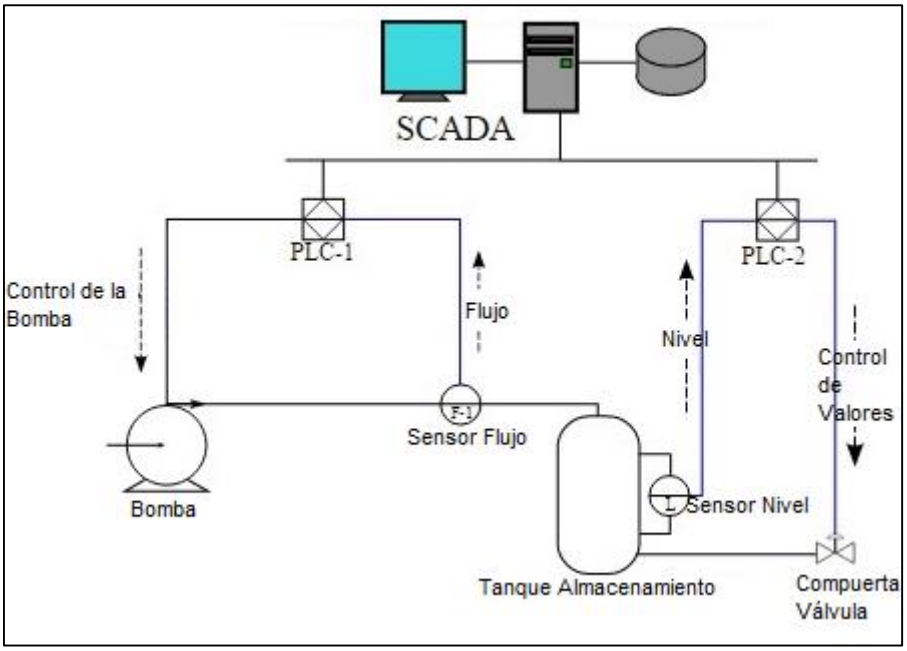


Figura N° 11: Esquema de un Sistema SCADA.
Fuente: (Automatización e Integración Tecnológica Argentina - AIT, 2015)

Una vulnerabilidad en la gestión de seguridad de este tipo de sistemas en la industria Petrolera, además de provocar pérdidas económicas, puede provocar daños colaterales como afectaciones irreversibles al medio ambiente, desabastecimiento de productos derivados del petróleo y hasta poner en riesgo la vida del personal que brinda sus servicios en este tipo de instalaciones (estaciones de bombeo, estaciones de almacenamiento, zonas de producción).

Para mitigar este tipo de riesgo, se deben cumplir requisitos obligatorios como son:

- Independencia de la red SCADA de la red corporativa de datos: Al ser SCADA un sistema de monitoreo y administración de infraestructura automatizada, el estar interconectado a la red empresarial donde se conectan cualquier dispositivo, podría provocar que de forma inintencionada un usuario acceda a la consola de administración del mismo y libere presión de un tramo o segmento

que controla el SCADA, poniendo en riesgo la vida del personal que trabaja en líneas de transmisión y provocando pérdidas económicas a la empresa por perdida de producción o daño en los sistemas de transmisión de y bombeo de crudo.

Por ende el sistema SCADA debe tener su red independiente, manejar sus propios protocolos de red y seguridad y no permitir interconexión de ningún dispositivo ajeno al mismo.

- Administración de perfiles para monitoreo, modificación y paradas de emergencia ante variaciones de parámetros: Permite definir un plan ante posibles alarmas por variación en sus sensores, dando la guía a los operadores para saber cómo actuar ante esas variaciones y entregándoles la potestad de realizar una modificación o una parada de emergencia para evitar inminentes riesgos que podrían producirse ante una variación de sus valores normales.

- Sistemas de monitoreo local (en estaciones productivas) y remoto (estación central) con delegación de responsabilidades: El sistema SCADA siempre debe contar con monitoreo local, considerando que la decisión para ejecutar un paro de emergencia ante la variación normal de sus valores debe ejecutarse de forma inmediata; si el mismo es monitoreado de forma remota pueden producirse riesgos que dificulten que la señal no llegue a la consola remota, la misma se bloquee por efectos de software local de la consola y denegar la ejecución de comandos de modificación o paradas de emergencia.

En la Figura N° 12, se muestra un ejemplo del Panel View (terminales gráficos con opciones de pantalla y teclado táctil que permiten visualizar al operador las variables que obtiene un PLC - Programmable Logic Controler / Controlador Lógico Programable) que controla una estación de producción en sitio. En la pantalla se muestran los indicadores que se obtienen de mediciones y las acciones que se puede ejecutar mediante comandos o secuencia de funciones.



Figura N° 12: Panel View SCADA en Estación de Producción
Fuente: (Rockwell Automation, 2016)

Se recomienda que el monitoreo se realice de forma independiente en las estaciones productivas y como medida de precaución se ejecute un monitoreo centralizado en una estación productiva dentro del mismo campo productivo.

Se debe delegar de igual forma personal responsable por turno y con su respectivo rol con el fin de que se determine, quien es el responsable de tomar una decisión, quien el responsable de aprobarla y quien es el responsable de ejecutarla, estando conscientes todos del riesgo y consecuencias que puede ocasionar el ejecutar o no una determinada acción.

- Sistema de respaldo para monitoreo en caso de fallas del sistema principal: Al ser SCADA un sistema que trabaja ininterrumpidamente al ritmo de las estaciones que administra, es necesario que se definan equipos de respaldo para evitar fueras de línea del sistema, sea de forma global o local en una estación. Por ello, es necesario que exista una consola de administración centralizada que administre todas las estaciones y los casos de paros por fallas o mantenimiento programados. También el monitoreo del SCADA pueda ser delegado de forma temporal a un equipo de respaldo pero dentro del mismo campo productivo.

- Cuadro de escalamiento y tiempos en caso de variación normal de parámetros normales de ejecución: Esto determina el personal responsable de tomar decisiones ante eventuales variaciones en los parámetros normales de ejecución en el sistema SCADA, logrando tener una cadena de confirmación para ejecutar cambios o paros de emergencia ante variaciones o, en el caso de no tener respuesta, delegar la responsabilidad al operador para ejecutar cualquier tipo de acción.

- Plan de ejecución con tiempos y responsabilidades ante variación normal de parámetros: El plan de ejecución es la guía que tiene el operador para seguir una

secuencia lógica de pasos para regresar el Sistema SCADA a sus parámetros normales de funcionamiento y por ende a la infraestructura que monitorea y en qué momento ejecutar cada acción. En el caso que el plan no funcione debería ejecutar un escalamiento para solicitar confirmación antes de ejecutar cambios que podrían afectar al sistema que monitorea el SCADA o detener el mismo mediante un paro de emergencia.

- Procesos operativos, delegación de responsabilidades, roles y funciones: Por último como todo sistema que funciona ininterrumpidamente, el sistema SCADA debe contar con un cronograma de mantenimiento preventivo, un organigrama con el personal responsable y la definición de roles y tareas para cada persona, con el fin de evitar duplicación de funciones, delegaciones incorrectas de tareas y por ende, mala administración en el mantenimiento del sistema lo cual obligaría a mantenimientos correctivos de emergencia.

La seguridad de la información en cualquiera de los puntos detallados anteriormente, busca la confidencialidad de los datos, protección de la información sensible (de suma importancia para la organización) y la protección de infraestructura catalogada como crítica.

No cumplir con los requisitos que detalla la gestión de seguridad de la información, puede representar pérdidas económicas para una organización por fuga de información o por estados “fuera de línea”, los cuales pueden presentarse en la infraestructura y en repositorios de información digital.

2.2 Modelos de gestión de Sistemas de gestión de Seguridad de la Información

En la actualidad existen varios modelos de gestión que aportan a la administración de la Seguridad de la Información y que son aplicables para cualquier tipo de organización y/o industria, cada uno de ellos es avalado por una institución reconocida internacionalmente. Entre los más destacados se encuentran:

- Familia de Normas ISO 27000.
- ITIL V3.

A continuación se detalla cada uno de ellos:

2.2.1 Familia de Normas ISO 27000.

Es la normativa internacional que hace referencia exclusivamente a seguridad de la información y entrega un marco de referencia basado en cinco estándares (Organización Internacional de Normalización, 2014):

- ISO/IEC 27001:2013 Tecnología de la Información – Técnicas de Seguridad – Sistema de Administración de Seguridad de la Información – Requisitos.
- ISO/IEC 27002:2013 Tecnología de la Información – Técnicas de Seguridad – Código de Prácticas para controles de Seguridad de la Información – Requisitos.
- ISO/IEC 27003 Tecnología de la Información – Técnicas de Seguridad – Guía para la Implementación de un Sistema de Administración de Seguridad de la Información.

- ISO/IEC 27004 Tecnología de la Información – Técnicas de Seguridad – Administración de Seguridad de la Información – Medición.
- ISO/IEC 27005 Tecnología de la Información – Técnicas de Seguridad – Gestión del riesgo de Seguridad de la Información.

La Norma ISO 27001:2013 es el estándar internacional vigente que "provee los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI)" (Organización Internacional de Normalización, 2014). Considera como punto indispensable que un SGSI es parte integrada de los procesos de la organización y de la administración de toda la estructura organizacional. Además, la implementación del SGSI puede ser escalable acorde a las expectativas y necesidades de la organización.

La Norma ISO 27001:2013 es un estándar aplicable a cualquier estructura organizacional y compatible con otros estándares de administración de sistemas de información.

La Norma ISO 27001:2013 puede ser utilizada por áreas internas o externas que requieran evaluar la capacidad de la organización respecto a la administración de sus propios requisitos de seguridad de la información, buscando preservar la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de la administración y análisis de riesgos.

Los puntos más importantes que la Norma ISO 27001:2013 propone son:

- Organización: Entender el contexto de la organización y expectativas de las partes.
- Definir un sistema de administración de seguridad de la información y entender su alcance dentro de una organización.
- Liderazgo: roles organizacionales, responsabilidades y autoridades en proceso de implementar un SGSI.
- Planeamiento: Acciones, riesgos y oportunidades, así como los objetivos de la gestión de la seguridad de la información.
- Soporte: Recursos, competencia, comunicaciones y documentación.
- Operación: Planeamiento y control operacional, evaluación y tratamiento de riesgos.
- Evaluación de Desempeño: Monitoreo, medición, análisis y evaluación; así como las auditorías internas y revisión de la administración.
- Mejora: No conformidades, su acción correctiva y por último la mejora continua.

En la Figura N° 13 se muestra una adaptación de los requisitos de ISO 27001:2013 enmarcado en el ciclo de Deming (PDCA: Plan – Do – Check – Act / PHVA: Planificar – Hacer – Verificar – Actuar):

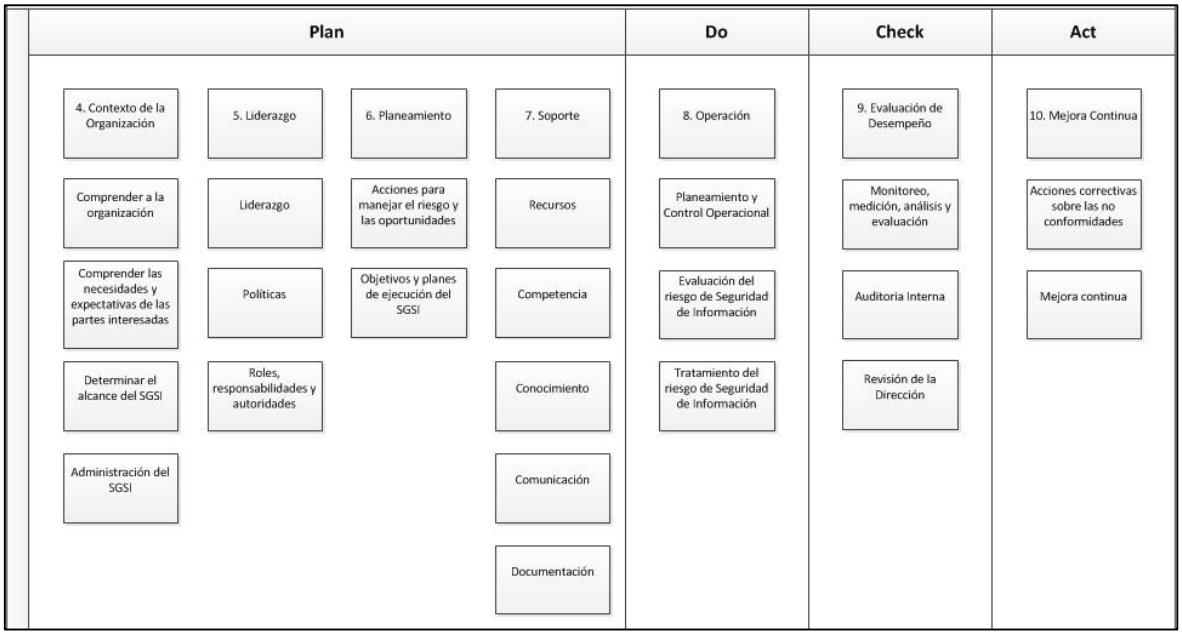


Figura N° 13: Adaptación Norma ISO 27001:2013 enmarcada en el ciclo de Deming (PDCA)
Fuente: (ITpreneurs, 2014)

ISO 27001:2013, valida el cumplimiento de la misma mediante ciento catorce (114) Objetivos de Control y Controles. El listado de estos objetivos se presenta en el Anexo 1.

Se debe considerar que la norma ISO 27001:2013 no es una actividad o tarea que está ligada estrictamente a las áreas de Tecnología de las empresas y que tampoco puede y/o debe ser aplicada únicamente por personal de Tecnología.

La norma ISO 27001:2013 como el resto de normas ISO es un compromiso de toda la empresa que viene acompañada del liderazgo de las gerencias de la empresa y no se trata únicamente de escribir nuevos procedimientos o políticas para publicarlas al resto de personal; aporta a que se descubran vulnerabilidades que pueden afectar a la seguridad de la información de la empresa y enseña como mitigar las mismas mediante herramientas.

ISO 27001:2013 es un estándar que permite reducir amenazas, riesgos y vulnerabilidades que a futuro podrían representar pérdidas económicas o de talento humano para las empresas y que su correcta aplicación ofrece la posibilidad de certificación externa.

2.2.2 ITIL V3 (Information Technology Infraestrucure Library - Biblioteca de Infraestructura de Tecnologías de Información)

Es un conjunto de conceptos y buenas prácticas utilizadas para la gestión de servicios de tecnología de la información desarrollada en los años 80 por la Agencia Central de Computación y Telecomunicaciones (Central Computer and Telecommunications Agency - CCTA de Gran Bretaña), enfocada en el ciclo de vida del servicio. Este ciclo es el siguiente (ver Figura N° 14):

- Estrategia del servicio.
- Diseño del servicio.
- Transición del servicio.
- Operación del servicio.
- Mejora continua del servicio.

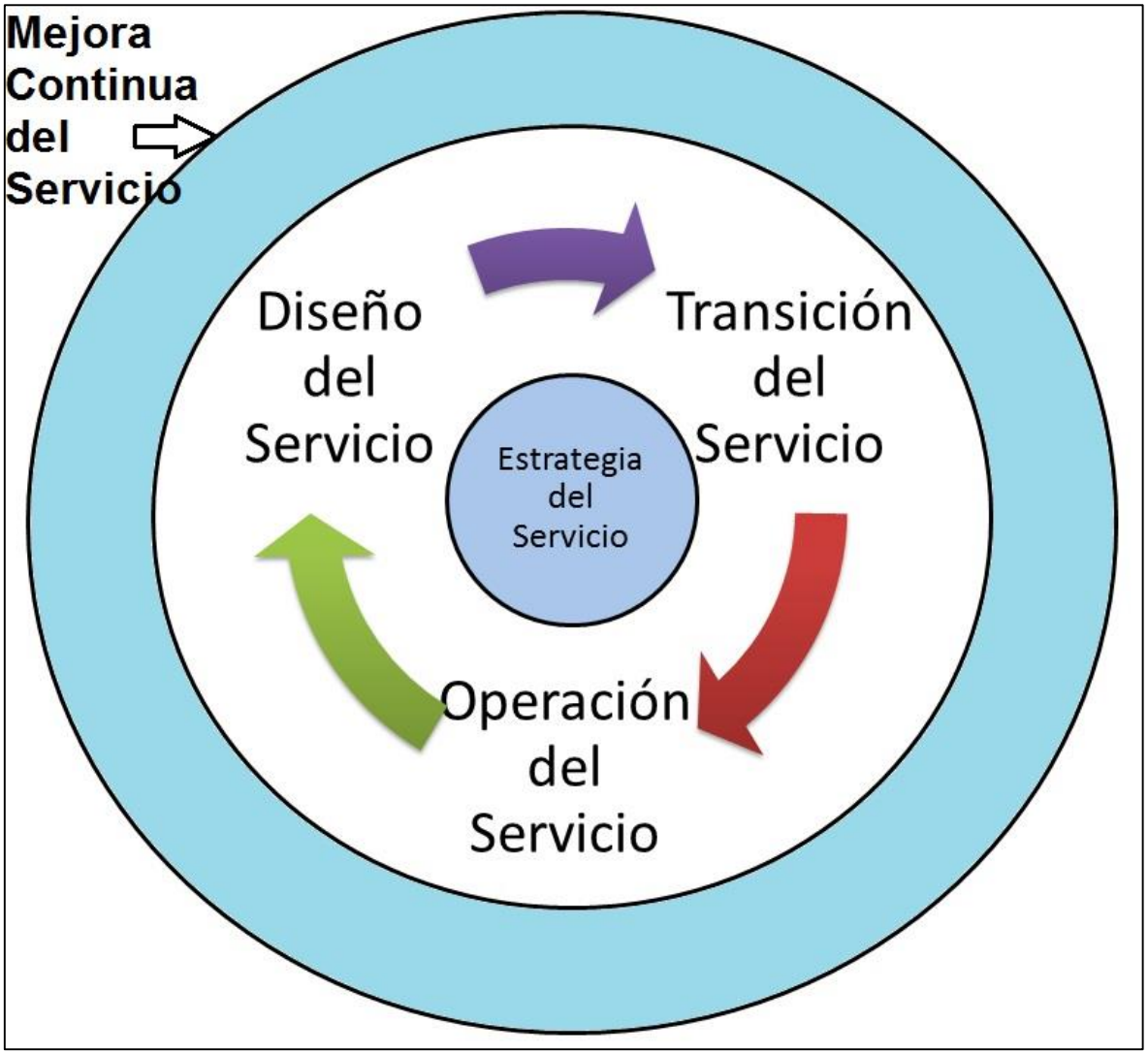


Figura N° 14: Adaptación del Ciclo de Vida del Servicio
Fuente: (ITpreneurs, 2014)

Dentro del proceso de Operación del servicio se incluye la Gestión de la Seguridad de la información cuya finalidad es alinear la seguridad de Tecnología de Información (TI) con la del negocio.

Además garantiza que la confidencialidad, integridad y disponibilidad de activos, información, datos y servicios de tecnología de la información de la organización siempre coincidan con las necesidades del mismo (ITpreneurs, 2014).

Bajo este modelo, se resumen los requisitos de Gestión de Seguridad incluido dentro de la Operación del Servicio (ver Figura N° 15):

Fase	Procesos	Requisitos
Estrategia del Servicio	Generación de la Estrategia	
	Administración Financiera	
	Administración del Portafolio de Servicio	
	Administración de la Demanda	
Diseño del Servicio	Administración del Catálogo de Servicios	
	Administración del SLA	
	Administración de la Capacidad	
	Administración de la Disponibilidad	
	Administración de la Continuidad del Servicio IT	
	Administración de la Seguridad de la Información	
	Administración de Proveedores	
Transición del Servicio	Palnificación y Soporte de la Transición	
	Administración de Cambios	
	Administración de la Configuración	
	Administración de Desarrollo y Liberación	
	Validación y Pruebas del Servicio	
	Evaluación	
	Administración del Conocimiento	
Operación del Servicio	Administración de Eventos	
	Administración de Incidentes	
	Solicitudes de cumplimiento	
	Administración de Problemas	
	Administración de Accesos	Política y Planes de Seguridad del Negocio La Operación del Negocio y sus necesidades de seguridad Planes y Necesidades de negocios futuros Requisitos legales y regulatorios Obligaciones y responsabilidades relativas a la seguridad incluida en SLA Riesgos del negocio, TI y su gestión
Mejora Continua del Servicio	7 pasos para mejorar los procesos	
	Reporte del Servicio	
	Medición del Servicio	

Figura N° 15: Requisitos de Gestión de Seguridad dentro de la Operación del Servicio en ITIL V3
Fuente: (ITpreneurs, 2014)

La revisión de los estándares ISO 27001:2013 e ITIL V3 permite concluir que los dos comparten requisitos en común, cuya profundidad varía de acuerdo al campo de aplicación. Sin embargo, ISO 27001:2013 está enteramente centrada en seguridad de la información enfocada en una organización, área o proceso y es el primer paso para poder certificar a un sistema con este estándar, mientras que ITIL V3 se centra en los servicios de TI que se aplican dentro de una organización y cuya finalidad es certificar dichos servicios que dentro de ella se administran pero sin dejar de lado la seguridad de la información.

Mediante la aplicación de los requisitos de la gestión de seguridad de la información, independiente del marco de referencia, norma o estándar que se siga; las organizaciones deben establecer y mantener una Gestión de Seguridad de la Información para salvaguardar la integridad de la información y su infraestructura (ITpreneurs, 2014).

2.3 Medición del Tiempo.

El “Estudio del Trabajo” (Criollo, 2005) propone varias técnicas para la Medición del Tiempo, una de las cuales se orienta a la Medición del Trabajo y de la cual se resume sus principales puntos.

2.3.1 Medición del Trabajo.

La Medición del trabajo es un Método Investigativo basado en la aplicación de varias técnicas para determinar el contenido de una tarea definida, fijando el tiempo que un trabajador calificado invierte en llevarla a cabo, con arreglo a una norma de rendimiento prestablecida.

Sus objetivos son:

- Incrementar la eficiencia del trabajo.
- Proporcionar estándares de tiempo que servirán de información a otros sistemas de la empresa, como el de costos de programación de la producción, supervisión, entre otros.

La Medición del Trabajo se utiliza para analizar el proceso, determinar si se aplica el mejor método de ejecución, eliminar toda actividad innecesaria, combinar, cambiar y/o simplificar actividades; además determinar una base de tiempo para poder evaluar a futuro el proceso ante la inclusión de mejoras o cambios en el mismo.

2.3.1.1 Conceptos Básicos para la Medición del Trabajo

Tiempo Tipo o Tiempo Estándar: Se denomina al tiempo que se concede para efectuar una determinada tarea, para calcular el mismo se debe considerar:

- Obtener y registrar información de la operación.
- Descomponer la tarea y registrar sus elementos.
- Tomar las lecturas.
- Nivelar el ritmo de trabajo.
- Calcular los suplementos del estudio de tiempo.

Muestreo del trabajo: Es una técnica para estimar la proporción del tiempo dedicado a un tipo de actividad dad durante un cierto tiempo, empleando para ello observaciones instantáneas, intermitentes y espaciadas al azar. Para calcular la misma se debe considerar:

- Definir objetivos.
- Estimar número satisfactorio de observaciones a realizar.
- Selección de la longitud del trabajo.

- Determinación de los detalles del procedimiento de muestreo (programación de observaciones, método exacto de observaciones, diseño de la hoja de observaciones y rutas a seguir).
- Recopilación de datos mediante la ejecución de un plan de muestreo.
- Procesamiento de cálculos.
- Presentación de resultados.

Observaciones necesarias para calcular el tiempo normal: Si el número de observaciones es significativo (por ejemplo, para tareas repetitivas de producción) puede determinarse el número de observaciones a realizarse en base a uno de los siguientes procedimientos:

- Fórmulas estadísticas.
- Ábaco de Lifson.
- Tabla Westinghouse.
- Criterio de General Eléctric.

2.3.2 Técnicas de Medición del Trabajo.

Para poder realizar la medición del trabajo se pueden utilizar las siguientes técnicas:

- Estimación de datos históricos.
- Estudio de tiempos con cronómetro.
- Por descomposición en micro movimientos de tiempos predeterminados.
- Métodos de las observaciones instantáneas (muestreo del trabajo).

- Datos estándar y fórmulas de tiempo.

Cualquiera de ellas permite obtener el tiempo tipo o estándar del trabajo medido. A continuación se describe el método de Estimación de Datos Históricos.

- Estimación de datos históricos.

Los datos históricos son la documentación que se tiene sobre experiencias pasadas en la ejecución de determinada actividad, donde se detalla las horas de mano de obra necesarias para producir una determinada cantidad de trabajo, en los casos de tareas mecánicas se incluye los registros históricos del uso del equipo que a futuro se utilizan para realiza el mantenimiento o reparación del mismo.

Para medir el trabajo sobre la base de datos históricos, se registra el tiempo requerido para terminar cada trabajo y para los casos que el trabajo incluye las mismas tareas recurrentes, se mide cada una de ellas y se agrega su resultado en un nuevo registro, para al final de la ejecución del trabajo o luego de determinado número de repeticiones se pueda evaluar cada resultado con el fin de validar la mejora en el tiempo de ejecución. Este enfoque puede ser especialmente efectivo cuando se acopla con un plan de incentivo salarial, donde el objetivo es hacer mejoras continuas sobre los niveles históricos.

En esta forma, es posible mantener en control continuo el tiempo requerido por unidad de trabajo y controlar también las desviaciones del promedio histórico.

Para algunos trabajos el enfoque de utilizar los datos históricos puede ser preferible, esto debido a que el trabajo en si se utiliza para desarrollar un estándar, además no se requieren de cronómetros y se permite la flexibilidad en el método, impulsando así la innovación, sin la necesidad de establecer un nuevo estándar.

Para ejecutar la medición del trabajo se debe seguir los siguientes pasos (Criollo, 2005):

1. Establecer el período de tiempo del que se desea obtener los datos históricos.
2. Recopilar los registros de datos históricos del período de tiempo a medir.
3. Ordenar los datos históricos con el fin de revisar cada uno de sus registros en base a las actividades o agruparlos en base a un criterio para su medición (complejidad o misma secuencia de ejecución de actividades, uso de herramientas, hora de ejecución, entre otros).
4. Definir el tamaño de la muestra a medir, justificando si la muestra es significativa, caso contrario se debe ampliar el rango de tiempo para recopilar un mayor registro de datos históricos, para ello se utiliza la siguiente fórmula (Murray & Larry, 2009):

$$n = \frac{N * Z_{\propto}^{2} * p * q}{d^{2} * (N-1) + Z_{\propto}^{2} * p * q}$$

Donde:

n = Tamaño de la muestra a calcular.

N = Tamaño de la población finita.

Z = Valor correspondiente a la distribución de gauss (Tabla de valores estándar) donde Zα = 0.05 = 1.96 que representa la seguridad del 95% para el cálculo.

p = Proporción esperada (en este caso p = 0.5 (50%) lo cual maximiza el tamaño muestral al combinar con el valor de q).

q = Diferencia de proporción esperada que equivale a 1 – p (en este caso 1 – 0,5 = 0,5).

d = Precisión o error que se prevé cometer, se recomienda utilizar el valor del 5%, es decir d = 0,05.

5. Ejecutar el proceso de cálculo.
6. Presentar y evaluar los resultados.

Al seguir esta secuencia de pasos se asegura una ejecución de la medición de tiempo ordenada, con criterios de comparación normalizados, rangos de tiempo tolerables, muestra de datos significativa y comprobable estadísticamente, permitiendo que los resultados que se presenten sean fiables y acertados una vez ejecutada la medición.

2.4 Normativa Legal Vigente.

El campo de la Seguridad de la Información está regulado en Ecuador mediante una normativa legal vigente, cuya aplicación está para el beneficio y resguardo de las partes que administran información de carácter privado.

Esta normativa es el “Código Orgánico Integral Penal” (COIP), el cual está enmarcado por un lado en proteger los derechos de las personas, y por otro a limitarlos; guardando simetría entre las sanciones y penas por los grados de lesión que se efectué sobre una persona o bien.

En lo referente a Seguridad de la Información, el COIP en su Capítulo Tercero – Delitos contra los Derechos del Buen Vivir – Sección Tercera, considera los "Delitos Contra la Seguridad de los Activos de los Sistemas de Información y Comunicación" y cita entre sus principales puntos, los siguientes artículos que están vinculados a los procesos para empresas del Sector Privado.

"Artículo 229.- Revelación ilegal de base de datos.- La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años." (Ministerio de Justicia, Derechos Humanos y Cultos del Ecuador, 2014).

"Artículo 230.- Interceptación ilegal de datos.- Será sancionada con pena privativa de libertad de tres a cinco años:"

- "La persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible." (Ministerio de Justicia, Derechos Humanos y Cultos del Ecuador, 2014)
- "La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del

delito descrito en el inciso anterior.” (Ministerio de Justicia, Derechos Humanos y Cultos del Ecuador, 2014).

“Artículo 232.- Ataque a la integridad de sistemas informáticos.- La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años.” (Ministerio de Justicia, Derechos Humanos y Cultos del Ecuador, 2014).

Con igual pena será sancionada la persona que:

- “Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.” (Ministerio de Justicia, Derechos Humanos y Cultos del Ecuador, 2014)
- “Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.” (Ministerio de Justicia, Derechos Humanos y Cultos del Ecuador, 2014).

“Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el

acceso logrado, modificar un portal web, desviar o re direccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.” (Ministerio de Justicia, Derechos Humanos y Cultos del Ecuador, 2014).

CAPÍTULO III: DIAGNÓSTICO Y DESARROLLO

3.1 Diagnóstico de la Situación Actual

3.1.1 Levantamiento del Proceso “Alta y Baja de Usuarios”

Para poder definir la situación actual de la empresa, se realizó el relevamiento de información en el proceso de “Alta y Baja de Usuarios”, entrevistando a los dueños de proceso y/o responsables asignados por la organización. Este relevamiento se realizó para los tres subprocesos del proceso en estudio y que son:

- Alta de Usuarios.
- Baja de Usuarios.
- Modificación de Permisos de Usuarios.

Para relevamiento de cada subproceso se utilizaron:

- Caracterizaciones de cada subproceso en las que se describen los siguientes elementos:
    - Entradas: Son los elementos que dan inicio al proceso.
    - Controles: Son los estándares que regulan la ejecución de las actividades del proceso.
    - Recursos: Son los actores que intervienen dentro del proceso, estos pueden ser de carácter humano, tecnológico y/o financiero.

- Salidas: Son los resultados finales o entregables, una vez que se han cumplido todos los estándares (controles), del proceso, pudiendo convertirse la salida de un proceso en la entrada de otro proceso. En la Figura N° 16, se muestra el esquema con los elementos para la caracterización de un proceso.

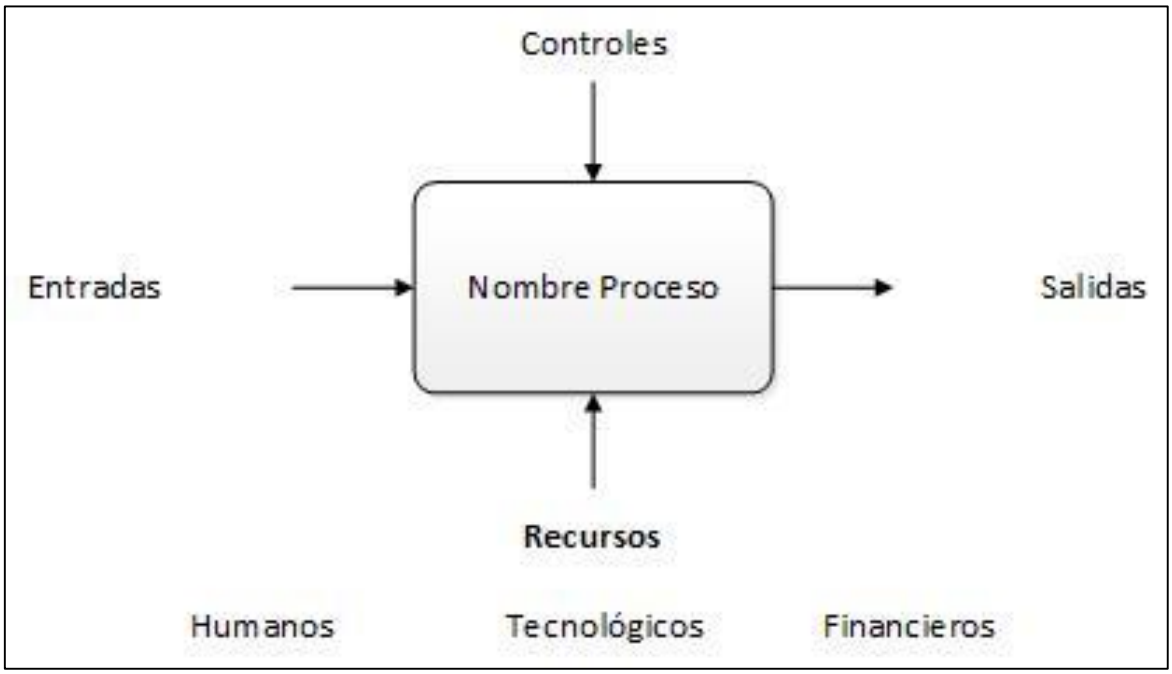


Figura N° 16: Adaptación de la Representación esquemática de los elementos de un proceso en base a la Norma ISO 9001:2015
Fuente: (Organización Internacional de Normalización, 2015)

- Diagramas de flujo corporativo y local de cada subproceso utilizando nomenclatura ANSI (American National Standards Institute).
- Actores corporativos y locales que intervienen en cada subproceso.

El diagnóstico y relevamiento de información fue indispensable para conocer la situación actual de la organización.

A continuación se presenta lo desarrollado para cada subproceso:

3.1.1.1 Levantamiento del Subproceso “Alta de Usuarios”.

a) Caracterización del Subproceso.

En la Figura N° 17 se representa la caracterización del subproceso “Alta de Usuarios”.

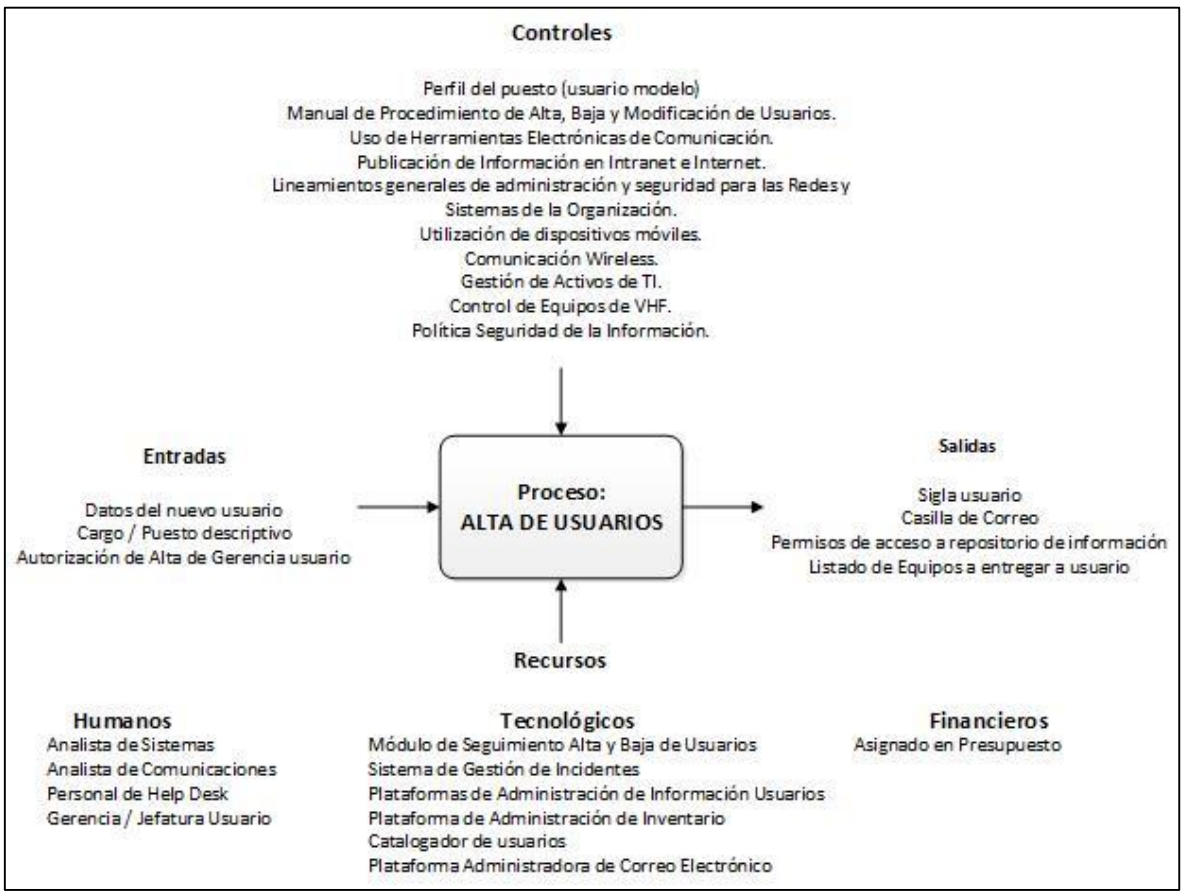


Figura N° 17: Caracterización del Subproceso de Alta de Usuarios
Fuente: Elaboración propia del Investigador

b) Diagramas de Flujo Corporativo y Local.

En la Figura N° 18, se muestra el diagrama de flujo que se identificó a nivel corporativo para el subproceso de “Alta de Usuarios” dentro del Manual de Procedimiento de “Alta, Baja

y Modificación de Usuarios" del año 2012 (última actualización). De este diagrama se partió para su contraste con las actividades en Ecuador.

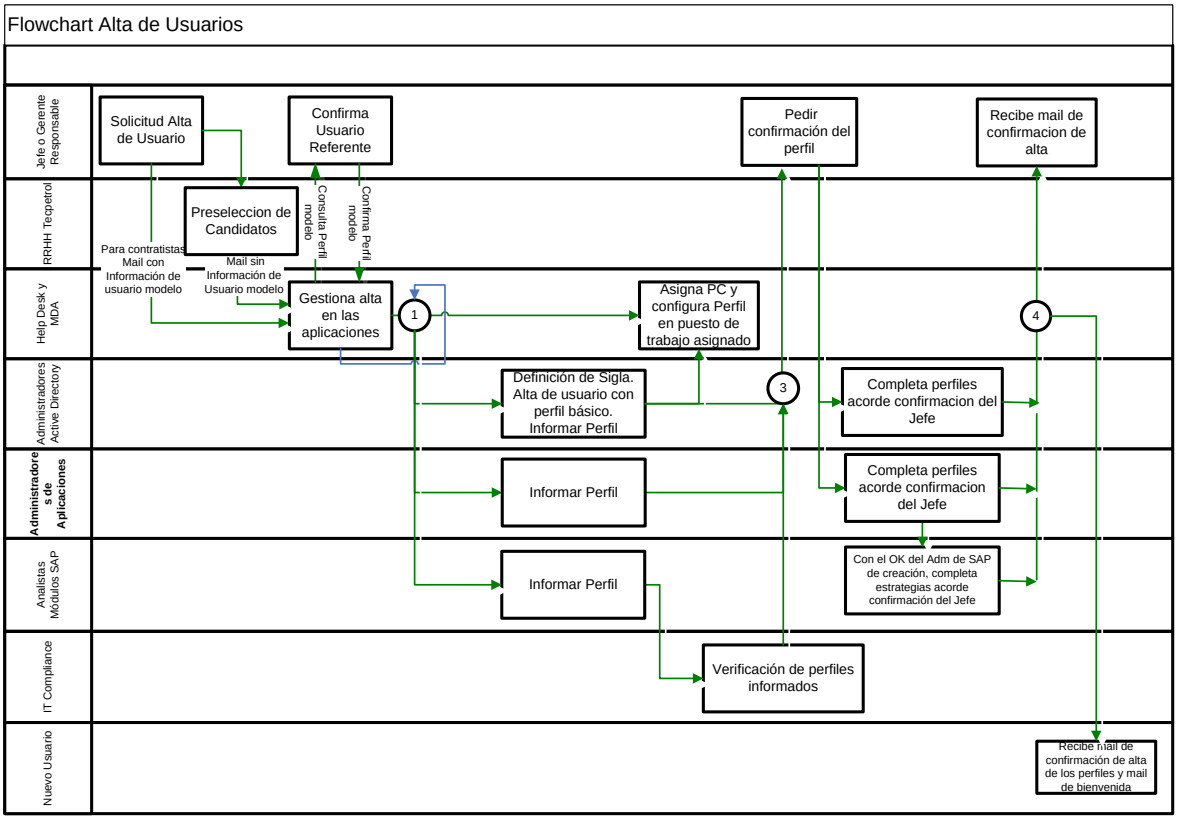


Figura N° 18: Esquema de Alta de Usuario a nivel Corporativo
Fuente: (Empresa de Consultoría para la Industria Petrolera, 2012)

Sin embargo, al revisar las actividades aplicadas en Ecuador, se requirió desarrollar el diagrama de flujo local (ver Figura N° 19) para detallar el subproceso de "Alta de Usuarios" que se estaba aplicando, con las diferencias respecto al esquema corporativo. En este diagrama se pueden identificar las áreas responsables y las actividades que ejecutan cada una para el subproceso.

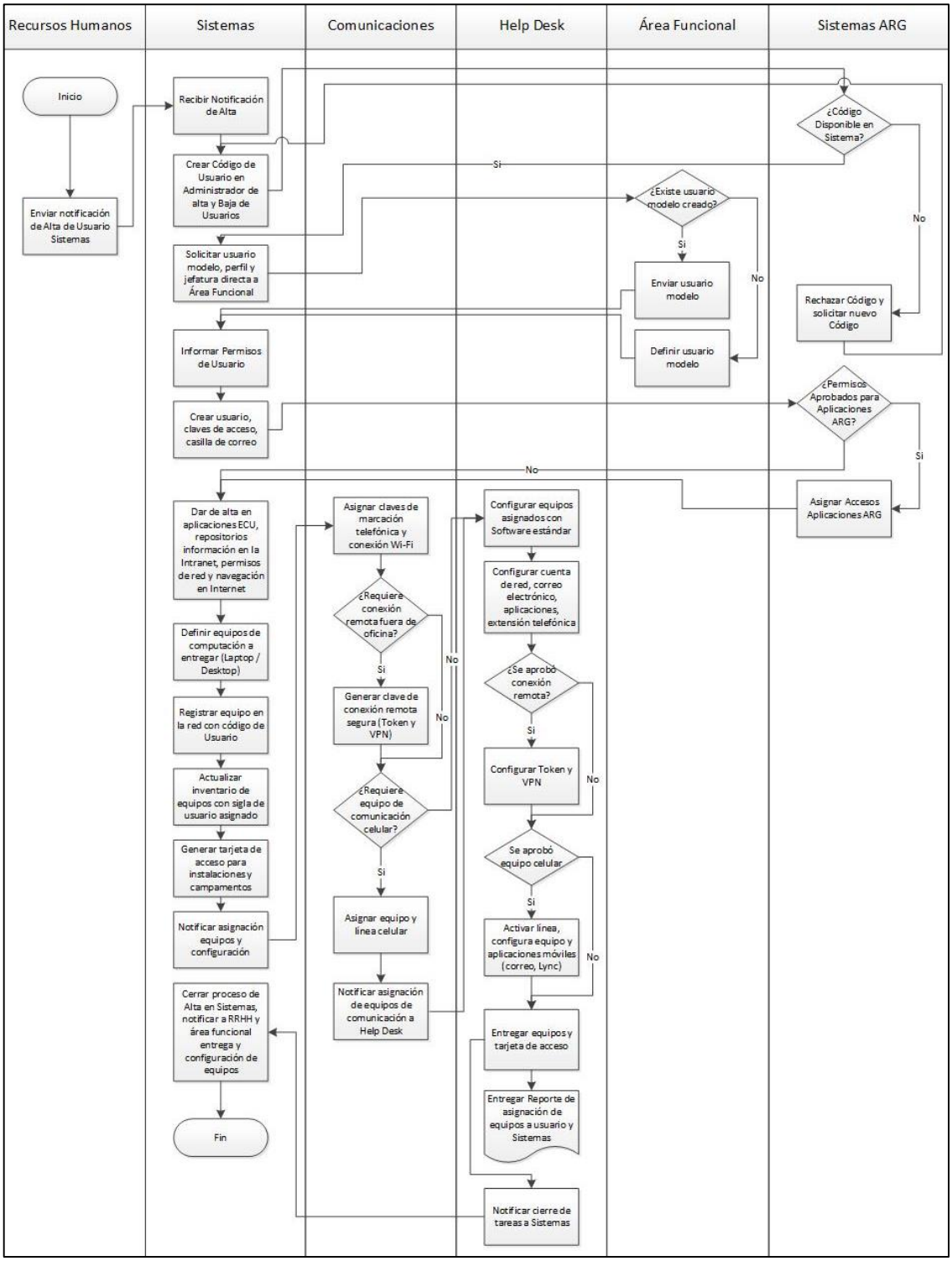


Figura N° 19: Diagrama de Flujo del Subproceso de “Alta de Usuarios”
Fuente: Elaboración propia del Investigador

c) Actores Corporativos y Locales.

La documentación existente (Manual de Procedimiento de "Alta, Baja y Modificación de Usuarios - ABM") para el presente proceso, identifica los actores y sus responsabilidades que se citan en la siguiente tabla (Ver Tabla N° 4).

Tabla N° 4:
Actores dentro del proceso de "Alta de Usuarios"

Actor Corporativo
Jefe o Gerente Responsable
Recursos Humanos
Help Desk y Mesa de ayuda
Administrador Active Directory
Administrador de Aplicaciones
Analista Módulos SAP
IT Compliance
Nuevo Usuario

Nota. Actores y funciones para el proceso de "Alta de Usuarios".
Fuente: (Empresa de Consultoría para la Industria Petrolera, 2012)

La comparativa de actores Corporativos – Ecuador para este subproceso es la siguiente (ver Tabla N° 5). Esta relación está justificada por el tamaño y estructura diferente entre oficinas corporativas y Ecuador.

Tabla N° 5:
Actores para Ecuador dentro del proceso de "Alta de Usuarios"

Actor Corporativo	**Actor (Ecuador)**
Jefe o Gerente Responsable	Gerente de Área funcional
Recursos Humanos	Recursos Humanos
Help Desk y Mesa de Ayuda	Ingeniero de Soporte
Administrador Active Directory	Analista de Sistemas

Administrador de Aplicaciones	Analista de Sistemas / Analista de Comunicaciones
Analista Módulos SAP	Analista Módulos SAP (Argentina)
IT Compliance	IT Compliance (Argentina)
Nuevo Usuario	Nuevo Usuario

Nota. Comparativa de funciones y responsables para el proceso de Alta y Baja de Usuarios.
Fuente: Elaboración propia de Investigador

3.1.1.2 Levantamiento del Subproceso “Baja de Usuarios”.

a) Caracterización del subproceso.

En la Figura N° 20 se representa la caracterización del subproceso “Baja de Usuarios”

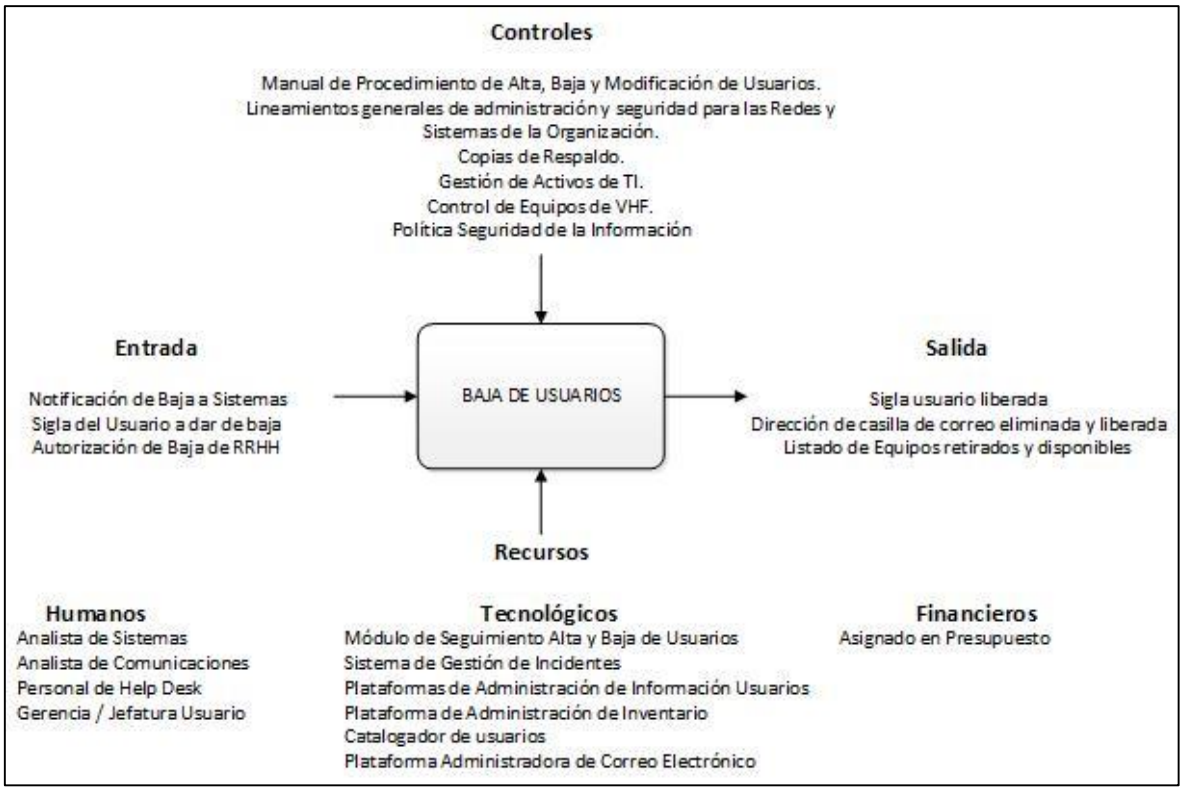


Figura N° 20: Caracterización del Subproceso de “Baja de Usuarios”
Fuente: Elaboración propia del Investigador

b) Diagramas de Flujo Corporativo y Local.

En la Figura N° 21, se muestra el diagrama de flujo que se define a nivel corporativo para el subproceso de “Baja de Usuarios” dentro del Manual de Procedimiento de “Alta, Baja y Modificación de Usuarios” del año 2012 (última actualización). De este diagrama se partió para su contraste con las actividades en Ecuador.

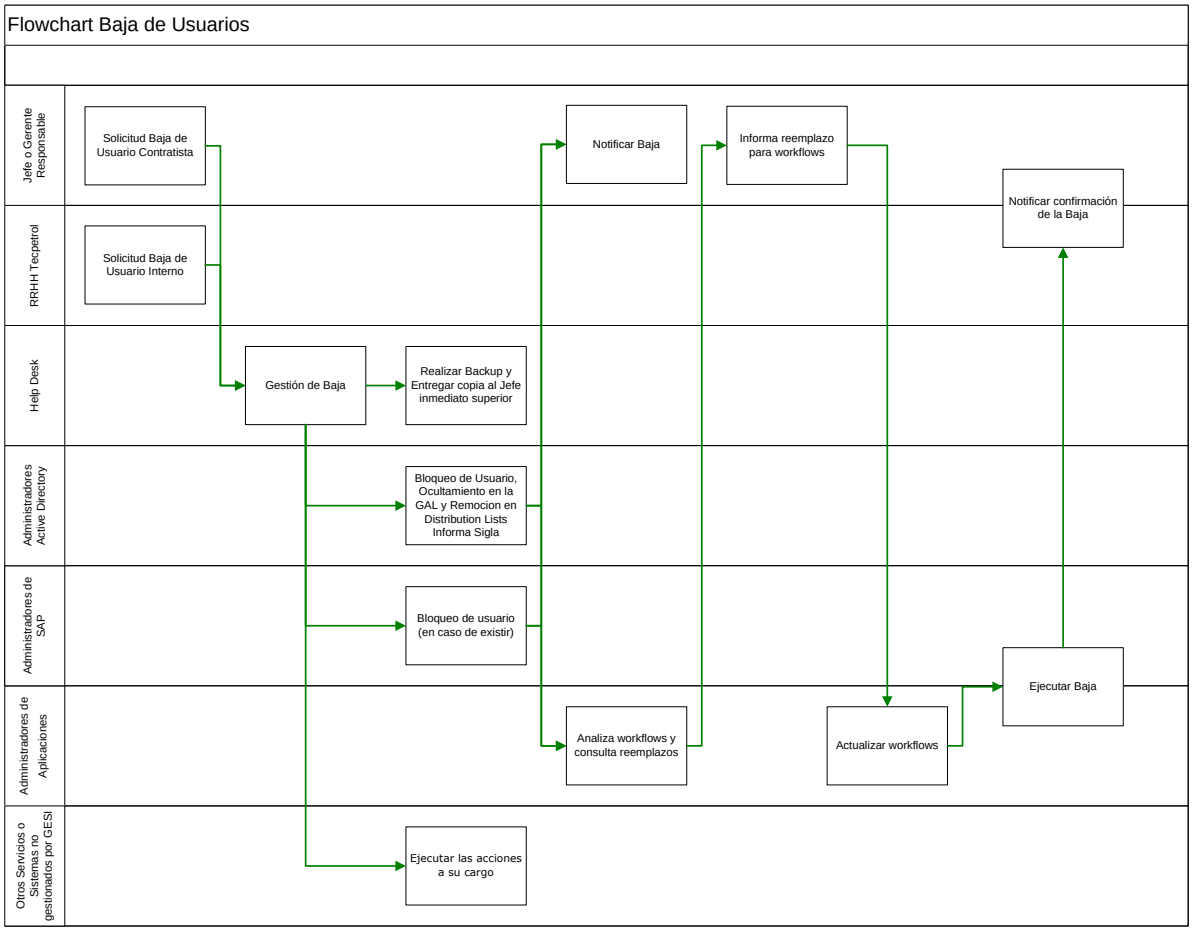


Figura N° 21: Esquema de Baja de Usuario a nivel Corporativo
Fuente: (Empresa de Consultoría para la Industria Petrolera, 2012)

Sin embargo, al revisar las actividades aplicadas en Ecuador, se requirió desarrollar el diagrama de flujo local (ver Figura N° 22) para detallar el subproceso de “Baja de Usuarios” que se estaba aplicando con las diferencias respecto al esquema corporativo. En este

diagrama se pueden identificar las áreas responsables y las actividades que ejecutan cada una para poder él subproceso.

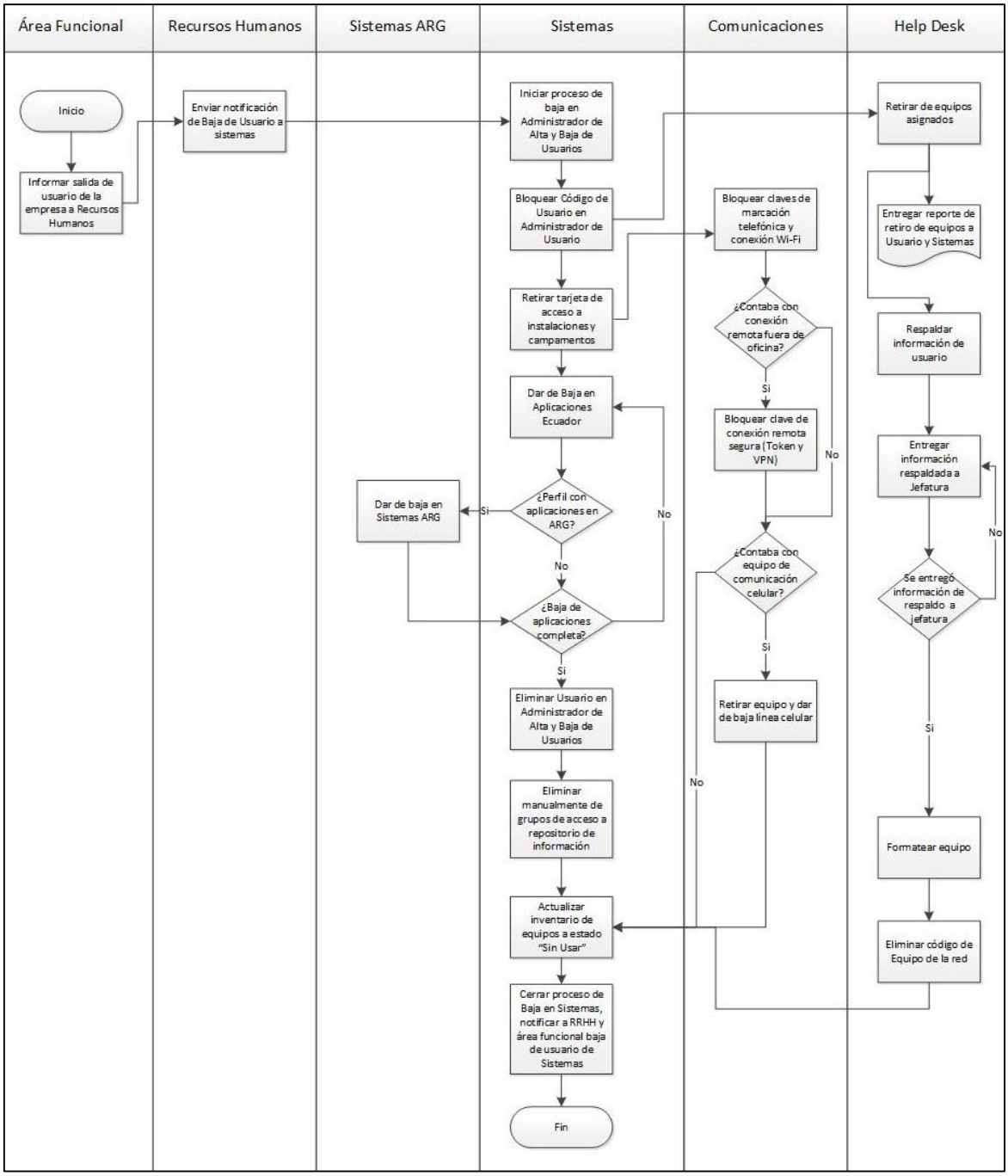


Figura N° 22: Diagrama de Flujo del Subproceso de "Baja de Usuarios"
Fuente: Elaboración propia del Investigador

c) Actores Corporativos y Locales.

La documentación existente (Manual de Procedimiento de "Alta, Baja y Modificación de Usuarios - ABM") para el presente proceso, identifica los actores y sus responsabilidades que se citan en la siguiente tabla (Ver Tabla N° 6).

Tabla N° 6:
Actores y Responsabilidades dentro del proceso de "Alta de Usuarios"

Actor Corporativo
Jefe o Gerente Responsable
Recursos Humanos
Help Desk y Mesa de ayuda
Administrador Active Directory
Administrador de Aplicaciones
Analista Módulos SAP

Nota. Actores y funciones para el proceso de "Alta y Baja de Usuarios".
Fuente: (Empresa de Consultoría para la Industria Petrolera, 2012)

La comparativa de actores Corporativos – Ecuador para este subproceso es la siguiente (ver Tabla N° 7). Esta relación está justificada por el tamaño y estructura diferente entre oficinas corporativas y Ecuador.

Tabla N° 7:
Actores para Ecuador dentro del proceso de "Alta de Usuarios"

Actor Corporativo	**Actor (Ecuador)**
Jefe o Gerente Responsable	Gerente de Área funcional
Recursos Humanos	Recursos Humanos
Help Desk y Mesa de Ayuda	Help Desk (Ingeniero de Soporte)
Administrador Active Directory	Analista de Sistemas
Administrador de Aplicaciones	Analista de Sistemas / Analista de Comunicaciones
Analista Módulos SAP	Analista Módulos SAP (Argentina)

Nota. Comparativa de funciones y responsables para el proceso de Alta y Baja de Usuarios.
Fuente: Elaboración propia de Investigador

3.1.1.3 Levantamiento del Subproceso “Modificación de Permisos de Usuarios”

a) Caracterización del Subproceso.

En la Figura N° 23 se representa la caracterización del subproceso “Modificación de Permisos de Usuario”.

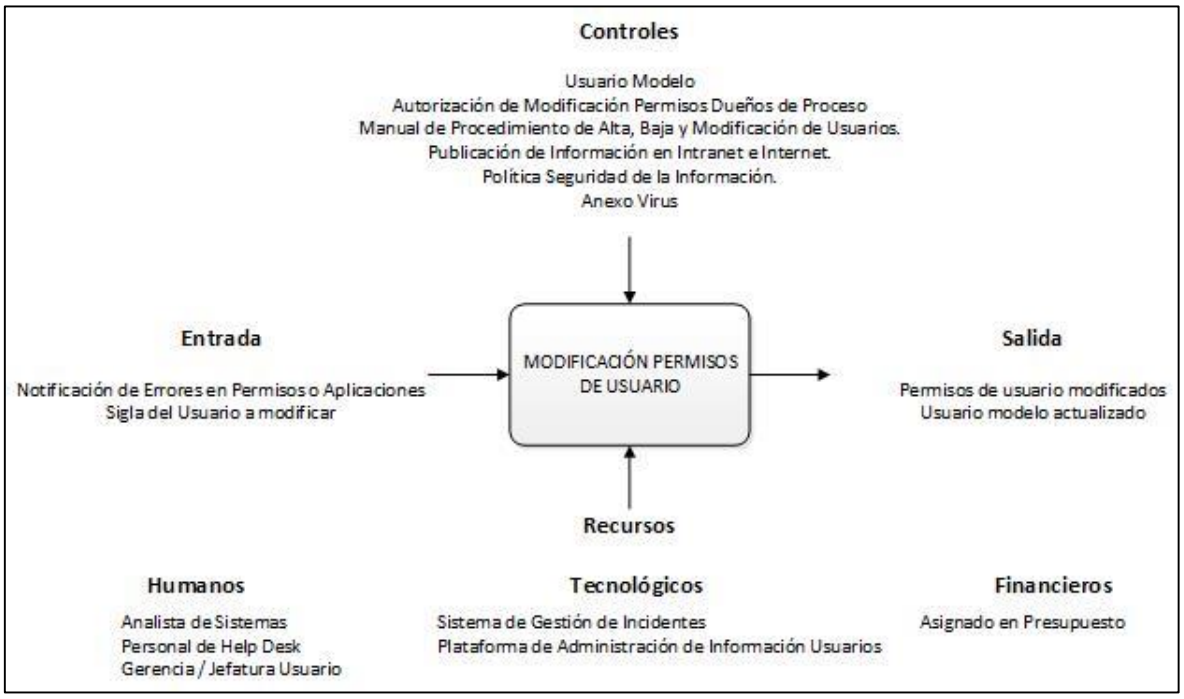


Figura N° 23: Caracterización del Subproceso de Modificación de Permisos de Usuario
Fuente: Elaboración propia del Investigador

b) Diagramas de Flujo Corporativo y Local.

Este subproceso no consta en el Manual de Procedimientos de “Alta, Baja y Modificación de Usuarios” que se maneja corporativamente, por ende se requirió desarrollar el diagrama de flujo local (ver Figura N° 24) para detallar el subproceso de “Modificación de Permisos de Usuarios” que se estaba aplicando. En este diagrama se pueden identificar las áreas responsables y las actividades que se ejecutan cada una para el subproceso.

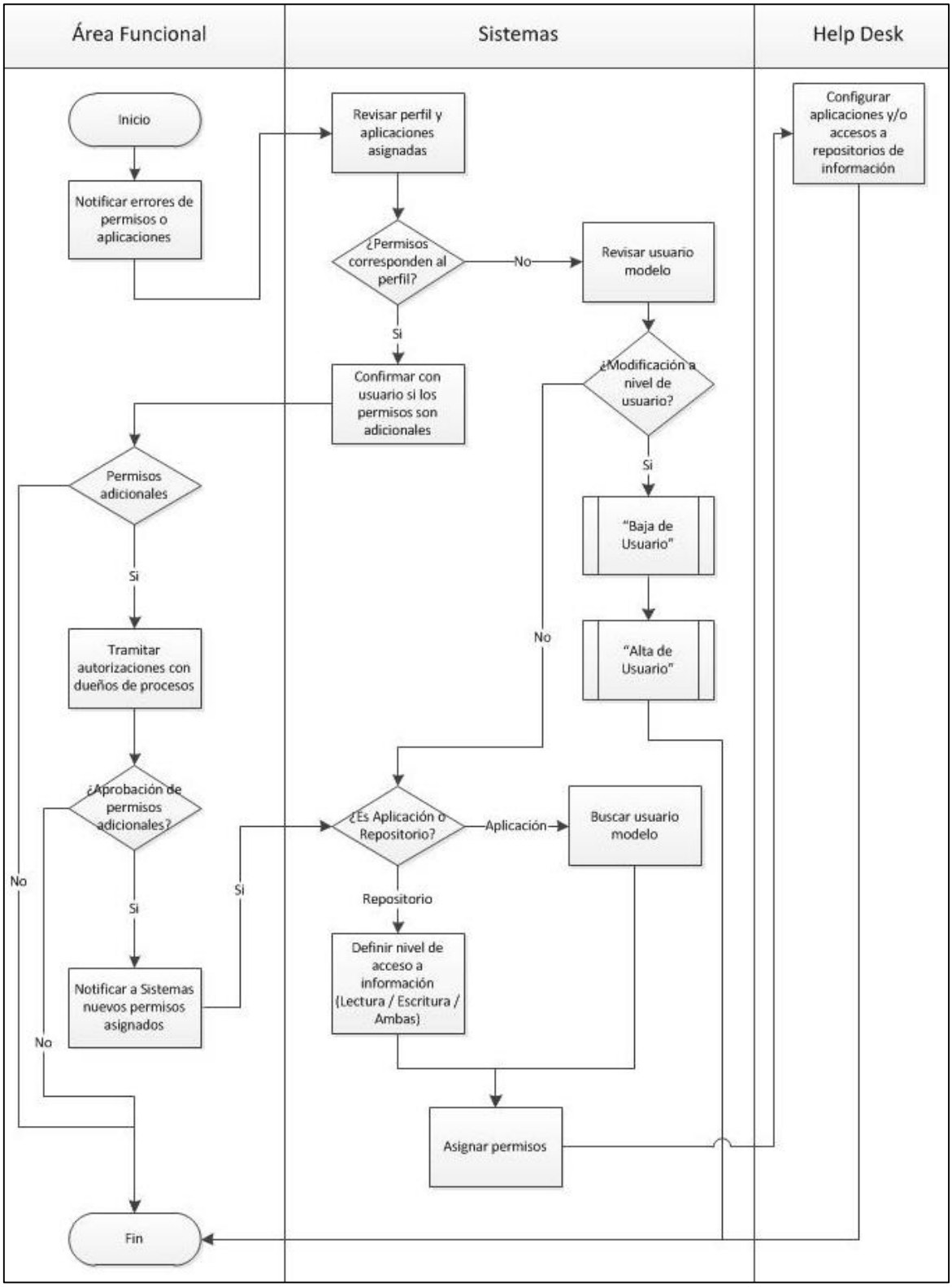


Figura N° 24: Diagrama de Flujo del Subproceso de "Modificación Permisos de Usuario"
Fuente: Elaboración propia del Investigador

c) Actores Corporativos y Locales.

La documentación existente (Manual de Procedimiento de "Alta, Baja y Modificación de Usuarios - ABM") para el presente proceso, identifica los actores y sus responsabilidades que se citan en la siguiente tabla (Ver Tabla N° 8).

Tabla N° 8:
Actores y Responsabilidades dentro del proceso de "Alta de Usuarios"

Actor Corporativo
Jefe o Gerente Responsable
Help Desk y Mesa de ayuda
Administrador Active Directory
Administrador de Aplicaciones

Nota. Actores y funciones para el proceso de "Alta y Baja de Usuarios".
Fuente: (Empresa de Consultoría para la Industria Petrolera, 2012)

La comparativa de actores Corporativos – Ecuador para este subproceso es la siguiente (ver Tabla N° 9). Esta relación está justificada por el tamaño y estructura diferente entre oficinas corporativas y Ecuador.

Tabla N° 9:
Actores para Ecuador dentro del proceso de "Alta de Usuarios".

Actor Corporativo	**Actor (Ecuador)**
Jefe o Gerente Responsable	Gerente de Área funcional
Help Desk y Mesa de Ayuda	Help Desk (Ingeniero de Soporte)
Administrador Active Directory	Analista de Sistemas
Administrador de Aplicaciones	Analista de Sistemas

Nota. Comparativa de funciones y responsables para el proceso de Alta y Baja de Usuarios.
Fuente: Elaboración propia de Investigador

3.1.2 Aplicabilidad de los requisitos de la Norma ISO 27001:2013 al proceso de "Alta y Baja de Usuarios"

En base al levantamiento de información realizado en el punto anterior, se realizó el análisis del proceso de "Alta y Baja de Usuarios" con los ciento catorce (114) Objetivos de Control y Controles que dicta la Norma ISO 27001:2013 para definir qué requisitos son aplicables y el resultado de este análisis se presenta en la Tabla N° 10.

Tabla N° 10:
Análisis de requisitos aplicables para el proceso de "Alta y Baja de Usuarios".

Objetivos de Control			Aplicable Si	Aplicable No	Subproceso Aplicable	Justificación
A.5	**Políticas de Seguridad de la Información**					
A.5.1	**Gestión de la dirección para seguridad de la información**					
Objetivo:	Proporcionar gestión de dirección y apoyo para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones pertinentes					
		Control				
A.5.1.1	Políticas de Seguridad de la Información	Grupo de políticas de seguridad de la información definidas, aprobadas por la dirección, publicadas y comunicadas a todos los empleados y terceras partes	X		Alta, Baja, Modificación de Usuarios	Definir y difundir una Política de Seguridad de la información y con la cual deben estar alineadas el resto de normas y procedimientos
		Control				
A.5.1.2	Revisión de Políticas de Seguridad de la Información	Las políticas de seguridad de la información se revisarán en intervalos previstos o si se producen cambios significativos para garantizar su idoneidad, suficiencia y efectividad	X		Alta, Baja, Modificación de Usuarios	Contar con una Política de Sistemas y Seguridad actualizada en lapsos de tiempo prudenciales, sobre la cual se sustentan el resto de procedimientos y normativas (Normativa de Alta, Baja y Modificación de usuarios) , lo cual asegura que pueda acoplarse a posibles modificaciones o cambios en la organización

Tabla N° 10:
Análisis de requisitos aplicables para el proceso de "Alta y Baja de Usuarios" (Continua).

	Objetivos de Control		Aplicable Si	Aplicable No	Subproceso Aplicable	Justificación
A.6	**Organización de Seguridad de la información**					
A.6.1	**Organización Interna**					
Objetivo:	Establecer un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización					
		Control				
A.6.1.1	Roles y responsabilidades de Seguridad de la información	Todas las responsabilidades de seguridad de la información serán definidas y asignadas	X		Alta, Baja, Modificación de Usuarios	Contar con una estructura independiente, con roles y responsabilidades definidas para administrar los puntos referentes a seguridad de la información
		Control				
A.6.1.2	Discriminación de obligaciones	Las funciones en conflicto y las áreas de responsabilidad deben ser segregados para reducir las oportunidades de modificación no autorizada o no intencional o mal uso de los activos de la organización	X		Alta, Baja, Modificación de Usuarios	Separar duplicidad o ambigüedad de obligaciones y definir quién o qué área debe ejecutar determinada acción ante un incidente de seguridad de la información
		Control				
A.6.1.3	Contacto con autoridades	Se mantendrán contactos apropiados con las autoridades pertinentes	X		Alta, Baja, Modificación de Usuarios	Definir un canal formal de comunicación y escalamiento ante cualquier incidente de seguridad, el cual debe ser conocido por toda la organización
		Control				
A.6.1.4	Contacto con grupos especiales de interés	Se mantendrán contactos apropiados con grupos de interés especial u otros foros especializados de seguridad y asociaciones profesionales.		X	-	El contacto sería con los especialistas de la organización y no necesariamente con foros o grupos fuera de la misma
A.6.1.5		***Control***				

Tabla N° 10:

Análisis de requisitos aplicables para el proceso de "Alta y Baja de Usuarios" (Continua).

	Objetivos de Control		Aplicable Si	Aplicable No	Subproceso Aplicable	Justificación
	Seguridad de la información en Administración de Proyectos	La seguridad de la información se abordará en la gestión del proyecto, independientemente del tipo de proyecto	X		Alta, Baja de Usuarios	Contar con un esquema de seguridad para todo tipo de proyecto definido por la organización y avalado por el área pertinente
A.6.2	**Dispositivos móviles y teletrabajo**					
Objetivo:	Asegurar la seguridad de teletrabajo y uso de dispositivos móviles					
		Control				
A.6.2.1	Política para dispositivos móviles	Se adoptará una política y medidas de seguridad de apoyo para gestionar el riesgo introducido por el uso de dispositivos móviles	X		Alta, Baja de Usuarios	Administrar un procedimiento para la asignación de equipos móviles que interactúe con el alta de usuarios; así también permita controlar la entrega y retiro del dispositivo al momento de una baja, así como permita difundir al usuario el buen uso de este tipo de dispositivos
		Control				
A.6.2.2	Teletrabajo	Se aplicará una política y medidas de seguridad de apoyo para proteger la información accesible, procesada o almacenada en los sitios de teletrabajo		X	-	En Ecuador no aplica la política de Teletrabajo, solo aplica para Argentina y Uruguay
A.7	**Seguridad de los recursos humanos**					
A.7.1	**Antes del empleo**					
Objetivo:	Asegurar que los empleados y los contratistas entiendan sus responsabilidades y sean adecuados para los roles para los cuales son considerados					
		Control				
A.7.1.1	Proyección	Los controles de verificación de antecedentes de todos los candidatos para el empleo se llevarán a cabo de conformidad con las leyes, reglamentos y ética pertinentes y serán proporcionales a los requerimientos de la empresa, la clasificación de la información a ser ingresada y los riesgos percibidos		X	-	El estudio se enfoca en el proceso de AB de usuarios dentro de sistemas, los controles previos realizados por otras áreas como RRHH o temas legales sobre la administración de la información de los nuevos colaboradores no es objeto del estudio
A.7.1.2		***Control***				

Tabla N° 10:
Análisis de requisitos aplicables para el proceso de "Alta y Baja de Usuarios" (Continua).

	Objetivos de Control		Aplicable Si	Aplicable No	Subproceso Aplicable	Justificación
	Términos y condiciones de empleo	Los acuerdos contractuales con los empleados y contratistas deberán establecer sus responsabilidades y la de la organización en materia de seguridad de la información		X	-	Contar con una política o acuerdo que indique al empleado sobre las responsabilidades en el tema referente a seguridad de la información, activos y debe quedar entendida, sin embargo está aún no interactúa con el proceso en estudio
A.7.2	**Durante el empleo**					
Objetivo:	Asegurar que los empleados y contratistas conozcan y cumplan sus responsabilidades de seguridad de la información					
		Control				
A.7.2.1	Administración de responsabilidades	La administración requerirá que todos los empleados y contratistas apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización	X		Alta de usuarios	Difundir y generar buenas prácticas de seguridad de la información en todos los usuarios (propios y externos) sobre el uso de activos y nivel de seguridad de la información, se debe recordar periódicamente estos puntos, así como controlar que los mismos se estén cumpliendo
		Control				
A.7.2.2	Sensibilización, educación y formación en materia de seguridad de la información	Todos los empleados de la organización y, en su caso, los contratistas recibirán una educación y capacitación apropiadas sobre la concienciación y actualizaciones regulares en las políticas y procedimientos de la organización, según sea relevante para su función de trabajo	X		Alta, Modificación de usuarios	Difundir y generar buenas prácticas de seguridad de la información en todos los usuarios (propios y externos) sobre el uso de activos y nivel de seguridad de la información, se debe recordar periódicamente estos puntos, así como controlar que los mismos se estén cumpliendo
A.7.2.3		***Control***				

Tabla N° 10:
Análisis de requisitos aplicables para el proceso de "Alta y Baja de Usuarios" (Continua).

	Objetivos de Control		Aplicable Si	Aplicable No	Subproceso Aplicable	Justificación
	Procesos disciplinarios	Habrá un proceso disciplinario formal y de comunicación para tomar acciones contra los empleados que han cometido una violación de la seguridad de la información	X		Modificación de usuarios	Validar el proceder de todo el personal de la organización respecto a controles o violaciones a la Seguridad de la Información, esto permitirá evaluar su cumplimiento y puede derivar en procesos disciplinarios internos por su no aplicación e inclusive sanciones que aplicables conforme la legislación local
A.7.3	**Terminación y cambio de empleo**					
Objetivo:	Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo					
		Control				
A.7.3.1	Terminación o cambio de responsabilidades laborales	Las responsabilidades y deberes de seguridad de la información que permanezcan vigentes después de la terminación o cambio de empleo serán definidos, comunicados al empleado o contratista y puestos en vigor	X		Baja de usuarios	Contar con una política para la baja de usuarios que indique el proceso, lineamientos y responsables para ejecutar este subproceso
A.8	**Gestión de activos**					

Tabla N° 10:
Análisis de requisitos aplicables para el proceso de "Alta y Baja de Usuarios" (Continua).

	Objetivos de Control		Aplicable Si	Aplicable No	Subproceso Aplicable	Justificación
A.8.1	**Responsabilidad de los activos**					
Objetivo:	Identificar los activos de la organización y definir las responsabilidades de protección apropiadas					
		Control				
A.8.1.1	Inventario de activos	Información asociada a los activos deberán ser identificada, elaborada y mantenida en un inventario	X		Alta de usuarios	Administrar los activos de la organización, permitiendo contar con: información actualizada, llevar la trazabilidad, registro de movimiento y/o asignación de los mismos, así también permite asignar activos (equipos) a un nuevo usuario (alta) o retirar activos (baja o modificación), para ello se debe contar con un procedimiento de asignación formal, inventario actualizado de activos y control de asignación/disponibilidad de los mismos
		Control				
A.8.1.2	Propiedad de activos	Los activos serán registrados y mantendrán en el inventario	X		Alta, Baja de usuarios	Administrar los activos de la organización, permitiendo contar con: información actualizada, llevar la trazabilidad, registro de movimiento y/o asignación de los mismos, así también permite asignar activos (equipos) a un nuevo usuario (alta) o retirar activos (baja o modificación), para ello se debe contar con un procedimiento de asignación formal, inventario actualizado de activos y control de asignación/disponibilidad de los mismos
A.8.1.3		***Control***				

Tabla N° 10:
Análisis de requisitos aplicables para el proceso de "Alta y Baja de Usuarios" (Continua).

	Objetivos de Control		Aplicable Si	Aplicable No	Subproceso Aplicable	Justificación
	Uso aceptable de activos	Las reglas para el uso aceptable de la información y de los activos asociados con las instalaciones de procesamiento de información e información deben ser identificadas, documentadas e implementadas	X		Alta de usuarios	Difundir a todos los usuarios los lineamientos para el buen uso de los activos (hardware, software) asignados por parte de la empresa, además de administrar los activos de la organización, permitiendo contar con: información actualizada, llevar la trazabilidad, registro de movimiento y/o asignación de los mismos, así también permite asignar activos (equipos) a un nuevo usuario (alta) o retirar activos (baja o modificación), para ello se debe contar con un procedimiento de asignación formal, inventario actualizado de activos y control de asignación/disponibilidad de los mismos
		Control				
A.8.1.4	Regreso de activos	Todos los empleados y usuarios de partes externas devolverán todos los activos de la organización en su poder al finalizar su empleo, contrato o acuerdo	X		Baja de usuarios	Definir el procedimiento de retiro de activos (hardware/software) ante una baja, además de administrar los activos de la organización, permitiendo contar con: información actualizada, llevar la trazabilidad, registro de movimiento y/o asignación de los mismos, así también permite asignar activos (equipos) a un nuevo usuario (alta) o retirar activos (baja o modificación), para ello se debe contar con un procedimiento de asignación formal, inventario actualizado de activos y control de asignación/disponibilidad de los mismos
A.8.2	**Clasificación de la Información**					

Tabla N° 10:

Análisis de requisitos aplicables para el proceso de "Alta y Baja de Usuarios" (Continua).

	Objetivos de Control		Aplicable Si	Aplicable No	Subproceso Aplicable	Justificación
Objetivo:	Asegurar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organización					
		Control				
A.8.2.1	Clasificación de la información	La información se clasificará en términos de requisitos legales, valor, criticidad y sensibilidad a la divulgación o modificación no autorizada	X		Alta, Modificación de usuarios	Definir niveles de seguridad (criticidad y tratamiento) de la información y por contar con niveles de aprobación para su acceso, así también difundir con el usuario la importancia y criticidad que tiene la misma para la organización
		Control				
A.8.2.2	Etiquetado de información	Se elaborará y aplicará un conjunto adecuado de procedimientos para el etiquetado de la información de conformidad con el esquema de clasificación de información adoptado por la organización		X	-	La información además de contar con niveles de seguridad, debe ser etiquetada para que quienes acceden a la misma entiendan el nivel de importancia, criticidad y daño que podría causar su mal uso, este proceso está fuera de estudio, ya que el etiquetado se realiza por fuera de cualquier subproceso y no depende de los mismos
A.8.2.3		***Control***				

Tabla N° 10:
Análisis de requisitos aplicables para el proceso de "Alta y Baja de Usuarios" (Continua).

	Objetivos de Control		Aplicable Si	Aplicable No	Subproceso Aplicable	Justificación
	Manejo de activos	Los procedimientos para el manejo de los activos se desarrollarán e implementarán de acuerdo con el esquema de clasificación de información adoptado por la organización	X		Alta de usuarios	Definir el buen manejo de los activos y las herramientas que existen para precautelar la integridad del activo así como la información que almacena, además de administrar los activos de la organización, permitiendo contar con: información actualizada, llevar la trazabilidad, registro de movimiento y/o asignación de los mismos, así también permite asignar activos (equipos) a un nuevo usuario (alta) o retirar activos (baja o modificación), para ello se debe contar con un procedimiento de asignación formal, inventario actualizado de activos y control de asignación/disponibilidad
A.8.3	**Manejo de Medios**					
Objetivo:	Para evitar la divulgación, modificación, eliminación o destrucción no autorizadas de la información almacenada en los medios					
		Control				
A.8.3.1	Gestión de medios extraíbles	Se aplicarán procedimientos para la gestión de medios extraíbles de conformidad con el esquema de clasificación adoptado por la organización		X	-	Si bien los medios extraíbles son parte de la clasificación de información y manejo de activos, no está dentro del proceso en estudio abordar el uso de los mismos, ya que no están atados o influyen en el mismo
		Control				
A.8.3.2	Eliminación de medios	Los medios deben ser eliminados de manera segura cuando ya no se requiera, usando procedimientos formales		X	-	Si bien los medios extraíbles son parte de la clasificación de información y manejo de activos, no está dentro del proceso en estudio abordar el uso de los mismos, ya que no están atados o influyen en el mismo
A.8.3.3		***Control***				

Tabla N° 10:
Análisis de requisitos aplicables para el proceso de "Alta y Baja de Usuarios" (Continua).

	Objetivos de Control		Aplicable Si	Aplicable No	Subproceso Aplicable	Justificación
	Transferencia de medios físicos	Los medios que contengan información deberán estar protegidos contra el acceso no autorizado, el mal uso o la corrupción durante el transporte		X	-	Si bien los medios extraíbles son parte de la clasificación de información y manejo de activos, no está dentro del proceso en estudio abordar el uso de los mismos, ya que no están atados o influyen en el mismo
A.9	**Control de Acceso**					
A.9.1	**Requerimientos empresariales de control de acceso**					
Objetivo:	Limitar el acceso a la información e instalaciones de procesamiento de la información					
		Control				
A.9.1.1	Política de Control de Acceso	Se establecerá, documentará y revisará una política de control de acceso basada en los requisitos de seguridad empresarial y de información	X		Alta de usuarios	Contar con una política y/o procedimiento que defina los lineamientos para controlar el acceso de todos los usuarios, definiendo roles y niveles de acceso a las diferentes locaciones de la organización así como restringir sitios que son de exclusivo acceso para personal especializado (Ejemplo: Acceso a Data Center solo personal Sistemas)
		Control				
A.9.1.2	Acceso a redes y servicios de redes	Los usuarios sólo tendrán acceso a la red y a los servicios de red que hayan sido específicamente autorizados a utilizar	X		Alta de usuarios	Asignar permisos de accesos a repositorios de información (lectura, escritura o ambos) y privilegios para utilizar la red corporativa (Ejemplo: Acceso a Internet o únicamente Intranet) de manera correcta acorde al perfil del usuario ante una nueva alta o modificación de usuarios, así como eliminar los permisos otorgados y que tenga vigentes al ejecutar su baja
A.9.2	**Gestión de acceso de los usuarios**					

Tabla N° 10:
Análisis de requisitos aplicables para el proceso de "Alta y Baja de Usuarios" (Continua).

	Objetivos de Control		Aplicable Si	Aplicable No	Subproceso Aplicable	Justificación
Objetivo:	Garantizar el acceso de los usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios					
		Control				
A.9.2.1	Registro y cancelación de registro del usuario	Se llevará a cabo un proceso formal de registro y cancelación de registro de usuarios para habilitar la asignación de derechos de acceso	X		Alta, Baja, Modificación de usuarios	Asignar permisos de accesos a repositorios de información (lectura, escritura o ambos) y privilegios para utilizar la red corporativa (Ejemplo: Acceso a Internet o únicamente Intranet) de manera correcta acorde al perfil del usuario ante una nueva alta o modificación de usuarios, así como eliminar los permisos otorgados y que tenga vigentes al ejecutar su baja
		Control				
A.9.2.2	Provisión de acceso de usuario	Proceso formal de provisión de acceso de usuario será implementado para asignar o revocar derechos de acceso para todo tipo de usuario a todos los sistemas y servicios	X		Alta de Usuarios	La vinculación de un colaborador o cambio de asignación comprende justamente la correcta asignación de permisos a los diferentes repositorios de información y aplicaciones
		Control				
A.9.2.3	Gestión de derechos de acceso privilegiados	La asignación y el uso de los derechos de acceso privilegiados serán restringidos y controlados		X	-	Bajo ningún motivo se deben manejar excepciones o privilegios adicionales para el acceso a repositorios o aplicaciones, estos casos se dan fuera del proceso por petición explicita del Country Manager
		Control				
A.9.2.4	Gestión de la información de autenticación secreta de los usuarios	La asignación de información secreta de autenticación se controlará mediante un proceso de gestión formal		X	-	Los registros de autenticación de usuarios en la red no interactúan con el proceso de estudio, están más enfocados en puntos de auditoria para validar que se lleve un registro de acceso a repositorios o aplicaciones, más no su asignación a los mismos
A.9.2.5		***Control***				

Tabla N° 10:
Análisis de requisitos aplicables para el proceso de "Alta y Baja de Usuarios" (Continua).

	Objetivos de Control		Aplicable Si	Aplicable No	Subproceso Aplicable	Justificación
	Revisión de los derechos de acceso de los usuarios	Los propietarios de activos deberán revisar los derechos de acceso de los usuarios a intervalos regulares	X		Alta, Modificación de usuarios	Asignar permisos de accesos a repositorios de información (lectura, escritura o ambos) y privilegios para utilizar la red corporativa (Ejemplo: Acceso a Internet o únicamente Intranet) de manera correcta acorde al perfil del usuario ante una nueva alta o modificación de usuarios, así como eliminar los permisos otorgados y que tenga vigentes al ejecutar su baja
		Control				
A.9.2.6	Eliminación o ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y usuarios de partes externas a las instalaciones de procesamiento de información e información se eliminarán al finalizar su empleo, contrato o acuerdo, o ajustarse al cambiar	X		Modificación de usuarios	Controlar la baja de permisos de acceso a usuarios (internos / externos) que finalicen sus servicios profesionales con la organización
A.9.3	**Responsabilidades del usuario**					
Objetivo:	Responsabilizar a los usuarios por la protección de su información de autenticación					
		Control				
A.9.3.1	Uso de la información secreta de autenticación	El usuario deberá seguir las prácticas de la organización en el uso de la información de autenticación secreta	X		Alta de usuarios	Definir y difundir las responsabilidades sobre el manejo de información, claves y permisos de acceso a nuevos colaboradores (alta)
A.9.4	**Control de acceso a sistemas y aplicaciones**					

Tabla N° 10:
Análisis de requisitos aplicables para el proceso de "Alta y Baja de Usuarios" (Continua).

	Objetivos de Control		Aplicable Si	Aplicable No	Subproceso Aplicable	Justificación
Objetivo:	Prevenir el acceso no autorizado a sistemas y aplicaciones					
		Control				
A.9.4.1	Restricción de acceso a la información	El acceso a la información y las funciones del sistema de aplicación se restringirán de conformidad con la política de control de acceso	X		Alta de usuarios	Asignar permisos de accesos a repositorios de información (lectura, escritura o ambos) y privilegios para utilizar la red corporativa (Ejemplo: Acceso a Internet o únicamente Intranet) de manera correcta acorde al perfil del usuario ante una nueva alta o modificación de usuarios, así como eliminar los permisos otorgados y que tenga vigentes al ejecutar su baja
		Control				
A.9.4.2	Procedimientos de conexión segura	Cuando así lo exija la política de control de acceso, el acceso a sistemas y aplicaciones se controlará mediante un procedimiento seguro de conexión		X	-	La conexión segura corresponde a un lineamiento de seguridad global y no interactúa con el proceso en estudio
		Control				
A.9.4.3	Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y garantizar contraseñas de calidad		X	-	La gestión de contraseñas no interactúa con el proceso en estudio, es un punto que aplica para el acceso a sistemas y uso de los mismos, que se debe cumplir en base al lineamiento corporativo
		Control				
A.9.4.4	Uso de programas de utilidad privilegiada	El uso de programas de utilidad que podrían ser capaces de anular los controles del sistema y aplicación debe ser restringido y controlado estrictamente		X	-	No existe excepción para el uso de programas que podrían anular controles de seguridad, en el caso de presentarse esta excepción no influiría en el proceso en estudio sino estaría enfocado en casos puntuales
		Control				
A.9.4.5	Control de acceso al código fuente del programa	Acceso al código fuente del programa debe ser restringido		X	-	En Ecuador no existe área de desarrollo por ende este punto no aplica
A.10	**Criptografía**					
A.10.1	**Controles Criptográficos**					

Tabla N° 10:
Análisis de requisitos aplicables para el proceso de "Alta y Baja de Usuarios" (Continua).

	Objetivos de Control		Aplicable Si	Aplicable No	Subproceso Aplicable	Justificación
Objetivo:	Asegurar un uso adecuado y efectivo de la criptografía para proteger la confidencialidad, autenticidad e integridad de la información					
		Control				
A.10.1.1	Política sobre el uso de controles criptográficos	Se elaborará y aplicará una política sobre el uso de los controles criptográficos para la protección de la información	X		Alta de usuarios	Aplicar los controles de seguridad (criptografía, claves de seguridad temporales, PIN de acceso, claves de acceso de usuarios) con los que cuentan todos los equipos de la organización, difundirlos a los usuarios y registrarlos mediante una política para poder revisarlos y actualizarlos conforme se lo requiera
		Control				
A.10.1.2	Gestión de claves	Se desarrollará y aplicará una política sobre el uso, la protección y la duración de las claves criptográficas durante todo su ciclo de vida	X		Alta, Baja de usuarios	Aplicar los controles de seguridad (criptografía, claves de seguridad temporales, PIN de acceso, claves de acceso de usuarios) con los que cuentan todos los equipos de la organización, difundirlos a los usuarios y registrarlos mediante una política para poder revisarlos y actualizarlos conforme se lo requiera
A.11	**Seguridad física y ambiental**					
A.11.1	**Áreas seguras**					
Objetivo:	Evitar accesos físicos no autorizados, daños e interferencias a las instalaciones de procesamiento de información e información de la organización					
		Control				
A.11.1.1	Seguridad perimetral física	Se definirán perímetros de seguridad y utilizarán para proteger las áreas que contengan información sensible o crítica e instalaciones de procesamiento de información	X		Alta de Usuarios	Aplicar normas para acceso a áreas restringidas (Ejemplo: Centros de Datos) donde únicamente podrá acceder personal específico y con el respectivo registro de acceso, igual aplica para las credenciales de acceso para el personal y pueda ingresar a oficinas, campamentos y demás facilidades
A.11.1.2		***Control***				

Tabla N° 10:
Análisis de requisitos aplicables para el proceso de "Alta y Baja de Usuarios" (Continua).

	Objetivos de Control		Aplicable Si	Aplicable No	Subproceso Aplicable	Justificación
	Controles físicos de entrada	Las zonas seguras deben estar protegidas por controles de entrada apropiados para garantizar que sólo el personal autorizado tenga acceso		X	-	La seguridad física no influye con el proceso en estudio, aplica lineamiento propios del área de Seguridad Física a los cuales se acopla el proceso en estudio pero no interactúa
		Control				
A.11.1.3	Asegurar oficinas, cuartos e instalaciones	Seguridad física para oficinas, cuartos y facilidades deben ser diseñadas y aplicadas		X	-	La seguridad física no influye con el proceso en estudio, aplica lineamiento propios del área de Seguridad Física a los cuales se acopla el proceso en estudio pero no interactúa
		Control				
A.11.1.4	Protección contra las amenazas externas y ambientales	Protección física contra desastres naturales, ataques maliciosos o accidentes deben ser diseñados y aplicados		X	-	Las amenazas externas o ambientales no interactúan con el proceso en estudio y serían parte de la política y responsabilidad del área de Seguridad Física
		Control				
A.11.1.5	Trabajo en áreas seguras	Procedimientos para trabajar en áreas seguras debe ser diseñado y aplicado		X	-	Este punto no interactúa con el proceso en estudio, sería parte de la política y responsabilidad del área de Seguridad Ambiental y Salud
		Control				
A.11.1.6	Zonas de entrega y carga	Los puntos de acceso, tales como las áreas de entrega / carga y otros puntos en los que personas no autorizadas puedan entrar en las instalaciones, serán controlados y, de ser posible, aislados de las instalaciones de procesamiento de información para evitar el acceso no autorizado		X	-	Este punto no interactúa con el proceso en estudio y serían parte de la política y responsabilidad del área de Seguridad Física y del área de Seguridad Ambiental y Salud
A.11.2	**Equipo**					

Tabla N° 10:
Análisis de requisitos aplicables para el proceso de "Alta y Baja de Usuarios" (Continua).

	Objetivos de Control		Aplicable Si	Aplicable No	Subproceso Aplicable	Justificación
Objetivo:	Evitar pérdidas, daños, robo o compromiso de los activos e interrupción de las operaciones de la organización					
		Control				
A.11.2.1	Ubicación de equipos y protección	Los equipos deberán estar situados y protegidos para reducir el riesgo de amenazas ambientales y las oportunidades de acceso no autorizado		X	-	La ubicación de equipos y su protección no está dentro del proceso en estudio, esto corresponde a la definición de RRHH sobre la ubicación del usuario y de Seguridad Física que define la seguridad perimetral y protección de equipos
		Control				
A.11.2.2	Utilidades de apoyo	El equipo debe estar protegido contra fallas de energía y otras interrupciones causadas por fallas en los servicios de apoyo		X	-	Cableado estructurado, protecciones eléctricas y seguridad en los centros de datos no están dentro del proceso en estudio, estos puntos los administra Seguridad Física y los lineamientos generales de Facilidades
		Control				
A.11.2.3	Seguridad de cableado	Los cables de energía y telecomunicaciones que transporten datos o servicios de información de apoyo deberán estar protegidos contra intercepciones, interferencias o daños		X	-	Cableado estructurado, protecciones eléctricas y seguridad en los centros de datos no están dentro del proceso en estudio, estos puntos los administra Seguridad Física y los lineamientos generales de Facilidades
		Control				
A.11.2.4	Mantenimiento de equipo	El equipo debe mantenerse correctamente para asegurar su continua disponibilidad e integridad		X	-	El mantenimiento preventivo o correctivo de equipos asignados al usuario no interactúa con el proceso en estudio
		Control				
A.11.2.5	Eliminación de activos	Equipos, información o software no deben ser extraídos fuera del sitio sin autorización previa		X	-	Aplica para la política de uso de activos de la organización pero que no influye en el proceso en estudio
A.11.2.6		***Control***				

Tabla N° 10:
Análisis de requisitos aplicables para el proceso de "Alta y Baja de Usuarios" (Continua).

	Objetivos de Control		Aplicable Si	Aplicable No	Subproceso Aplicable	Justificación
	Seguridad de equipos y activos fuera de las instalaciones	La seguridad se aplicará a los activos fuera de sitio teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización	X		Alta de usuarios	Abarcar además de la protección del activo (mediante contratación de seguros), velar por el buen funcionamiento (contratación de garantías), considera usar claves y controles criptográficos para salvaguardar la información que se almacena en los mismos, aplica en especial para equipos portátiles/móviles asignados a los usuarios que pueden ser trasladados fueras de las oficinas o campamentos y pueden ser susceptibles a robos, pérdidas o daños
		Control				
A.11.2.7	Eliminación segura o reutilización del equipo	Todos los elementos del equipo que contengan medios de almacenamiento deberán ser verificados para asegurar que los datos sensibles y el software bajo licencia hayan sido eliminados o sobrescritos de forma segura antes de su eliminación o reutilización	X		Baja de usuarios	Contar con un procedimiento que asegure que al equipo que es retirado (baja) debe realizarse el formateo y respaldo de información del mismo antes de poder reutilizarlo y asignarlo a un nuevo usuario, detallando los responsables de la ejecución del respaldo y custodio de la información
		Control				
A.11.2.8	Equipo desatendido de usuario	Los usuarios deberán asegurarse de que el equipo desatendido tiene la protección adecuada		X	-	El uso cotidiano de los equipos así como las medidas de seguridad que debe aplicar el usuario (bloquear equipos desatendidos) no es parte del proceso en estudio
		Control				
A.11.2.9	Política de escritorio y pantalla limpia	Se adoptará una política de escritorio limpio de papeles y medios de almacenamiento extraíbles y una política de pantalla limpia para las instalaciones de procesamiento de información		X	-	El uso cotidiano de los equipos así como las medidas de seguridad que debe aplicar el usuario (bloquear equipos desatendidos) no es parte del proceso en estudio
A.12	**Seguridad operacional**					

Tabla N° 10:
Análisis de requisitos aplicables para el proceso de "Alta y Baja de Usuarios" (Continua).

	Objetivos de Control		Aplicable Si	Aplicable No	Subproceso Aplicable	Justificación
A.12.1	**Procedimientos y responsabilidades operacionales**					
Objetivo:	Asegurar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información					
		Control				
A.12.1.1	Procedimientos operativos documentados	Los procedimientos operativos deberán documentarse y ponerse a disposición de todos los usuarios que los necesiten		X	-	Existe una política específica para la administración de centros de datos (almacenamiento, procesamiento y/o desarrollo) así como los planes de contingencia de los mismos, los cuales no dependen o interactúan con el proceso en estudio
		Control				
A.12.1.2	Gestión del cambio	Los cambios en la organización, los procesos de negocio, las instalaciones de procesamiento de información y los sistemas que afectan a la seguridad de la información deben ser controlados		X	-	Existe una política específica para la administración de centros de datos (almacenamiento, procesamiento y/o desarrollo) así como los planes de contingencia de los mismos, los cuales no dependen o interactúan con el proceso en estudio
		Control				
A.12.1.3	Gestión de la capacidad	El uso de los recursos será monitoreado, ajustado y realizarán proyecciones de los requerimientos futuros de capacidad para asegurar el desempeño del sistema requerido		X	-	Existe una política específica para la administración de centros de datos (almacenamiento, procesamiento y/o desarrollo) así como los planes de contingencia de los mismos, los cuales no dependen o interactúan con el proceso en estudio
		Control				
A.12.1.4	Separación de entornos de desarrollo, prueba y operación	Los entornos de desarrollo, prueba y operación deben estar separados para reducir el riesgo de acceso no autorizado o cambios en el entorno operacional		X	-	Existe una política específica para la administración de centros de datos (almacenamiento, procesamiento y/o desarrollo) así como los planes de contingencia de los mismos, los cuales no dependen o interactúan con el proceso en estudio
A.12.2	**Protección contra el malware**					

Tabla N° 10:

Análisis de requisitos aplicables para el proceso de "Alta y Baja de Usuarios" (Continua).

	Objetivos de Control		Aplicable Si	Aplicable No	Subproceso Aplicable	Justificación
Objetivo:	Garantizar que la información y las instalaciones de procesamiento de información estén protegidas contra el malware					
		Control				
A.12.2.1	Controles contra el malware	Se implementarán controles de detección, prevención y recuperación para proteger contra el malware, combinados con el conocimiento apropiado del usuario	X		Alta de usuarios	Contar con herramientas de control de virus estandarizadas y su respectivo procedimiento para implementarlas en los equipos antes de ser entregados a los usuarios, las mismas deben ser evaluadas periódicamente para verificar su buen funcionamiento y actualización
A.12.3	**Copia de seguridad**					
Objetivo:	Proteger contra la perdida de información					
		Control				
A.12.3.1	Copia de seguridad de información	Copias de seguridad de la información, software e imágenes del sistema se tomarán y probarán periódicamente de acuerdo con una política de respaldo acordada	X		Alta de usuarios	Valida que se ejecuten copias de respaldo y ejecute el software corporativo de réplica hacia los repositorios de información, así como definir vigencia de respaldos y responsables de custodio de información
A.12.4	**Registro y monitoreo**					
Objetivo:	Para registrar eventos y generar evidencia					
		Control				
A.12.4.1	Registro de sucesos	Registros de eventos que registran actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información deberán ser realizados, mantenidos y revisados regularmente		X	-	El registro y monitoreo de eventos / actividades no está dentro del proceso en estudio, esto implica actividades de auditoría y control
		Control				
A.12.4.2	Protección del registro de información	Registros de instalaciones y registros de información estarán protegidos contra la manipulación y acceso no autorizado		X	-	El registro y monitoreo de eventos / actividades no está dentro del proceso en estudio, esto implica actividades de auditoría y control
A.12.4.3		***Control***				

Tabla N° 10:
Análisis de requisitos aplicables para el proceso de "Alta y Baja de Usuarios" (Continua).

	Objetivos de Control		Aplicable Si	Aplicable No	Subproceso Aplicable	Justificación
	Registros del administrador y del operador	Las actividades del administrador del sistema y del operador del sistema deberán ser registradas y los registros protegidos y revisados periódicamente		X	-	El registro y monitoreo de eventos / actividades no está dentro del proceso en estudio, esto implica actividades de auditoría y control
		Control				
A.12.4.4	Sincronización de reloj	Los relojes de todos los sistemas de procesamiento de información relevantes dentro de una organización o dominio de seguridad se sincronizarán con una única fuente de tiempo de referencia		X	-	La sincronización de reloj de Sistemas (aplicaciones e infraestructura) no está dentro del proceso en estudio
A.12.5	**Control de software operativo**					
Objetivo:	Asegurar la integridad de los sistemas operativos					
		Control				
A.12.5.1	Instalación de software en sistemas operativos	Se implementarán procedimientos para controlar la instalación de software en sistemas operativos	X		Alta de usuarios	Contar con herramientas y procedimientos que permitan controlar la instalación de software (Sistema Operativo) estándar para la organización y los controles para que los usuarios puedan instalar software o características adicionales al mismo
A.12.6	**Gestión de vulnerabilidades técnicas**					
Objetivo:	Evitar la explotación de vulnerabilidades técnicas					
		Control				
A.12.6.1	Gestión de vulnerabilidades técnicas	La información sobre las vulnerabilidades técnicas de los sistemas de información que se utilicen se obtendrá oportunamente, se evaluará la exposición de la organización a dichas vulnerabilidades y se adoptarán medidas apropiadas para abordar el riesgo asociado		X	-	La gestión de vulnerabilidades es un proceso a parte y no interactúa con el proceso en estudio
A.12.6.2		***Control***				

Tabla N° 10:
Análisis de requisitos aplicables para el proceso de "Alta y Baja de Usuarios" (Continua).

	Objetivos de Control		Aplicable Si	Aplicable No	Subproceso Aplicable	Justificación
	Restricción en la instalación del software	Normas que rigen la instalación de software por parte de los usuarios se establecerán e implementarán	X		Alta de usuarios	Contar con herramientas y procedimientos que permitan controlar la instalación de software (Sistema Operativo) estándar para la organización y los controles para que los usuarios puedan instalar software o características adicionales al mismo
A.12.7	**Consideraciones sobre la auditoría de los sistemas de información**					
Objetivo:	Minimizar el impacto de las actividades de auditoría en los sistemas operativos					
		Control				
A.12.7.1	Controles de auditoría de sistemas de información	Los requisitos de auditoría y las actividades que impliquen la verificación de los sistemas operativos se planificarán y acordarán cuidadosamente para minimizar las interrupciones en los procesos de negocio		X	-	Los controles o planificación de auditorías no son parte del proceso en estudio
A.13	**Seguridad de las comunicaciones**					
A.13.1	**Gestión de la seguridad de la red**					
Objetivo:	Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información					
		Control				
A.13.1.1	Controles de red	La red será gestionada y controlada para proteger la información en sistemas y aplicaciones		X	-	Los controles en la red se aplican independiente del proceso de Alta y Baja de usuarios
		Control				
A.13.1.2	Seguridad de los servicios de red	Los mecanismos de seguridad, los niveles de servicios y los requisitos de gestión de todos los servicios de red se identificarán e incluirán en los acuerdos de servicios de red, ya se trate de servicios internos o subcontratado		X	-	Los controles en la red se aplican independiente del proceso de Alta y Baja de usuarios
A.13.1.3		***Control***				

Tabla N° 10:
Análisis de requisitos aplicables para el proceso de "Alta y Baja de Usuarios" (Continua).

	Objetivos de Control		Aplicable Si	Aplicable No	Subproceso Aplicable	Justificación
	Segregación en redes	Los grupos de servicios de información, usuarios y sistemas de información se segregarán en redes		X	-	El diseño y aplicación de la segmentación de la red se aplica independiente del proceso de Alta y Baja de usuarios
A.13.2	**Transferencia de información**					
Objetivo:	Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa					
		Control				
A.13.2.1	Políticas y procedimientos de transferencia de información	Se establecerán políticas, procedimientos y controles de transferencia formal para proteger la transferencia de información mediante el uso de todo tipo de medios de comunicación		X	-	La transferencia de información es un proceso independiente que administra el área de Sistemas y está enmarcado en los procedimientos de transmisión, replica y respaldo de información
		Control				
A.13.2.2	Acuerdos sobre transferencia de información	Acuerdos deberán abordar la transferencia segura de información comercial entre la organización y las partes externas		X	-	La transferencia de información es un proceso independiente que administra el área de Sistemas y está enmarcado en los procedimientos de transmisión, replica y respaldo de información
		Control				
A.13.2.3	Mensajería electrónica	La información relacionada con la mensajería electrónica estará debidamente protegida	X		Alta de usuarios	Contar con herramientas y canales de comunicación seguros, así como software que salvaguarde la información referente a mensajería electrónica
A.13.2.4		***Control***				

Tabla N° 10:
Análisis de requisitos aplicables para el proceso de "Alta y Baja de Usuarios" (Continua).

	Objetivos de Control		Aplicable Si	Aplicable No	Subproceso Aplicable	Justificación
	Acuerdos de confidencialidad o no divulgación	Los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de protección de la organización serán identificados, revisados y documentados periódicamente	X		Alta de usuarios	Definir y difundir para todos los usuarios los acuerdos de confidencialidad y no divulgación de información que lleva la empresa y a la cual están sujetos, en el mismo se deben especifica las sanciones que pueden acarrear el incumplimiento de los mismos, adicional al momento de entregar el equipo y configurar la cuenta de usuario se recuerda este particular. Considerar también que si bien la empresa mantiene políticas y sanciones internas ante la violación de acuerdos de confidencialidad, en el Ecuador mediante el COIP se pueden revisar las sanciones que pueden derivarse de un hecho que comprometa la información de carácter privado
A.14	**Adquisición, desarrollo y mantenimiento de sistemas**					
A.14.1	**Requisitos de seguridad de los sistemas de información**					
Objetivo:	Asegurar que la seguridad de la información es una parte integral del sistema de información a lo largo de todo el ciclo de vida. Esto incluye también los requisitos para los sistemas de información que proporcionan servicios a través de redes públicas					
		Control				
A.14.1.1	Análisis y especificaciones de requisitos de seguridad de la información	Los requisitos relacionados con la seguridad de la información se incluirán en los requisitos para nuevos sistemas de información o mejoras en los sistemas de información existentes		X	-	La adquisición, desarrollo o mejoras de nuevos sistemas de información no interactúa con el proceso de Alta y Baja de usuarios
A.14.1.2		***Control***				

Tabla N° 10:
Análisis de requisitos aplicables para el proceso de "Alta y Baja de Usuarios" (Continua).

	Objetivos de Control		Aplicable Si	Aplicable No	Subproceso Aplicable	Justificación
	Asegurar servicios de aplicación en redes públicas	La información involucrada en los servicios de aplicación que pasa por redes públicas estará protegida contra actividad fraudulenta, disputa contractual, divulgación y modificación no autorizada		X	-	La transmisión de datos por redes públicas no involucra el proceso de Alta y Baja de usuarios
		Control				
A.14.1.3	Protección de transacciones de servicios de aplicaciones	La información involucrada en las transacciones de servicios de aplicación estará protegida para evitar la transmisión incompleta, el enrutamiento erróneo, la alteración no autorizada de mensajes, la divulgación no autorizada, la duplicación o reproducción no autorizada de mensajes		X	-	La transmisión de datos por redes públicas y la no divulgación de información no afecta o involucra el proceso de Alta y Baja de usuarios
A.14.2	**Seguridad en procesos de desarrollo y soporte**					
Objetivo:	Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida del desarrollo de los sistemas de información					
		Control				
A.14.2.1	Política de desarrollo seguro	Se establecerán y aplicarán reglas para el desarrollo de software y sistemas a los desarrollos dentro de la organización		X	-	No existe área de desarrollo en Ecuador, por ende no aplica
		Control				
A.14.2.2	Procedimientos de control de cambios del sistema	Los cambios en los sistemas dentro del ciclo de vida del desarrollo se controlarán mediante el uso de procedimientos formales de control de cambios		X	-	No existe área de desarrollo en Ecuador, por ende no aplica
A.14.2.3		***Control***				

Tabla N° 10:
Análisis de requisitos aplicables para el proceso de "Alta y Baja de Usuarios" (Continua).

	Objetivos de Control		Aplicable Si	Aplicable No	Subproceso Aplicable	Justificación
	Revisión técnica de aplicaciones tras cambios en la plataforma operativa	Cuando se cambien las plataformas operativas, las aplicaciones críticas de negocio serán revisadas y probadas para asegurar que no haya impacto adverso en las operaciones de la organización o en la seguridad		X	-	No existe área de desarrollo en Ecuador, por ende no aplica
		Control				
A.14.2.4	Restricciones a los cambios en los paquetes de software	Las modificaciones a los paquetes de software deberán ser rechazadas, limitadas a los cambios necesarios y todos los cambios deberán ser estrictamente controlados		X	-	No existe área de desarrollo en Ecuador, por ende no aplica
		Control				
A.14.2.5	Principios seguros de ingeniería de sistemas	Los principios para la ingeniería de sistemas seguros se establecerán, documentarán, se mantendrán y se aplicarán a cualquier esfuerzo de implementación del sistema de información		X	-	No existe área de desarrollo en Ecuador, por ende no aplica
		Control				
A.14.2.6	Entorno de desarrollo seguro	La Organización establecerá y protegerá apropiadamente los entornos de desarrollo seguro para los esfuerzos de desarrollo e integración del sistema que abarquen todo el ciclo de desarrollo del sistema		X	-	No existe área de desarrollo en Ecuador, por ende no aplica
		Control				
A.14.2.7	Desarrollo subcontratado	La organización supervisará y monitoreará la actividad de desarrollo de sistemas subcontratado		X	-	No existe área de desarrollo en Ecuador, por ende no aplica
		Control				
A.14.2.8	Pruebas de seguridad del sistema	Las pruebas de funcionalidad de seguridad se llevarán a cabo durante el desarrollo		X	-	No existe área de desarrollo en Ecuador, por ende no aplica
A.14.2.9		***Control***				

Tabla N° 10:
Análisis de requisitos aplicables para el proceso de "Alta y Baja de Usuarios" (Continua).

	Objetivos de Control		Aplicable Si	Aplicable No	Subproceso Aplicable	Justificación
	Pruebas de aceptación del sistema	Se establecerán programas de pruebas de aceptación y criterios relacionados para los nuevos sistemas de información, actualizaciones y nuevas versiones		X	-	No existe área de desarrollo en Ecuador, por ende no aplica
A.14.3	**Datos de prueba**					
Objetivo:	Para garantizar la protección de los datos utilizados para las pruebas					
		Control				
A.14.3.1	Protección de datos de prueba	Los datos de prueba se seleccionarán cuidadosamente, se protegerán y se controlarán		X	-	No existe área de pruebas en Ecuador, por ende no aplica
A.15	**Relaciones con proveedores**					
A.15.1	**Seguridad de la información en las relaciones con proveedores**					
Objetivo:	Asegurar la protección de los activos de la organización a los que pueden acceder los proveedores					
		Control				
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	Requisitos de seguridad de la información para mitigar el riesgo asociado con el acceso del proveedor a los activos de la organización serán acordados con el proveedor y documentados	X		Alta de usuarios	Difundir y generar buenas prácticas de seguridad de la información en todos los usuarios (propios y externos) sobre el uso de activos y nivel de seguridad de la información, se debe recordar periódicamente estos puntos, así como controlar que los mismos se estén cumpliendo
		Control				
A.15.1.2	Abordar la seguridad dentro de los acuerdos de proveedores	Todos los requerimientos relevantes de seguridad de la información serán establecidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI para la información de la organización	X		Alta de usuarios	Difundir y generar buenas prácticas de seguridad de la información en todos los usuarios (propios y externos) sobre el uso de activos y nivel de seguridad de la información, se debe recordar periódicamente estos puntos, así como controlar que los mismos se estén cumpliendo
A.15.1.3		***Control***				

Tabla N° 10:
Análisis de requisitos aplicables para el proceso de "Alta y Baja de Usuarios" (Continua).

	Objetivos de Control		Aplicable Si	Aplicable No	Subproceso Aplicable	Justificación
	Cadena de suministro de tecnología de la información y comunicación	Los acuerdos con proveedores incluirán requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información, las comunicaciones y la cadena de suministro de productos	X		Alta de usuarios	Difundir y generar buenas prácticas de seguridad de la información en todos los usuarios (propios y externos) sobre el uso de activos y nivel de seguridad de la información, se debe recordar periódicamente estos puntos, así como controlar que los mismos se estén cumpliendo
A.15.2	**Gestión de la entrega de servicios de proveedores**					
Objetivo:	Mantener un nivel de acuerdo de seguridad de la información y prestación de servicios en línea con los acuerdos de proveedores					
		Control				
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	Las organizaciones deben monitorear, revisar y auditar regularmente la prestación de servicios del proveedor		X	-	Los servicios que brinden los proveedores están fuera del proceso o no influyen con el Alta y Baja de usuarios
		Control				
A.15.2.2	Gestión de cambios en los servicios de proveedores	Los cambios en la prestación de servicios por parte de los proveedores, incluido el mantenimiento, mejora de las políticas, procedimientos y controles de seguridad de la información existentes; se administrarán teniendo en cuenta la criticidad de la información comercial, los sistemas, procesos implicados y la reevaluación de los riesgos		X	-	Los servicios que brinden los proveedores están fuera del proceso o no influyen con el Alta y Baja de usuarios
A.16	**Gestión de incidentes de seguridad de la información**					

Tabla N° 10:

Análisis de requisitos aplicables para el proceso de "Alta y Baja de Usuarios" (Continua).

	Objetivos de Control		Aplicable Si	Aplicable No	Subproceso Aplicable	Justificación
A.16.1	**Gestión de incidentes y mejoras en seguridad de la información**					
Objetivo:	Asegurar un enfoque coherente y efectivo para la gestión de incidentes de seguridad de la información, incluyendo la comunicación sobre eventos y debilidades de seguridad					
		Control				
A.16.1.1	Responsabilidades y procedimientos	Gestión de responsabilidades y procedimientos para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información	X		Alta, Baja, Modificación de usuarios	Definir la cadena de comunicación, medio y responsables ante un evento de seguridad, este contacto inicialmente debería ser interno y ser el canal de enlace en el caso que se requiera intervención de organismos o entidades externas
		Control				
A.16.1.2	Reporte de eventos de seguridad de la información	Los eventos de seguridad de la información deben ser reportados a través de canales de administración apropiados tan pronto como sea posible	X		Alta, Baja, Modificación de usuarios	Definir la cadena de comunicación, medio y responsables ante un evento de seguridad, este contacto inicialmente debería ser interno y ser el canal de enlace en el caso que se requiera intervención de organismos o entidades externas
		Control				
A.16.1.3	Informar sobre las debilidades en la seguridad de la información	Los empleados y contratistas que utilicen los sistemas y servicios de información de la organización deberán tomar nota de cualquier falla observada o presunta debilidad de seguridad de la información en sistemas o servicios	X		Alta, Baja, Modificación de usuarios	Generar el compromiso de personal propio y externo (proveedores) para que informen sobre posibles debilidades en la administración de seguridad de la información que podrían afectar a la organización
		Control				
A.16.1.4	Evaluación y decisión sobre los eventos de seguridad de la información	Se evaluarán los eventos de seguridad de la información y se decidirá si se van a clasificar como incidentes de seguridad de la información		X	-	Se considera un procedimiento general enfocado en el diagnóstico de incidentes de seguridad en cualquier proceso
A.16.1.5		***Control***				

Tabla N° 10:

Análisis de requisitos aplicables para el proceso de "Alta y Baja de Usuarios" (Continua).

	Objetivos de Control		Aplicable Si	Aplicable No	Subproceso Aplicable	Justificación
	Respuesta a incidentes de seguridad de la información	Se responderá a los incidentes de seguridad de la información de conformidad con los procedimientos documentados		X	-	Se considera un procedimiento general enfocado en el diagnóstico de incidentes de seguridad en cualquier proceso
		Control				
A.16.1.6	Aprender de los incidentes de seguridad de la información	Los conocimientos obtenidos del análisis y resolución de incidentes de seguridad de la información se utilizarán para reducir la probabilidad o el impacto de futuros incidentes		X	-	Se considera un procedimiento general enfocado en el diagnóstico de incidentes de seguridad en cualquier proceso
		Control				
A.16.1.7	Recolección de pruebas	La organización deberá definir y aplicar procedimientos para la identificación, recolección, adquisición y conservación de la información, que puedan servir como prueba		X	-	Se considera un procedimiento general enfocado en el diagnóstico de incidentes de seguridad en cualquier proceso
A.17	**Aspectos de la seguridad de la información en la gestión de la continuidad del negocio**					
A.17.1	**Continuidad de la seguridad de la información**					
Objetivo:	La continuidad de la seguridad de la información se integrará en los sistemas de gestión de continuidad del negocio					
		Control				
A.17.1.1	Planificación de la continuidad de la seguridad de la información	La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo: durante una crisis o un desastre		X	-	Proceso enfocado en planes de contingencia que no están dentro del proceso de Alta y Baja de usuarios
A.17.1.2		***Control***				

Tabla N° 10:
Análisis de requisitos aplicables para el proceso de "Alta y Baja de Usuarios" (Continua).

	Objetivos de Control		Aplicable Si	Aplicable No	Subproceso Aplicable	Justificación
	Implementación de la continuidad de la seguridad de la información	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad para la seguridad de la información durante una situación adversa		X	-	Proceso enfocado en planes de contingencia que no están dentro del proceso de Alta y Baja de usuarios
		Control				
A.17.1.3	Verificar, revisar y evaluar la continuidad de la seguridad de la información	La organización verificará el control de continuidad de seguridad de la información establecido y aplicado, a intervalos regulares a fin de asegurar que sean válidos y eficaces durante situaciones adversas		X	-	Proceso enfocado en planes de contingencia que no están dentro del proceso de Alta y Baja de usuarios
A.17.2	**Redundancias**					
Objetivo:	Asegurar la disponibilidad de instalaciones de procesamiento de información					
		Control				
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	Las instalaciones de procesamiento de la información se implementarán con una redundancia suficiente para satisfacer los requisitos de disponibilidad		X	-	Enfocado a centros de datos alternos que aseguren la disponibilidad y que no interactúa con el proceso de Alta y Baja de usuarios
A.18	**Cumplimiento**					

Tabla N° 10:

Análisis de requisitos aplicables para el proceso de "Alta y Baja de Usuarios" (Continua).

	Objetivos de Control		Aplicable Si	Aplicable No	Subproceso Aplicable	Justificación
A.18.1	**Cumplimiento de las exigencias legales y contractuales**					
Objetivo:	Para evitar infracciones legales, estatutarias, reglamentarias u obligaciones contractuales relacionadas con la seguridad de la información y de cualquier requerimiento de seguridad					
		Control				
A.18.1.1	Identificación de la legislación aplicable y requisitos contractuales	Todos los requisitos legislativos, regulatorios y contractuales relevantes, y el enfoque de la organización para cumplir con estos requisitos deberán ser identificados, documentados y actualizados explícitamente para cada sistema de información y la organización		X	-	El proceso de Alta y Baja de usuarios define controles y normativas corporativas que se ajustan a la legislación de cada país, sin embargo no se incluye este análisis dentro del proceso ya que en el ámbito contractual es donde se revisarían estos puntos, por ende no aplica dentro del proceso en estudio
		Control				
A.18.1.2	Derechos de propiedad intelectual	Se aplicarán procedimientos adecuados para garantizar el cumplimiento de los requisitos legislativos, regulatorios y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados		X	-	El proceso de Alta y Baja de usuarios define controles y normativas corporativas que se ajustan a la legislación de cada país, sin embargo no se incluye este análisis dentro del proceso ya que en el ámbito contractual es donde se revisarían estos puntos, por ende no aplica dentro del proceso en estudio
		Control				
A.18.1.3	Protección de registros	Los registros estarán protegidos contra la pérdida, destrucción, falsificación, acceso y liberación no autorizada, de conformidad con los requisitos legislativos, regulatorios, contractuales y comerciales		X	-	El proceso de Alta y Baja de usuarios define controles y normativas corporativas que se ajustan a la legislación de cada país, sin embargo no se incluye este análisis dentro del proceso ya que en el ámbito contractual es donde se revisarían estos puntos, por ende no aplica dentro del proceso en estudio
A.18.1.4		***Control***				

Tabla N° 10:
Análisis de requisitos aplicables para el proceso de "Alta y Baja de Usuarios" (Continua).

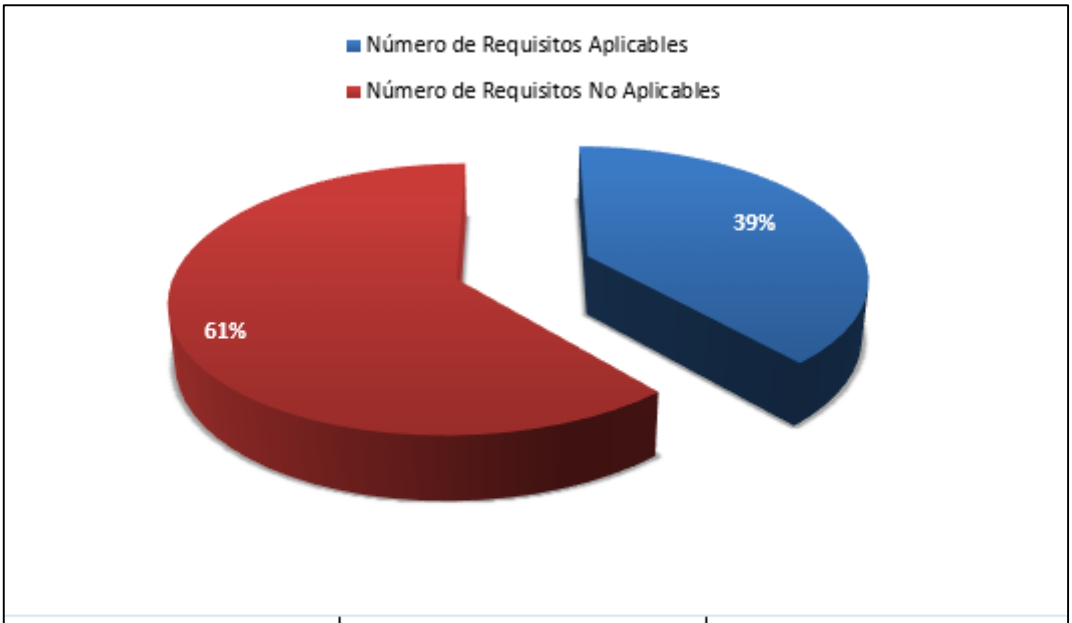
	Objetivos de Control		Aplicable Si	Aplicable No	Subproceso Aplicable	Justificación
	Privacidad y protección de información de identificación personal	Se garantizará la privacidad y la protección de la información de identificación personal, según se requiera en la legislación y la regulación pertinentes donde sea aplicable		X	-	El proceso de Alta y Baja de usuarios define controles y normativas corporativas que se ajustan a la legislación de cada país, sin embargo no se incluye este análisis dentro del proceso ya que en el ámbito contractual es donde se revisarían estos puntos, por ende no aplica dentro del proceso en estudio
		Control				
A.18.1.5	Regulación de los controles criptográficos	Los controles criptográficos se utilizarán de conformidad con todos los acuerdos, leyes y regulaciones pertinentes		X	-	Se utilizan controles criptográficos estándares y acorde a las licencias del software que se utiliza, más el análisis de los mismos no está dentro del proceso en estudio
A.18.2	**Revisión de seguridad de la información**					
Objetivo:	Asegurar que la seguridad de la información sea implementada y operada de acuerdo con las políticas y procedimientos de la organización					
		Control				
A.18.2.1	Revisión independiente de la seguridad de la información	El enfoque de la organización para administrar la seguridad de la información y su implementación (es decir, objetivos de control, controles, procesos de políticas y procedimientos para la seguridad de la información) será revisado independientemente a intervalos planificados o cuando ocurran cambios significativos	X		Alta, Baja, Modificación de usuarios	Contar con una evaluación Interna / Externa para validar que se cumplen las Políticas, normas y procedimientos de seguridad de la información
A.18.2.2		***Control***				

Tabla N° 10:
Análisis de requisitos aplicables para el proceso de "Alta y Baja de Usuarios" (Continua).

	Objetivos de Control		Aplicable Si	Aplicable No	Subproceso Aplicable	Justificación
	Cumplimiento de las políticas y estándares de seguridad	Los administradores revisarán periódicamente el cumplimiento del procesamiento de información y los procedimientos dentro de su área de responsabilidad con las políticas de seguridad adecuadas, estándares y cualquier otro requisito de seguridad	X		Alta, Baja, Modificación de usuarios	Contar con una evaluación Interna / Externa para validar que se cumplen las Políticas, normas y procedimientos de seguridad de la información
		Control				
A.18.2.3	Revisión del cumplimiento técnico	Los sistemas de información se revisarán periódicamente para verificar el cumplimiento de las políticas y normas de seguridad de la información de la organización		X	-	La revisión de los sistemas de información está fuera del proceso en estudio

Nota. Base de referencia para análisis 114 Objetivos de Control y Controles de la Norma ISO 27001:2013.
Fuente: Elaboración propia de Investigador

Una vez realizado el análisis de requisitos aplicables, en base a los ciento catorce Objetivos de Control y Controles que cita la Norma ISO 27001:2013 en el proceso de "Alta y Baja de Usuarios", la Figura N° 25 muestra el resultado de los requisitos que son aplicables al proceso en investigación.



Número Total de Requisitos	Número de Requisitos Aplicables	Número de Requisitos No Aplicables
114	44	70

Figura N° 25: Resultados Objetivos de Control y Controles aplicado al Proceso de "Alta y Baja de Usuarios".
Fuente: Elaboración propia del Investigador

3.1.3 Nivel de Cumplimiento de los requerimientos aplicables de la Norma ISO 27001:2013 al proceso de "Alta y Baja de Usuarios"

Considerando los requisitos aplicables de la Norma ISO 27001:2013 identificados, se procedió a definir el nivel de cumplimiento de cada uno de ellos y su vinculación con el requisito legal vigente para el Ecuador.

Las escalas de cumplimiento utilizadas se detallan en la Tabla N° 11.

Tabla N° 11:
Escalas de Cumplimiento de objetivos respecto a la Norma ISO 27001:2013 para el proceso de "Alta y Baja de Usuarios"

Escala	Significado	Leyenda
Si	Cumplimiento Total	
Parcial	Cumplimiento Parcial	
No	Incumplimiento Total	

Nota. Escala desarrollada para la medición de cumplimiento de objetivos.
Fuente: Elaboración propia de Investigador

Los resultados de esta evaluación se presentan en las siguientes tablas (Ver Tablas N° 12 hasta la Tabla N° 29):

Tabla N° 12:
A.5 Objetivo de Control - Políticas de Seguridad de la Información aplicable para el proceso de "Alta y Baja de Usuarios".

	Objetivos de Control		Si	No	Parcial	Evidencia	Observaciones	Artículo de Requisito Legal Vinculado
A.5	**Políticas de Seguridad de la Información**							
A.5.1	**Gestión de la dirección para seguridad de la información**							
Objetivo:	Proporcionar gestión de dirección y apoyo para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones pertinentes							
		Control						
A.5.1.1	Políticas de Seguridad de la Información	Grupo de políticas de seguridad de la información definidas, aprobadas por la dirección, publicadas y comunicadas a todos los empleados y terceras partes	X			Política de Sistemas (ENE 10 SI PO 002) Política Seguridad de Información (ENE 08 SI PO 001)	Todos los documentos normativos como: Políticas, Códigos, Procedimientos y Normas están publicados en la Intranet de la Organización y disponibles para todos los usuarios para que puedan acceder y revisarlos.	N/A

Tabla N° 12:

A.5 Objetivo de Control - Políticas de Seguridad de la Información aplicable para el proceso de "Alta y Baja de Usuarios" (Continua).

		Objetivos de Control	Si	No	Parcial	Evidencia	Observaciones	Artículo de Requisito Legal Vinculado
		Control						
A.5.1.2	Revisión de Políticas de Seguridad de la Información	Las políticas de seguridad de la información se revisarán en intervalos previstos o si se producen cambios significativos para garantizar su idoneidad, suficiencia y efectividad		X		Política de Sistemas (ENE 10 SI PO 002) Política Seguridad de Información (ENE 08 SI PO 001)	Políticas desactualizadas: Política de Sistemas (ENE 10 SI PO 002) – Desactualizada, última revisión 2010. Política Seguridad de Información (ENE 08 SI PO 001) – Desactualizada, última revisión 2008.	N/A

Nota. Objetivos de Control y Controles aplicables al proceso de "Alta y Baja de Usuarios" en base a la Norma ISO 27001:2013.
Fuente: Elaboración propia de Investigador

Tabla N° 13:

A.6 Objetivo de Control – Organización de Seguridad de la información aplicable para el proceso de "Alta y Baja de Usuarios".

	Objetivos de Control		Si	No	Parcial	Evidencia	Observaciones	Artículo de Requisito Legal Vinculado
A.6	**Organización de Seguridad de la información**							
A.6.1	**Organización Interna**							
Objetivo:	Establecer un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización							
		Control						
A.6.1.1	Roles y responsabilidades de Seguridad de la información	Todas las responsabilidades de seguridad de la información serán definidas y asignadas	X			Política Seguridad de Información (ENE 08 SI PO 001)	La Política de Seguridad de la Información enuncia claramente los responsables y funciones para cada área, delegando un Administrador de Seguridad de la Información para administrar lo referente a este punto.	N/A

Tabla N° 13:
A.6 Objetivo de Control – Organización de Seguridad de la información aplicable para el proceso de "Alta y Baja de Usuarios" (Continua).

		Objetivos de Control	Si	No	Parcial	Evidencia	Observaciones	Artículo de Requisito Legal Vinculado
		Control						
A.6.1.2	Discriminación de obligaciones	Las funciones en conflicto y las áreas de responsabilidad deben ser segregados para reducir las oportunidades de modificación no autorizada o no intencional o mal uso de los activos de la organización	X			Política Seguridad de Información (ENE 08 SI PO 001)	La Política de Seguridad de la Información enuncia claramente los responsables y funciones para cada área, delegando un Administrador de Seguridad de la Información para administrar lo referente a este punto.	N/A
		Control						
A.6.1.3	Contacto con autoridades	Se mantendrán contactos apropiados con las autoridades pertinentes			X	Norma DIAMM S04 - Lineamientos generales de administración y seguridad para las Redes y Sistemas de la Organización	No existe una sección donde se detalle el flujo para contacto interno ante incidentes de Seguridad y/o contacto externo, ante eventos que ameriten inclusión de autoridades (fraudes o delitos que atenten contra la información y/o activos de tecnología de la organización).	COIP, Sección Tercera
A.6.1.4	Contacto con grupos especiales de interés	***Control***						
		Control						
A.6.1.5	Seguridad de la información en Administración de Proyectos	La seguridad de la información se abordará en la gestión del proyecto, independientemente del tipo de proyecto	X			Política Seguridad de Información (ENE 08 SI PO 001)	El concepto de seguridad de la información se aplica para todo proyecto (infraestructura y desarrollo) y es enunciado en la Política de Seguridad.	N/A

Tabla N° 13:

A.6 Objetivo de Control – Organización de Seguridad de la información aplicable para el proceso de "Alta y Baja de Usuarios" (Continua).

		Objetivos de Control	Si	No	Parcial	Evidencia	Observaciones	Artículo de Requisito Legal Vinculado
A.6.2	**Dispositivos móviles y teletrabajo**							
Objetivo:	Asegurar la seguridad de teletrabajo y uso de dispositivos móviles							
		Control						
A.6.2.1	Política para dispositivos móviles	Se adoptará una política y medidas de seguridad de apoyo para gestionar el riesgo introducido por el uso de dispositivos móviles			X	Norma Utilización de dispositivos móviles (TEC 15 SI NO 001) Procedimiento de Alta, Baja y Modificación de Usuarios (ENE 12 SI IS PR 001) Procedimiento de Gestión de Activos de IT (ENE 10 SI IT PR 003)	Norma Utilización de dispositivos móviles - 3.4 Monitoreo y Control: Se detalla que la empresa asume los costos por la activación del dispositivo móvil así como los cargos que genere el mismo, pero al momento de dar de baja un usuario entra en conflicto la propiedad de la línea telefónica, donde el usuario solicita quedarse con la línea para su uso personal y la cual pertenece a la empresa ya que en el punto 3.4 se detalla que el dispositivo móvil se utilizará exclusivamente con fines laborales y "eventualmente" con fines personal, el no detallar la propiedad de la línea, genera conflictos al momento de dar da baja una línea ya que el usuario generalmente ancla a la mayoría de sus actividades personales a la línea asignada. Norma Utilización de dispositivos móviles revisada en el 2015. Procedimiento de Alta, Baja y Modificación de Usuarios - 5.2.2 Baja de Usuarios - Análisis y Ejecución: No se incluye al momento de la ejecución de la Baja	N/A

Tabla N° 13:

A.6 Objetivo de Control – Organización de Seguridad de la información aplicable para el proceso de "Alta y Baja de Usuarios" (Continua).

	Objetivos de Control	Si	No	Parcial	Evidencia	Observaciones	Artículo de Requisito Legal Vinculado
						del usuario el retiro de equipos asignados. Procedimiento de Gestión de Activos de IT, punto 3. Responsabilidades - Responsable de Sistemas de áreas: Cita la entrega y actualización del inventario, más no detalla retiro de equipos por bajas de usuario o bajas de equipos en el inventario por daño, robos y cualquier evento que afecte a los equipos/activos entregados.	

Nota. Objetivos de Control y Controles aplicables al proceso de "Alta y Baja de Usuarios" en base a la Norma ISO 27001:2013.

Fuente: Elaboración propia de Investigador

Tabla N° 14:

A.7 Objetivo de Control – Seguridad de los recursos humanos aplicable para el proceso de "Alta y Baja de Usuarios".

	Objetivos de Control		Si	No	Parcial	Evidencia	Observaciones	Artículo de Requisito Legal Vinculado
A.7	**Seguridad de los recursos humanos**							
A.7.2	**Durante el empleo**							
Objetivo:	Asegurar que los empleados y contratistas conozcan y cumplan sus responsabilidades de seguridad de la información							
		Control						
A.7.2.1	Administración de responsabilidades	La administración requerirá que todos los empleados y contratistas apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización	X			Política Seguridad de Información (ENE 08 SI PO 001)	La Política de Seguridad de la Información, punto 3. Responsabilidades y Control, cita las responsabilidades de los colaboradores respecto a Seguridad y la obligatoriedad de informarse sobre las normativas de seguridad de la información que deben cumplir.	N/A
		Control						
A.7.2.2	Sensibilización, educación y formación en materia de seguridad de la información	Todos los empleados de la organización y, en su caso, los contratistas recibirán una educación y capacitación apropiadas sobre la concienciación y actualizaciones regulares en las políticas y procedimientos de la organización, según sea relevante para su función de trabajo	X			Política Seguridad de Información (ENE 08 SI PO 001)	La Política de Seguridad de la Información punto 3. Responsabilidades y Control, cita las responsabilidades de los colaboradores respecto a Seguridad de Sistemas y la obligatoriedad de informarse sobre las normativas de seguridad de la información que deben cumplir.	N/A
		Control						
A.7.2.3	Procesos disciplinarios	Habrá un proceso disciplinario formal y de comunicación para tomar acciones contra los empleados que han cometido una violación de la seguridad de la información			X	Norma DIAMM S04 - Lineamientos generales de administración y seguridad para las Redes y Sistemas de la Organización	No existe una sección donde se detalle el flujo para contacto interno ante incidentes de Seguridad y/o contacto externo, ante eventos que ameriten inclusión de autoridades (fraudes o delitos que atenten contra la información y/o activos de tecnología de la organización).	COIP, Sección Tercera

Tabla N° 14:

A.7 Objetivo de Control – Seguridad de los recursos humanos aplicable para el proceso de "Alta y Baja de Usuarios" (Continua).

	Objetivos de Control		Si	No	Parcial	Evidencia	Observaciones	Artículo de Requisito Legal Vinculado
A.7.3	**Terminación y cambio de empleo**							
Objetivo:	Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo							
		Control						
A.7.3.1	Terminación o cambio de responsabilidades laborales	Las responsabilidades y deberes de seguridad de la información que permanezcan vigentes después de la terminación o cambio de empleo serán definidos, comunicados al empleado o contratista y puestos en vigor	X			Procedimiento de Alta, Baja y Modificación de Usuarios (ENE 12 SI IS PR 001)	El Procedimiento detalla responsables, acciones, comunicación y flujo para ejecutar la baja de usuarios.	N/A

Nota. Objetivos de Control y Controles aplicables al proceso de "Alta y Baja de Usuarios" en base a la Norma ISO 27001:2013.

Fuente: Elaboración propia de Investigador

Tabla N° 15:

A.8 Objetivo de Control – Gestión de Activos aplicable para el proceso de "Alta y Baja de Usuarios".

	Objetivos de Control		Si	No	Parcial	Evidencia	Observaciones	Artículo de Requisito Legal Vinculado
A.8	**Gestión de activos**							
A.8.1	**Responsabilidad de los activos**							
Objetivo:	Identificar los activos de la organización y definir las responsabilidades de protección apropiadas							
		Control						
A.8.1.1	Inventario de activos	Información asociada a los activos deberán ser identificada, elaborada y mantenida en un inventario			X	Procedimiento de Gestión de Activos de IT (ENE 10 SI IT PR 003) Sistema de Inventarios (Inventar) Planilla de Asignación / Retiro de Activos	Procedimiento de Gestión de Activos de IT, punto 3. Responsabilidades - Responsable de Sistemas de áreas: Cita la entrega y actualización del inventario, más no detalla retiro de equipos por bajas de usuario o bajas de equipos en el inventario por daño, robos y cualquier evento que afecte a los equipos/activos entregados. Sistema de Inventarios: Inventario de equipos de Ecuador desactualizado. Planilla de Asignación / Retiro de Equipos: Desactualizada, sin formato específico y su control se lo hace manualmente.	N/A

Tabla N° 15:
A.8 Objetivo de Control – Gestión de Activos aplicable para el proceso de "Alta y Baja de Usuarios" (Continua).

		Objetivos de Control	Si	No	Parcial	Evidencia	Observaciones	Artículo de Requisito Legal Vinculado
		Control						
A.8.1.2	Propiedad de activos	Los activos serán registrados y mantendrán en el inventario			X	Procedimiento de Gestión de Activos de IT (ENE 10 SI IT PR 003) Sistema de Inventarios (Inventar) Planilla de Asignación / Retiro de Activos	Procedimiento de Gestión de Activos de IT, punto 3. Responsabilidades - Responsable de Sistemas de áreas: Cita la entrega y actualización del inventario, más no detalla retiro de equipos por bajas de usuario o bajas de equipos en el inventario por daño, robos y cualquier evento que afecte a los equipos/activos entregados. Sistema de Inventarios: Inventario de equipos de Ecuador desactualizado. Planilla de Asignación / Retiro de Equipos: Desactualizada, sin formato específico y su control se lo hace manualmente.	N/A

Tabla N° 15:

A.8 Objetivo de Control – Gestión de Activos aplicable para el proceso de "Alta y Baja de Usuarios" (Continua).

		Objetivos de Control	Si	No	Parcial	Evidencia	Observaciones	Artículo de Requisito Legal Vinculado
		Control						
A.8.1.3	Uso aceptable de activos	Las reglas para el uso aceptable de la información y de los activos asociados con las instalaciones de procesamiento de información e información deben ser identificadas, documentadas e implementadas			X	Norma DIAMM 7.01 - Uso Herramientas Electrónicas de Comunicación Procedimiento de Gestión de Activos de IT (ENE 10 SI IT PR 003) Planilla de Asignación / Retiro de Activos	La Norma DIAMM 7.01 - Uso Herramientas Electrónicas de Comunicación en su punto 2.1 Uso Aceptable, detalla sobre el buen uso de los activos, sin embargo es recomendable registrar la instrucción al usuario sobre este punto al momento de la entrega de los equipos. El Procedimiento de Gestión de Activos de IT (ENE 10 SI IT PR 003) no detalla un proceso de control para validar el buen uso de los activos, ni responsables para esta actividad. El control de activos que incluye al software, no tiene un parámetro para su validación (Software estándar). El control de activos que incluye al software, no tiene un control sobre la instalación/desinstalación del mismo en los computadores asignados a los usuarios.	N/A

Tabla N° 15:

A.8 Objetivo de Control – Gestión de Activos aplicable para el proceso de "Alta y Baja de Usuarios" (Continua).

		Objetivos de Control	Si	No	Parcial	Evidencia	Observaciones	Artículo de Requisito Legal Vinculado
		Control						
A.8.1.4	Regreso de activos	Todos los empleados y usuarios de partes externas devolverán todos los activos de la organización en su poder al finalizar su empleo, contrato o acuerdo			X	Procedimiento de Alta, Baja y Modificación de Usuarios (ENE 12 SI IS PR 001) Procedimiento de Gestión de Activos de IT (ENE 10 SI IT PR 003)	Procedimiento de Alta, Baja y Modificación de Usuarios - 5.2.2 Baja de Usuarios - Análisis y Ejecución: No se incluye al momento de su ejecución el retiro de equipos asignados al personal. Procedimiento de Alta, Baja y Modificación de Usuarios - 5.2.2 Baja de Usuarios - Análisis y Ejecución: No se incluye al momento de la ejecución de la Baja del usuario el retiro de equipos asignados.	N/A
A.8.2	**Clasificación de la Información**							
Objetivo:	Asegurar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organización							
		Control						
A.8.2.1	Clasificación de la información	La información se clasificará en términos de requisitos legales, valor, criticidad y sensibilidad a la divulgación o modificación no autorizada			X	Norma DIAMM S04 - Lineamientos generales de administración y seguridad para las Redes y Sistemas de la Organización	La Norma DIAMM S04 - Lineamientos generales de administración y seguridad para las Redes y Sistemas de la Organización, en su punto 3. Confidencialidad y seguridad de los datos, cita los términos Información Confidencial o Sensitiva y el manejo de la misma, sin embargo, no se detallan la clasificación de la información que maneja actualmente la empresa.	N/A

Tabla N° 15:

A.8 Objetivo de Control – Gestión de Activos aplicable para el proceso de "Alta y Baja de Usuarios" (Continua).

		Objetivos de Control	Si	No	Parcial	Evidencia	Observaciones	Artículo de Requisito Legal Vinculado
		Control						
A.8.2.3	Manejo de activos	Los procedimientos para el manejo de los activos se desarrollarán e implementarán de acuerdo con el esquema de clasificación de información adoptado por la organización		X		Norma DIAMM S04 - Lineamientos generales de administración y seguridad para las Redes y Sistemas de la Organización Procedimiento de Gestión de Activos de IT (ENE 10 SI IT PR 003)	La Norma DIAMM S04 - Lineamientos generales de administración y seguridad para las Redes y Sistemas de la Organización en su punto 3. Confidencialidad y seguridad de los datos, cita los términos Información Confidencial o Sensitiva y el manejo de la misma, sin embargo, no se detallan la clasificación de la información que maneja actualmente la empresa. La Norma DIAMM S04 - Lineamientos generales de administración y seguridad para las Redes y Sistemas de la Organización en su punto 3.8, cita el especial cuidado que debe tener el personal de sistemas respecto a control de virus, pero no detalla los controles que existen para salvaguardar la información de los usuarios (encriptación, PIN de seguridad, clave de Windows, respaldo de información, software antivirus, parches de seguridad, ente otros.)	N/A

Nota. Objetivos de Control y Controles aplicables al proceso de "Alta y Baja de Usuarios" en base a la Norma ISO 27001:2013.

Fuente: Elaboración propia de Investigador

Tabla N° 16:

A.9 Objetivo de Control – Control de Acceso aplicable para el proceso de "Alta y Baja de Usuarios".

	Objetivos de Control		Si	No	Parcial	Evidencia	Observaciones	Artículo de Requisito Legal Vinculado
A.9	**Control de Acceso**							
A.9.1	**Requerimientos empresariales de control de acceso**							
Objetivo:	Limitar el acceso a la información e instalaciones de procesamiento de la información							
		Control						
A.9.1.1	Política de Control de Acceso	Se establecerá, documentará y revisará una política de control de acceso basada en los requisitos de seguridad empresarial y de información			X	Norma DIAMM S04 - Lineamientos generales de administración y seguridad para las Redes y Sistemas de la Organización Procedimiento Protección Física (ENE 09 SI IT PR 002) Procedimiento de Alta, Baja y Modificación de Usuarios (ENE 12 SI IS PR 001)	La Norma DIAMM S04 - Lineamientos generales de administración y seguridad para las Redes y Sistemas de la Organización, cita en su punto 6.4 Seguridad Física, los niveles de acceso que puede tener un usuario de forma general y cita que pueden existir áreas restringidas, debiendo detallarse el concepto de "áreas restringidas". El Procedimiento de Alta, Baja y Modificación de Usuarios (ENE 12 SI IS PR 001) en su punto Procedimiento de Alta, Baja y Modificación de Usuarios - 5.1.2 Alta de Usuarios - Análisis y Ejecución: No se incluye la asignación de permisos para acceso físico a sitios de trabajo.	N/A

Tabla N° 16:

A.9 Objetivo de Control – Control de Acceso aplicable para el proceso de "Alta y Baja de Usuarios" (Continua).

		Objetivos de Control	Si	No	Parcial	Evidencia	Observaciones	Artículo de Requisito Legal Vinculado
		Control						
A.9.1.2	Acceso a redes y servicios de redes	Los usuarios sólo tendrán acceso a la red y a los servicios de red que hayan sido específicamente autorizados a utilizar			X	Procedimiento de Alta, Baja y Modificación de Usuarios (ENE 12 SI IS PR 001)	El Procedimiento de Alta, Baja y Modificación de Usuarios (ENE 12 SI IS PR 001) en su punto Procedimiento de Alta, Baja y Modificación de Usuarios - 5.1.2 Alta de Usuarios - Análisis y Ejecución, cita que los permisos que se asignarán se tomarán de un usuario modelo, sin embargo existen casos en los cuales el usuario modelo tiene asignados erróneamente sus permisos y esta asignación errónea se sigue repitiendo.	N/A
A.9.2	**Gestión de acceso de los usuarios**							
Objetivo:	Garantizar el acceso de los usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios							
		Control						
A.9.2.1	Registro y cancelación de registro del usuario	Se llevará a cabo un proceso formal de registro y cancelación de registro de usuarios para habilitar la asignación de derechos de acceso			X	Procedimiento de Alta, Baja y Modificación de Usuarios (ENE 12 SI IS PR 001)	El Procedimiento de Alta, Baja y Modificación de Usuarios (ENE 12 SI IS PR 001) en su punto Procedimiento de Alta, Baja y Modificación de Usuarios - 5.1.2 Alta de Usuarios - Análisis y Ejecución, cita que los permisos se toman de un usuario modelo, sin embargo existen casos en los cuales el usuario modelo tiene asignados erróneamente sus permisos y esta asignación errónea se sigue repitiendo.	N/A

Tabla N° 16:

A.9 Objetivo de Control – Control de Acceso aplicable para el proceso de "Alta y Baja de Usuarios" (Continua).

		Objetivos de Control	Si	No	Parcial	Evidencia	Observaciones	Artículo de Requisito Legal Vinculado
		Control						
A.9.2.2	Provisión de acceso de usuario	Proceso formal de provisión de acceso de usuario será implementado para asignar o revocar derechos de acceso para todo tipo de usuario a todos los sistemas y servicios			X	Procedimiento de Alta, Baja y Modificación de Usuarios (ENE 12 SI IS PR 001)	El Procedimiento de Alta, Baja y Modificación de Usuarios (ENE 12 SI IS PR 001) en su punto Procedimiento de Alta, Baja y Modificación de Usuarios - 5.1.2 Alta de Usuarios - Análisis y Ejecución, cita que los permisos que se asignarán se tomarán de un usuario modelo, sin embargo existen casos en los cuales el usuario modelo tiene asignados erróneamente sus permisos y esta asignación errónea se sigue repitiendo.	N/A
		Control						
A.9.2.5	Revisión de los derechos de acceso de los usuarios	Los propietarios de activos deberán revisar los derechos de acceso de los usuarios a intervalos regulares		X		Norma DIAMM S04 - Lineamientos generales de administración y seguridad para las Redes y Sistemas de la Organización	La Norma DIAMM S04 - Lineamientos generales de administración y seguridad para las Redes y Sistemas de la Organización en su punto 5.2 Control de Acceso indica que debe revisarse periódicamente los permisos para validar su uso, caso contrario se eliminaran, sin embargo no existe un criterio de comparación fiable para validar que permisos tiene asignados y deberían ser retirados.	N/A

Tabla N° 16:

A.9 Objetivo de Control – Control de Acceso aplicable para el proceso de "Alta y Baja de Usuarios" (Continua).

		Objetivos de Control	Si	No	Parcial	Evidencia	Observaciones	Artículo de Requisito Legal Vinculado
		Control						
A.9.2.6	Eliminación o ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y usuarios de partes externas a las instalaciones de procesamiento de información e información se eliminarán al finalizar su empleo, contrato o acuerdo, o ajustarse al cambiar			X	Norma DIAMM S04 - Lineamientos generales de administración y seguridad para las Redes y Sistemas de la Organización	La Norma DIAMM S04 - Lineamientos generales de administración y seguridad para las Redes y Sistemas de la Organización en su punto 5.2 Control de Acceso, no hace referencia al retiro de permisos de acceso para todos los usuarios (solo detalla para personal de sistemas) y no tiene un criterio de validación para conocer que permisos tiene activos al momento de su baja, dejando abierta la posibilidad de quedar permisos abiertos para un usuario que ha sido dado de baja.	N/A
A.9.3	**Responsabilidades del usuario**							
Objetivo:	Responsabilizar a los usuarios por la protección de su información de autenticación							
		Control						
A.9.3.1	Uso de la información secreta de autenticación	El usuario deberá seguir las prácticas de la organización en el uso de la información de autenticación secreta			X	Norma DIAMM S04 - Lineamientos generales de administración y seguridad para las Redes y Sistemas de la Organización	La Norma DIAMM S04 no detalla en su sección 4.6 Identificación y Autenticación de usuarios un estándar para claves seguras y/o controles de seguridad.	N/A

Tabla N° 16:

A.9 Objetivo de Control – Control de Acceso aplicable para el proceso de "Alta y Baja de Usuarios" (Continua).

		Objetivos de Control	Si	No	Parcial	Evidencia	Observaciones	Artículo de Requisito Legal Vinculado
A.9.4	**Control de acceso a sistemas y aplicaciones**							
Objetivo:	Prevenir el acceso no autorizado a sistemas y aplicaciones							
		Control						
A.9.4.1	Restricción de acceso a la información	El acceso a la información y las funciones del sistema de aplicación se restringirán de conformidad con la política de control de acceso			X	Procedimiento de Alta, Baja y Modificación de Usuarios (ENE 12 SI IS PR 001)	El Procedimiento de Alta, Baja y Modificación de Usuarios (ENE 12 SI IS PR 001) en su punto Procedimiento de Alta, Baja y Modificación de Usuarios - 5.1.2 Alta de Usuarios - Análisis y Ejecución, cita que los permisos que se asignarán se tomarán de un usuario modelo, sin embargo existen casos en los cuales el usuario modelo tiene asignados erróneamente sus permisos y esta asignación errónea se sigue repitiendo.	N/A

Nota. Objetivos de Control y Controles aplicables al proceso de "Alta y Baja de Usuarios" en base a la Norma ISO 27001:2013.

Fuente: Elaboración propia de Investigador

Tabla N° 17:

A.10 Objetivo de Control – Criptografía aplicable para el proceso de "Alta y Baja de Usuarios".

	Objetivos de Control		Si	No	Parcial	Evidencia	Observaciones	Artículo de Requisito Legal Vinculado
A.10	**Criptografía**							
A.10.1	**Controles Criptográficos**							
Objetivo:	Asegurar un uso adecuado y efectivo de la criptografía para proteger la confidencialidad, autenticidad e integridad de la información							
		Control						
A.10.1.1	Política sobre el uso de controles criptográficos	Se elaborará y aplicará una política sobre el uso de los controles criptográficos para la protección de la información		X		Norma DIAMM S04 - Lineamientos generales de administración y seguridad para las Redes y Sistemas de la Organización	La Norma DIAMM S04 no detalla en su sección 4.6 Identificación y Autenticación de usuarios un estándar para claves seguras y/o controles de seguridad.	N/A
		Control						
A.10.1.2	Gestión de claves	Se desarrollará y aplicará una política sobre el uso, la protección y la duración de las claves criptográficas durante todo su ciclo de vida		X		Procedimiento de Alta, Baja y Modificación de Usuarios (ENE 12 SI IS PR 001) Norma DIAMM S04 - Lineamientos generales de administración y seguridad para las Redes y Sistemas de la Organización	La Norma DIAMM S04 no detalla en su sección 4.6 Identificación y Autenticación de usuarios un estándar para claves seguras y/o controles de seguridad.	N/A

Nota. Objetivos de Control y Controles aplicables al proceso de "Alta y Baja de Usuarios" en base a la Norma ISO 27001:2013.

Fuente: Elaboración propia de Investigador

Tabla N° 18:

A.11 Objetivo de Control – Seguridad física y ambiental aplicable para el proceso de "Alta y Baja de Usuarios".

	Objetivos de Control		Si	No	Parcial	Evidencia	Observaciones	Artículo de Requisito Legal Vinculado
A.11	**Seguridad física y ambiental**							
A.11.1	**Áreas seguras**							
Objetivo:	Evitar accesos físicos no autorizados, daños e interferencias a las instalaciones de procesamiento de información e información de la organización							
		Control						
A.11.1.1	Seguridad perimetral física	Se definirán perímetros de seguridad y utilizarán para proteger las áreas que contengan información sensible o crítica e instalaciones de procesamiento de información	X			Procedimiento Protección Física (ENE 09 SI IT PR 002)	El Procedimiento Protección Física (ENE 09 SI IT PR 002) se enfoca específicamente en los sitios de acceso para personal calificado (Sistemas) y diferencia entre sitios de trabajo donde todos los colaboradores pueden tener acceso.	N/A
A.11.2	**Equipo**							
Objetivo:	Evitar pérdidas, daños, robo o compromiso de los activos e interrupción de las operaciones de la organización							
		Control						
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	La seguridad se aplicará a los activos fuera de sitio teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización			X	Procedimiento de Gestión de Activos de IT (ENE 10 SI IT PR 003) Procedimiento de Alta, Baja y Modificación de Usuarios (ENE 12 SI IS PR 001) Norma DIAMM S04 - Lineamientos generales de administración y seguridad para las Redes y Sistemas de la Organización Procedimiento Copias de Respaldo (ENE XX SI IS PR 001)	El Procedimiento de Gestión de Activos de IT (ENE 10 SI IT PR 003) indica que debe contratarse seguros y garantías para precautelar el activo ante eventualidades como robos o daños, sin embargo no detalla los controles implementados para salvaguardar la información ante este tipo de eventos.	N/A

Tabla N° 18:

A.11 Objetivo de Control – Seguridad física y ambiental aplicable para el proceso de "Alta y Baja de Usuarios" (Continua)

		Objetivos de Control	Si	No	Parcial	Evidencia	Observaciones	Artículo de Requisito Legal Vinculado
		Control						
A.11.2.7	Eliminación segura o reutilización del equipo	Todos los elementos del equipo que contengan medios de almacenamiento deberán ser verificados para asegurar que los datos sensibles y el software bajo licencia hayan sido eliminados o sobrescritos de forma segura antes de su eliminación o reutilización			X	Procedimiento de Gestión de Activos de IT (ENE 10 SI IT PR 003) Procedimiento de Gestión de Activos de IT (ENE 10 SI IT PR 003) Procedimiento Copias de Respaldo (ENE 09 SI IS PR 001)	Procedimiento de Alta, Baja y Modificación de Usuarios - 5.2.2 Baja de Usuarios - Análisis y Ejecución: No se incluye al momento de su ejecución el retiro de equipos asignados al personal. Procedimiento de Gestión de Activos de IT, punto 3. Responsabilidades - Responsable de Sistemas de áreas: Cita la entrega y actualización del inventario, más no detalla retiro de equipos por bajas de usuario o bajas de equipos en el inventario por daño, robos y cualquier evento que afecte a los equipos/activos entregados.	N/A

Nota. Objetivos de Control y Controles aplicables al proceso de "Alta y Baja de Usuarios" en base a la Norma ISO 27001:2013.

Fuente: Elaboración propia de Investigador

Tabla N° 19:

A.12 Objetivo de Control – Seguridad Operacional aplicable para el proceso de "Alta y Baja de Usuarios".

	Objetivos de Control		Si	No	Parcial	Evidencia	Observaciones	Artículo de Requisito Legal Vinculado
A.12	**Seguridad operacional**							
A.12.2	**Protección contra el malware**							
Objetivo:	Garantizar que la información y las instalaciones de procesamiento de información estén protegidas contra el malware							
		Control						
A.12.2.1	Controles contra el malware	Se implementarán controles de detección, prevención y recuperación para proteger contra el malware, combinados con el conocimiento apropiado del usuario			X	Norma DIAMM S04 - Lineamientos generales de administración y seguridad para las Redes y Sistemas de la Organización Texto Ampliatorio del Punto 3.8 norma DIAMM S-004: Anexo Virus	La Norma DIAMM S04 - Lineamientos generales de administración y seguridad para las Redes y Sistemas de la Organización en su punto 3.8, cita el especial cuidado que debe tener el personal de sistemas respecto a control de virus, pero no detalla los controles que existen para salvaguardar la información de los usuarios (encriptación, PIN de seguridad, clave de Windows, respaldo de información, software antivirus, parches de seguridad, ente otros.)	N/A
A.12.3	**Copia de seguridad**							
Objetivo:	Proteger contra la perdida de información							
		Control						
A.12.3.1	Copia de seguridad de información	Copias de seguridad de la información, software e imágenes del sistema se tomarán y probarán periódicamente de acuerdo con una política de respaldo acordada	X			Procedimiento Copias de Respaldo (ENE 09 SI IS PR 001)	Procedimiento Copias de Respaldo (ENE 09 SI IS PR 001) detalla el tipo de información a respaldar, directorios a respaldar, vigencia de respaldos y responsables todos para contar con copias de seguridad.	N/A

Tabla N° 19:

A.12 Objetivo de Control – Seguridad Operacional aplicable para el proceso de "Alta y Baja de Usuarios" (Continua)

	Objetivos de Control		Si	No	Parcial	Evidencia	Observaciones	Artículo de Requisito Legal Vinculado
A.12.5	**Control de software operativo**							
Objetivo:	Asegurar la integridad de los sistemas operativos							
		Control						
A.12.5.1	Instalación de software en sistemas operativos	Se implementarán procedimientos para controlar la instalación de software en sistemas operativos			X	Procedimiento de Gestión de Activos de IT (ENE 10 SI IT PR 003)	El Procedimiento de Gestión de Activos de IT (ENE 10 SI IT PR 003) no detalla un proceso de control para validar el buen uso de los activos, ni responsables para esta actividad.	N/A
A.12.6	**Gestión de vulnerabilidades técnicas**							
Objetivo:	Evitar la explotación de vulnerabilidades técnicas							
		Control						
A.12.6.2	Restricción en la instalación del software	Normas que rigen la instalación de software por parte de los usuarios se establecerán e implementarán			X	Procedimiento de Gestión de Activos de IT (ENE 10 SI IT PR 003)	El Procedimiento de Gestión de Activos de IT (ENE 10 SI IT PR 003) no detalla un proceso de control para validar el buen uso de los activos, ni responsables para esta actividad.	N/A

Nota. Objetivos de Control y Controles aplicables al proceso de "Alta y Baja de Usuarios" en base a la Norma ISO 27001:2013.

Fuente: Elaboración propia de Investigador

Tabla N° 20:

A.13 Objetivo de Control – Seguridad de las comunicaciones aplicable para el proceso de "Alta y Baja de Usuarios".

	Objetivos de Control		Si	No	Parcial	Evidencia	Observaciones	Artículo de Requisito Legal Vinculado
A.13	**Seguridad de las comunicaciones**							
A.13.2	**Transferencia de información**							
Objetivo:	Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa							
		Control						
A.13.2.3	Mensajería electrónica	La información relacionada con la mensajería electrónica estará debidamente protegida	X			Norma DIAMM S04 - Lineamientos generales de administración y seguridad para las Redes y Sistemas de la Organización Acuerdos de Servicio con proveedores de Servicio de Transmisión de datos (Confidencial)	La Norma DIAMM S04 - Lineamientos generales de administración y seguridad para las Redes y Sistemas de la Organización en su punto 3 Confidencialidad y seguridad de los datos, detalla los controles que deben manejarse para la comunicación (donde está incluida la mensajería electrónica), adicional existen acuerdos de servicio con los proveedores de enlaces de datos que proporcionan medios de comunicación seguros y encriptados para salvaguardar la información que se transmite por estos.	N/A

Tabla N° 20:

A.13 Objetivo de Control – Seguridad de las comunicaciones aplicable para el proceso de "Alta y Baja de Usuarios" (Continua)

		Objetivos de Control	Si	No	Parcial	Evidencia	Observaciones	Artículo de Requisito Legal Vinculado
		Control						
A.13.2.4	Acuerdos de confidencialidad o no divulgación	Los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de protección de la organización serán identificados, revisados y documentados periódicamente			X	Norma DIAMM S04 - Lineamientos generales de administración y seguridad para las Redes y Sistemas de la Organización Procedimiento de Alta, Baja y Modificación de Usuarios (ENE 12 SI IS PR 001)	El Procedimiento de Alta, Baja y Modificación de Usuarios (ENE 12 SI IS PR 001) en su punto Procedimiento de Alta, Baja y Modificación de Usuarios - 5.1.2 Alta de Usuarios - Análisis y Ejecución, cita que los permisos que se asignarán se tomarán de un usuario modelo, sin embargo existen casos en los cuales el usuario modelo tiene asignados erróneamente sus permisos y esta asignación errónea se sigue repitiendo, esto puede provocar una brecha en la confidencialidad de la información al asignar permisos a repositorios de información que no le corresponden al usuario. No existe una sección donde se detalle el flujo para contacto interno ante incidentes de Seguridad y/o contacto externo, ante eventos que ameriten inclusión de autoridades (fraudes o delitos que atenten contra la información y/o activos de tecnología de la organización).	COIP, Sección Tercera

Nota. Objetivos de Control y Controles aplicables al proceso de "Alta y Baja de Usuarios" en base a la Norma ISO 27001:2013.

Fuente: Elaboración propia de Investigador

Tabla N° 21:

A.15 Objetivo de Control – Relación con proveedores aplicable para el proceso de "Alta y Baja de Usuarios".

	Objetivos de Control		Si	No	Parcial	Evidencia	Observaciones	Artículo de Requisito Legal Vinculado
A.15	**Relaciones con proveedores**							
A.15.1	**Seguridad de la información en las relaciones con proveedores**							
Objetivo:	Asegurar la protección de los activos de la organización a los que pueden acceder los proveedores							
		Control						
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	Requisitos de seguridad de la información para mitigar el riesgo asociado con el acceso del proveedor a los activos de la organización serán acordados con el proveedor y documentados	X			Política Seguridad de Información (ENE 08 SI PO 001) Acuerdos de confidencialidad con Proveedores	La Política de Seguridad de la Información en su punto 3. 3. Responsabilidades y Control, cita las responsabilidades de los colaboradores (internos/externos) respecto a Seguridad de Sistemas y la obligatoriedad de informarse sobre las normativas de seguridad de la información que deben cumplir Todo proveedor que brinde sus servicios en la organización firma previamente antes de iniciar su contrato de servicios tiene la obligación de firmar los acuerdos de confidencialidad que maneja la organización, los mismos que varían su alcance respecto al área de prestación de servicios donde el proveedor se vaya a desempeñar.	N/A

Tabla N° 21:

A.15 Objetivo de Control – Relación con proveedores aplicable para el proceso de "Alta y Baja de Usuarios" (Continua)

		Objetivos de Control	Si	No	Parcial	Evidencia	Observaciones	Artículo de Requisito Legal Vinculado
		Control						
A.15.1.2	Abordar la seguridad dentro de los acuerdos de proveedores	Todos los requerimientos relevantes de seguridad de la información serán establecidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI para la información de la organización	X			Política Seguridad de Información (ENE 08 SI PO 001) Acuerdos de confidencialidad con Proveedores	La Política de Seguridad de la Información en su punto 3. 3. Responsabilidades y Control, cita las responsabilidades de los colaboradores (internos/externos) respecto a Seguridad de Sistemas y la obligatoriedad de informarse sobre las normativas de seguridad de la información que deben cumplir Todo proveedor que brinde sus servicios en la organización firma previamente antes de iniciar su contrato de servicios tiene la obligación de firmar los acuerdos de confidencialidad que maneja la organización, los mismos que varían su alcance respecto al área de prestación de servicios donde el proveedor se vaya a desempeñar.	N/A
		Control						
A.15.1.3	Cadena de suministro de tecnología de la información y comunicación	Los acuerdos con proveedores incluirán requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información, las comunicaciones y la cadena de suministro de productos	X			Procedimiento de Gestión de Activos de IT (ENE 10 SI IT PR 003) Norma DIAMM 7.01 - Uso Herramientas Electrónicas de Comunicación Norma DIAMM S-05: Publicación de Información en	La Política de Seguridad de la Información en su punto 3. 3. Responsabilidades y Control, cita las responsabilidades de los colaboradores (internos/externos) respecto a Seguridad de Sistemas y la obligatoriedad de informarse sobre las normativas de seguridad de la información que deben	N/A

Tabla N° 21:

A.15 Objetivo de Control – Relación con proveedores aplicable para el proceso de "Alta y Baja de Usuarios" (Continua)

	Objetivos de Control	Si	No	Parcial	Evidencia	Observaciones	Artículo de Requisito Legal Vinculado
					Intranet e Internet	cumplir Todo proveedor que brinde sus servicios en la organización firma previamente antes de iniciar su contrato de servicios tiene la obligación de firmar los acuerdos de confidencialidad que maneja la organización, los mismos que varían su alcance respecto al área de prestación de servicios donde el proveedor se vaya a desempeñar.	

Nota. Objetivos de Control y Controles aplicables al proceso de "Alta y Baja de Usuarios" en base a la Norma ISO 27001:2013.

Fuente: Elaboración propia de Investigador

Tabla N° 22:

A.16 Objetivo de Control – Gestión de incidentes de Seguridad de la información aplicable para el proceso de "Alta y Baja de Usuarios".

	Objetivos de Control		Si	No	Parcial	Evidencia	Observaciones	Artículo de Requisito Legal Vinculado
A.16	**Gestión de incidentes de seguridad de la información**							
A.16.1	**Gestión de incidentes y mejoras en seguridad de la información**							
Objetivo:	Asegurar un enfoque coherente y efectivo para la gestión de incidentes de seguridad de la información, incluyendo la comunicación sobre eventos y debilidades de seguridad							
		Control						
A.16.1.1	Responsabilidades y procedimientos	Gestión de responsabilidades y procedimientos para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información		X		Norma DIAMM S04 - Lineamientos generales de administración y seguridad para las Redes y Sistemas de la Organización	No existe una sección donde se detalle el flujo para contacto interno ante incidentes de Seguridad y/o contacto externo, ante eventos que ameriten inclusión de autoridades (fraudes o delitos que atenten contra la información).	COIP, Sección Tercera
		Control						
A.16.1.2	Reporte de eventos de seguridad de la información	Los eventos de seguridad de la información deben ser reportados a través de canales de administración apropiados tan pronto como sea posible		X		Norma DIAMM S04 - Lineamientos generales de administración y seguridad para las Redes y Sistemas de la Organización	No existe una sección donde se detalle el flujo para contacto interno ante incidentes de Seguridad y/o contacto externo, ante eventos que ameriten inclusión de autoridades (fraudes o delitos que atenten contra la información).	COIP, Sección Tercera
		Control						
A.16.1.3	Informar sobre las debilidades en la seguridad de la información	Los empleados y contratistas que utilicen los sistemas y servicios de información de la organización deberán tomar nota de cualquier falla observada o presunta debilidad de seguridad de la información en sistemas o servicios		X		Procedimiento de Alta, Baja y Modificación de Usuarios (ENE 12 SI IS PR 001)	El Procedimiento de Alta, Baja y Modificación de Usuarios (ENE 12 SI IS PR 001) sección de Alta de Usuarios, no detalla el compromiso del usuario (interno/externo) para mejorar la Seguridad de la Información notificando sobre posibles debilidades que podría detectar.	N/A

Nota. Objetivos de Control y Controles aplicables al proceso de "Alta y Baja de Usuarios" en base a la Norma ISO 27001:2013.

Fuente: Elaboración propia de Investigador

Tabla N° 23:

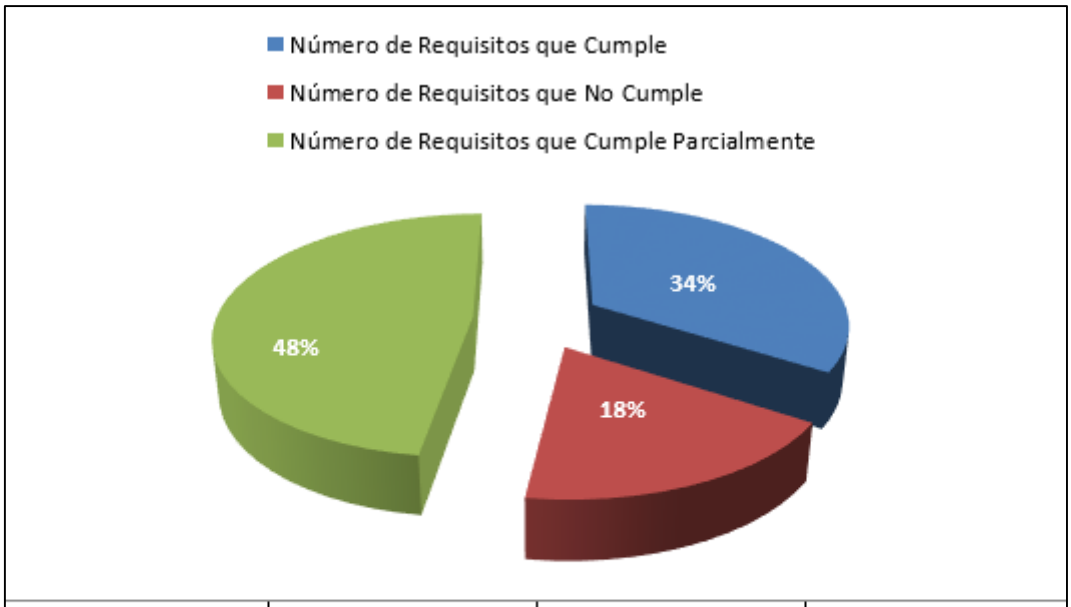
A.18 Objetivo de Control – Cumplimiento aplicable para el proceso de "Alta y Baja de Usuarios".

	Objetivos de Control		Si	No	Parcial	Evidencia	Observaciones	Artículo de Requisito Legal Vinculado
A.18	**Cumplimiento**							
A.18.2	**Revisión de seguridad de la información**							
Objetivo:	Asegurar que la seguridad de la información sea implementada y operada de acuerdo con las políticas y procedimientos de la organización							
		Control						
A.18.2.1	Revisión independiente de la seguridad de la información	El enfoque de la organización para administrar la seguridad de la información y su implementación (es decir, objetivos de control, controles, procesos de políticas y procedimientos para la seguridad de la información) será revisado independientemente a intervalos planificados o cuando ocurran cambios significativos	X			Ejecución de revisiones internas semestrales y auditorias anuales para controlar que se cumplen las políticas y procedimientos de la organización	Se ejecutan auditorias semestrales / anuales, las cuales pueden ser realizadas por personal interno de la organización o contratarse los servicios de un proveedor para la ejecución de la misma.	N/A
		Control						
A.18.2.2	Cumplimiento de las políticas y estándares de seguridad	Los administradores revisarán periódicamente el cumplimiento del procesamiento de información y los procedimientos dentro de su área de responsabilidad con las políticas de seguridad adecuadas, estándares y cualquier otro requisito de seguridad	X			Ejecución de revisiones internas semestrales y auditorias anuales para controlar que se cumplen las políticas y procedimientos de la organización	Se ejecutan auditorias semestrales / anuales, las cuales pueden ser realizadas por personal interno de la organización o contratarse los servicios de un proveedor para la ejecución de la misma.	N/A

Nota. Objetivos de Control y Controles aplicables al proceso de "Alta y Baja de Usuarios" en base a la Norma ISO 27001:2013.

Fuente: Elaboración propia de Investigador

Los resultados de cumplimiento de los Controles aplicables al Proceso de "Alta y Baja de Usuarios" se muestran en la siguiente Figura (ver Figura N° 26).



Número Total de Requisitos Aplicables	Número de Requisitos que Cumple	Número de Requisitos que No Cumple	Número de Requisitos que Cumple Parcialmente
44	15	8	21

Figura N° 26 Resultados Objetivos de Control y Controles que cumple el Proceso de "Alta y Baja de Usuarios".
Fuente: Elaboración propia del Investigador

3.2 Desarrollo de requerimientos aplicables de la Norma ISO 27001:2013 al proceso de "Alta y Baja de Usuarios"

3.2.1 Acciones Desarrolladas para el Cumplimiento de los requerimientos aplicables de la Norma ISO 27001:2013 al proceso de "Alta y Baja de Usuarios"

En las siguientes tablas (Ver Tabla N° 24 hasta la Tabla N° 52), se detallan las acciones tomadas para cubrir las observaciones que se levantaron para los objetivos aplicables de la Norma ISO 27001:2013 para el proceso de "Alta y Baja de Usuarios" cuyos niveles de cumplimiento fueron "No cumple" y "Cumple parcialmente". Cada número de "observación identificada" se corresponde al número de "acción a ejecutar" y al número de

"evidencia de desarrollo", donde consta lo implementado para el cumplimiento de cada control de la Norma.

Tabla N° 24:

Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.5.1.2 Revisión de Políticas de Seguridad de la Información, respecto a la Norma ISO 27001:2013 para el proceso de "Alta y Baja de Usuarios".

Objetivos de Control y Controles	A.5 Políticas de Seguridad de la Información A.5.1 Gestión de la dirección para seguridad de la información A.5.1.2 Revisión de Políticas de Seguridad de la Información
Observaciones Identificadas: 1. Políticas desactualizadas: - Política de Sistemas (ENE 10 SI PO 002) – Desactualizada**,** última revisión 2010**.** - Política Seguridad de Información (ENE 08 SI PO 001) – Desactualizada**,** última revisión 2008**.**	
Acciones a ejecutar: 1. Actualización por parte de Compliance para incluir el listado actualizado de responsables, firmas, vigencia de la política y validar que las políticas estén acorde a la situación actual de la organización.	
Evidencia de desarrollo: 1. Políticas actualizadas a marzo del 2017 - Anexo 2: Extracto Política de Sistemas (MAR 17 SI PO 002) actualizada. - Anexo 3: Extracto Política Seguridad de Información (MAR 17 SI PO 001) actualizada.	

Fuente: Elaboración propia de Investigador

Tabla N° 25:

Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.6.1.3 Contacto con Autoridades, respecto a la Norma ISO 27001:2013 para el proceso de "Alta y Baja de Usuarios".

Objetivos de Control y Controles	A.6 Organización de Seguridad de la información A.6.1 Organización Interna A.6.1.3Contacto con autoridades
Observaciones Identificadas: **1.** No existe una sección donde se detalle el flujo para contacto interno ante incidentes de Seguridad y/o contacto externo, ante eventos que ameriten inclusión de autoridades (fraudes o delitos que atenten contra la información y/o activos de tecnología de la organización).	

Acciones a ejecutar: 1. Anexar a la Norma DIAMM S04 el flujo para reportar actividades que violen esta normativa así como eventos que puedan representar atentados a la seguridad de la información, pudiendo citarse que la Normativa Legal Vigente en Ecuador (COIP).
Evidencia de desarrollo: 1. Anexos a la Norma DIAMM S04 - Anexo 4: Flujograma de escalamiento y reporte de eventos que afecten a la Seguridad de la Información.

Fuente: Elaboración propia de Investigador

Tabla N° 26:

Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.6.2.1 Política para dispositivos móviles, respecto a la Norma ISO 27001:2013 para el proceso de "Alta y Baja de Usuarios".

Objetivos de Control y Controles	A.6 Organización de Seguridad de la información A.6.2 Dispositivos móviles y teletrabajo A.6.2.1 Política para dispositivos móviles
Observaciones Identificadas: 1. Norma Utilización de dispositivos móviles - 3.4 Monitoreo y Control: Se detalla que la empresa asume los costos por la activación del dispositivo móvil así como los cargos que genere el mismo, pero al momento de dar de baja un usuario entra en conflicto la propiedad de la línea telefónica, donde el usuario solicita quedarse con la línea para su uso personal y la cual pertenece a la empresa ya que en el punto 3.4 se detalla que el dispositivo móvil se utilizará exclusivamente con fines laborales y "eventualmente" con fines personal, el no detallar la propiedad de la línea, genera conflictos al momento de dar da baja una línea ya que el usuario generalmente ancla a la mayoría de sus actividades personales a la línea asignada. 2. Norma Utilización de dispositivos móviles revisada en Septiembre del 2015. 3. Procedimiento de Alta, Baja y Modificación de Usuarios - 5.2.2 Baja de Usuarios - Análisis y Ejecución: No se incluye al momento de la ejecución de la Baja del usuario el retiro de equipos asignados. 4. Procedimiento de Gestión de Activos de IT, punto 3. Responsabilidades - Responsable de Sistemas de áreas: Cita la entrega y actualización del inventario, más no detalla retiro de equipos por bajas de usuario o bajas de equipos en el inventario por daño, robos y cualquier evento que afecte a los equipos/activos entregados.	

Acciones a ejecutar:

1. Definir el concepto de propiedad de la línea, para evitar que los usuarios la utilicen con fines personales y evitar conflictos al momento de entregar la misma al momento de la baja de usuarios.

2. Actualizar la fecha de última revisión de la Norma Utilización de dispositivos móviles así como responsables y vigencia de la Norma.

3. Agregar dentro del punto 5.2.2 en la política de Alta, Baja y Modificación de Usuarios el retiro de equipos (computadores, dispositivos móviles, tarjetas de acceso, token, radios VHF, módems) y cualquier elemento de propiedad de la empresa que le haya sido asignado al momento de su alta.

4. Agregar al Procedimiento de Gestión de Activos de IT dentro del punto 3. Responsabilidades - Responsable de Sistemas de área: las actividades de retiro de equipos por baja de usuarios y baja en el inventario por cualquier evento (robo, pérdida, daño) que afecte al desempeño de los activos asignados.

Evidencia de desarrollo:

1. Anexo 5: Aclaratoria a la Norma Utilización de dispositivos móviles - 3.4 Monitoreo y Control, concepto de “Propiedad de la línea”.

2. Anexo 6: Extracto Norma Utilización de dispositivos móviles actualizada a Marzo del 2017.

3. Anexo 7: Extracto Política de Alta, Baja y Modificación de Usuarios, punto 5.2.2, inclusión actividad “Entrega y Retiro de equipos”.

4. Anexo 8: Extracto Procedimiento de Gestión de Activos de IT, 3. Responsabilidades - Responsable de Sistemas de área: “actividades de retiro de equipos”.

Fuente: Elaboración propia de Investigador

Tabla N° 27:

Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.7.2.3 Procesos disciplinarios, respecto a la Norma ISO 27001:2013 para el proceso de "Alta y Baja de Usuarios".

Objetivos de Control y Controles	A.7 Seguridad de los recursos humanos A.7.2 Durante el empleo A.7.2.3 Procesos disciplinarios
Observaciones Identificadas: 1. No existe una sección donde se detalle el flujo para contacto interno ante incidentes de Seguridad y/o contacto externo, ante eventos que ameriten inclusión de autoridades (fraudes o delitos que atenten contra la información y/o activos de tecnología de la organización).	
Acciones a ejecutar: 1. Anexar a la Norma DIAMM S04 el flujo para reportar actividades que violen esta normativa así como eventos que puedan representar atentados a la seguridad de la información, pudiendo citarse que la Normativa Legal Vigente en Ecuador (COIP).	
Evidencia de desarrollo: 1. Anexos a la Norma DIAMM S04 - Anexo 4: Flujograma de escalamiento y reporte de eventos que afecten a la Seguridad de la Información.	

Fuente: Elaboración propia de Investigador

Tabla N° 28:

Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.8.1.1 Inventario de activos, respecto a la Norma ISO 27001:2013 para el proceso de "Alta y Baja de Usuarios".

Objetivos de Control y Controles	A.8 Gestión de activos A.8.1 Responsabilidad de los activos A.8.1.1 Inventario de activos
Observaciones Identificadas: 1. Procedimiento de Gestión de Activos de IT, punto 3. Responsabilidades - Responsable de Sistemas de áreas: Cita la entrega y actualización del inventario, más no detalla retiro de equipos por bajas de usuario o bajas de equipos en el inventario por daño, robos y cualquier evento que afecte a los equipos/activos entregados. 2. Sistema de Inventarios: Inventario de equipos de Ecuador desactualizado. 3. Planilla de Asignación / Retiro de Equipos: Desactualizada, sin formato específico y su control se lo hace manualmente.	

Acciones a ejecutar: 1. Agregar al Procedimiento de Gestión de Activos de IT dentro del punto 3. Responsabilidades - Responsable de Sistemas de área: las actividades de retiro de equipos por baja de usuarios y baja en el inventario por cualquier evento (robo, pérdida, daño) que afecte al desempeño de los activos asignados. 2. Actualizar inventario de equipos (activos) de Ecuador. 3. Estandarizar la Planilla de Asignación / Retiro de Equipos y automatizar el control de asignación de equipos mediante herramientas propias de la empresa que permita llevar un mejor control de los mismos.
Evidencia de desarrollo: 1. Anexo 8: Extracto Procedimiento de Gestión de Activos de IT, 3. Responsabilidades - Responsable de Sistemas de área: "actividades de retiro de equipos". 2. Anexo 9: Captura Pantalla Sistema de Inventarios – Reporte de Activos Ecuador. 3. Anexos: - Anexo 10: Planilla de Asignación / Retiro de Equipos actualizada a Marzo 2017. - Anexo 11: Captura Pantalla Formulario de registro de Equipos en Intranet Corporativa.

Fuente: Elaboración propia de Investigador

Tabla N° 29:

Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.8.1.2 Propiedad de activos, respecto a la Norma ISO 27001:2013 para el proceso de "Alta y Baja de Usuarios".

Objetivos de Control y Controles	A.8 Gestión de activos A.8.1 Responsabilidad de los activos A.8.1.2Propiedad de activos
Observaciones Identificadas: 1. Procedimiento de Gestión de Activos de IT, punto 3. Responsabilidades - Responsable de Sistemas de áreas: Cita la entrega y actualización del inventario, más no detalla retiro de equipos por bajas de usuario o bajas de equipos en el inventario por daño, robos y cualquier evento que afecte a los equipos/activos entregados. 2. Sistema de Inventarios: Inventario de equipos de Ecuador desactualizado. 3. Planilla de Asignación / Retiro de Equipos: Desactualizada, sin formato específico y su control se lo hace manualmente.	

Acciones a ejecutar: 1. Agregar al Procedimiento de Gestión de Activos de IT dentro del punto 3. Responsabilidades - Responsable de Sistemas de área: las actividades de retiro de equipos por baja de usuarios y baja en el inventario por cualquier evento (robo, pérdida, daño) que afecte al desempeño de los activos asignados. 2. Actualizar inventario de equipos (activos) de Ecuador. 3. Estandarizar la Planilla de Asignación / Retiro de Equipos y automatizar el control de asignación de equipos mediante herramientas propias de la empresa que permita llevar un mejor control de los mismos.
Evidencia de desarrollo: 1. Anexo 8: Extracto Procedimiento de Gestión de Activos de IT, 3. Responsabilidades - Responsable de Sistemas de área: "actividades de retiro de equipos". 2. Anexo 9: Captura Pantalla Sistema de Inventarios – Reporte de Activos Ecuador. 3. Anexos: - Anexo 10: Planilla de Asignación / Retiro de Equipos actualizada a Marzo 2017. - Anexo 11: Captura Pantalla Formulario de registro de Equipos en Intranet Corporativa.

Fuente: Elaboración propia de Investigador

Tabla N° 30:

Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.8.1.3 Uso aceptable de activos, respecto a la Norma ISO 27001:2013 para el proceso de "Alta y Baja de Usuarios".

Objetivos de Control y Controles	A.8 Gestión de activos A.8.1 Responsabilidad de los activos A.8.1.3Uso aceptable de activos
Observaciones Identificadas: 1. La Norma DIAMM 7.01 - Uso Herramientas Electrónicas de Comunicación en su punto 2.1 Uso Aceptable, detalla sobre el buen uso de los activos, sin embargo es recomendable registrar la instrucción al usuario sobre este punto al momento de la entrega de los equipos. 2. El Procedimiento de Gestión de Activos de IT (ENE 10 SI IT PR 003) no detalla un proceso de control para validar el buen uso de los activos, ni responsables para esta actividad.	

3. El control de activos que incluye al software, no tiene un parámetro para su validación (Software estándar).

4. El control de activos que incluye al software, no tiene un control sobre la instalación/desinstalación del mismo en los computadores asignados a los usuarios.

Acciones a ejecutar:

1. Procedimiento de Gestión de Activos. Agregar dentro del punto 3. Responsabilidades - Responsable de Sistemas de área: las actividades de comunicación sobre el buen uso de los activos y que al firmar la Planilla de Asignación / Retiro de Activos entiende y acepta la misma.

2. Procedimiento de Gestión de Activos. Agregar dentro del punto 3. Responsabilidades - Responsable de Sistemas de área: las actividades de control sobre el buen uso de los activos.

3. Generar una matriz con el Software estándar disponible para Ecuador, la cual puede ser evaluada automáticamente para detectar software ilegal o no estándar utilizando las herramientas de la organización.

4. Validar y eliminar perfiles de administrador de usuarios para evitar la instalación de software no estándar o software libre.

Evidencia de desarrollo:

1. Anexos:
   - Anexo 12: Extracto Procedimiento de Gestión de Activos dentro del punto que cita las actividades de comunicación sobre el buen uso de los activos.
   - Anexo 10: Planilla de Asignación / Retiro de Equipos actualizada a Marzo 2017.

2. Anexo 13: Extracto Procedimiento de Gestión de Activos – Actividades de control sobre el buen uso de los activos.

3. Anexo 14: Matriz de Software Estándar para Ecuador.

4. Anexo 15: Listado de perfiles de usuario (privilegios) para Ecuador.

Fuente: Elaboración propia de Investigador

Tabla N° 31:

Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.8.1.4 Regreso de activos, respecto a la Norma ISO 27001:2013 para el proceso de "Alta y Baja de Usuarios".

Objetivos de Control y Controles	A.8 Gestión de activos A.8.1 Responsabilidad de los activos A.8.1.4 Regreso de activos
Observaciones Identificadas: 1. Procedimiento de Alta, Baja y Modificación de Usuarios - 5.2.2 Baja de Usuarios - Análisis y Ejecución: No se incluye al momento de su ejecución el retiro de equipos asignados al personal. 2. Procedimiento de Alta, Baja y Modificación de Usuarios - 5.2.2 Baja de Usuarios - Análisis y Ejecución: No se incluye al momento de la ejecución de la Baja del usuario el retiro de equipos asignados.	
Acciones a ejecutar: 1. Agregar dentro del punto 5.2.2 en la política de Alta, Baja y Modificación de Usuarios el retiro de equipos (computadores, dispositivos móviles, tarjetas de acceso, token, radios VHF, módems) y cualquier elemento de propiedad de la empresa que le haya sido asignado al momento de su alta. 2. Agregar al Procedimiento de Gestión de Activos de IT dentro del punto 3. Responsabilidades - Responsable de Sistemas de área: las actividades de retiro de equipos por baja de usuarios y baja en el inventario por cualquier evento (robo, pérdida, daño) que afecte al desempeño de los activos asignados.	
Evidencia de desarrollo: 1. Anexo 7: Extracto Política de Alta, Baja y Modificación de Usuarios, punto 5.2.2, inclusión actividad "Entrega y Retiro de equipos". 2. Anexo 8: Extracto Procedimiento de Gestión de Activos de IT, 3. Responsabilidades - Responsable de Sistemas de área: "actividades de retiro de equipos".	

Fuente: Elaboración propia de Investigador

Tabla N° 32:

Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.8.2.1 Clasificación de la Información, respecto a la Norma ISO 27001:2013 para el proceso de "Alta y Baja de Usuarios".

Objetivos de Control y Controles	A.8 Gestión de activos A.8.2 Clasificación de la Información A.8.2.1 Clasificación de la información
Observaciones Identificadas: 1. La Norma DIAMM S04 - Lineamientos generales de administración y seguridad para las Redes y Sistemas de la Organización, en su punto 3. Confidencialidad y seguridad de los datos, cita los términos Información Confidencial o Sensitiva y el manejo de la misma, sin embargo, no se detalla la clasificación de la información que maneja actualmente la empresa.	
Acciones a ejecutar: 1. Anexar al Procedimiento, el detalle de la administración (uso y/o difusión) de información de la organización, donde se detalla la clasificación y niveles de autorización para el uso de la misma.	
Evidencia de desarrollo: 1. Anexo 16: Clasificación de información.	

Fuente: Elaboración propia de Investigador

Tabla N° 33:

Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.8.2.1 Clasificación de la Información, respecto a la Norma ISO 27001:2013 para el proceso de "Alta y Baja de Usuarios".

Objetivos de Control y Controles	A.8 Gestión de activos A.8.2 Clasificación de la Información A.8.2.3 Manejo de activos
Observaciones Identificadas: 1. La Norma DIAMM S04 - Lineamientos generales de administración y seguridad para las Redes y Sistemas de la Organización, en su punto 3. Confidencialidad y seguridad de los datos, cita los términos Información Confidencial o Sensitiva y el manejo de la misma, sin embargo, no se detalla la clasificación de la información que maneja actualmente la empresa. 2. La Norma DIAMM S04 - Lineamientos generales de administración y seguridad para las Redes y Sistemas de la Organización en su punto 3.8, cita el especial cuidado que debe tener el personal de sistemas respecto a control de virus, pero no detalla los controles que existen para salvaguardar la información de los usuarios (encriptación, PIN de seguridad, clave de Windows, respaldo de información, software antivirus, parches de seguridad, ente otros.)	

Acciones a ejecutar: 1. Anexar al Procedimiento, el detalle de la administración (uso y/o difusión) de información de la organización, donde se detalla la clasificación y niveles de autorización para el uso de la misma. 2. Anexar a la Norma los controles que existen para salvaguardar la información de los usuarios (encriptación, PIN de seguridad, clave de Windows, respaldo de información, software antivirus, parches de seguridad, ente otros).
Evidencia de desarrollo: 1. Anexo 16: Clasificación de información. 2. Anexo 17: Controles de Seguridad.

Fuente: Elaboración propia de Investigador

Tabla N° 34:

Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.9.1.1 Política de Control de Acceso, respecto a la Norma ISO 27001:2013 para el proceso de "Alta y Baja de Usuarios".

Objetivos de Control y Controles	A.9 Control de Acceso A.9.1 Requerimientos empresariales de control de acceso A.9.1.1Política de Control de Acceso
Observaciones Identificadas: 1. La Norma DIAMM S04 - Lineamientos generales de administración y seguridad para las Redes y Sistemas de la Organización, cita en su punto 6.4 Seguridad Física, los niveles de acceso que puede tener un usuario de forma general y cita que pueden existir áreas restringidas, debiendo detallarse el concepto de "áreas restringidas". 2. El Procedimiento de Alta, Baja y Modificación de Usuarios (ENE 12 SI IS PR 001) en su punto Procedimiento de Alta, Baja y Modificación de Usuarios - 5.1.2 Alta de Usuarios - Análisis y Ejecución: No se incluye la asignación de permisos para acceso físico a sitios de trabajo.	
Acciones a ejecutar: 1. Describir las áreas restringidas de la Organización y hacer referencia al Procedimiento Protección Física (ENE 09 SI IT PR 002) que se enfoca específicamente en el acceso al área de Sistemas, restringida para el resto de usuarios (Data Center, Cuarto de Comunicaciones) para un mejor entendimiento. 2. Incluir la asignación de medios magnéticos o credenciales al ejecutar el alta de un usuario, para que el mismo pueda ingresar a los sitios de trabajo asignados.	

Evidencia de desarrollo:
1. Anexo 18: Acceso a Áreas restringidas. 2. Anexo 20: Asignación de credenciales de acceso.

Fuente: Elaboración propia de Investigador

Tabla N° 35:

Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.9.1.2 Acceso a redes y servicios de redes, respecto a la Norma ISO 27001:2013 para el proceso de "Alta y Baja de Usuarios".

Objetivos de Control y Controles	A.9 Control de Acceso A.9.1 Requerimientos empresariales de control de acceso A.9.1.2 Acceso a redes y servicios de redes
Observaciones Identificadas: 1. El Procedimiento de Alta, Baja y Modificación de Usuarios (ENE 12 SI IS PR 001) en su punto Procedimiento de Alta, Baja y Modificación de Usuarios - 5.1.2 Alta de Usuarios - Análisis y Ejecución, cita que los permisos que se asignarán se tomarán de un usuario modelo, sin embargo existen casos en los cuales el usuario modelo tiene asignados erróneamente sus permisos y esta asignación errónea se sigue repitiendo.	
Acciones a ejecutar: 1. Desarrollar una matriz con los perfiles de usuario aplicables para determinar que aplicaciones, repositorios de información y con qué accesos físicos deberá contar el usuario al momento de su alta, con ello se eliminaría la asignación errónea de permisos al tomar como referencia un "usuario modelo", también esto eliminaría reproceso por modificación de permisos de usuarios, agilitaría su proceso de alta así como también sería un base fiable para desactivar los permisos que tenga asignados en caso de baja del usuario.	
Evidencia de desarrollo: 1. Anexo 19: Matriz de Perfiles de Usuario.	

Fuente: Elaboración propia de Investigador

Tabla N° 36:

Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.9.2.1 Registro y cancelación de registro de usuario, respecto a la Norma ISO 27001:2013 para el proceso de "Alta y Baja de Usuarios".

Objetivos de Control y Controles	A.9 Control de Acceso A.9.2 Gestión de acceso de los usuarios A.9.2.1 Registro y cancelación de registro del usuario
Observaciones Identificadas: 1. El Procedimiento de Alta, Baja y Modificación de Usuarios (ENE 12 SI IS PR 001) en su punto Procedimiento de Alta, Baja y Modificación de Usuarios - 5.1.2 Alta de Usuarios - Análisis y Ejecución, cita que los permisos que se asignarán se tomarán de un usuario modelo, sin embargo existen casos en los cuales el usuario modelo tiene asignados erróneamente sus permisos y esta asignación errónea se sigue repitiendo.	
Acciones a ejecutar: 1. Desarrollar una matriz con los perfiles de usuario aplicables para determinar que aplicaciones, repositorios de información y con qué accesos físicos deberá contar el usuario al momento de su alta, con ello se eliminaría la asignación errónea de permisos al tomar como referencia un "usuario modelo", también esto eliminaría reproceso por modificación de permisos de usuarios, agilitaría su proceso de alta así como también sería un base fiable para desactivar los permisos que tenga asignados en caso de baja del usuario.	
Evidencia de desarrollo: 1. Anexo 19: Matriz de Perfiles de Usuario.	

Fuente: Elaboración propia de Investigador

Tabla N° 37:

Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.9.2.2 Provisión de acceso de usuario, respecto a la Norma ISO 27001:2013 para el proceso de "Alta y Baja de Usuarios".

Objetivos de Control y Controles	A.9 Control de Acceso A.9.2 Gestión de acceso de los usuarios A.9.2.2 Provisión de acceso de usuario
Observaciones Identificadas: 1. El Procedimiento de Alta, Baja y Modificación de Usuarios (ENE 12 SI IS PR 001) en su punto Procedimiento de Alta, Baja y Modificación de Usuarios - 5.1.2 Alta de Usuarios - Análisis y Ejecución, cita que los permisos que se asignarán se tomarán de un usuario modelo, sin embargo existen casos en los cuales el usuario modelo tiene asignados erróneamente sus permisos y esta asignación errónea se sigue repitiendo.	

Acciones a ejecutar: 1. Desarrollar una matriz con los perfiles de usuario aplicables para determinar que aplicaciones, repositorios de información y con qué accesos físicos deberá contar el usuario al momento de su alta, con ello se eliminaría la asignación errónea de permisos al tomar como referencia un "usuario modelo", también esto eliminaría reproceso por modificación de permisos de usuarios, agilitaría su proceso de alta así como también sería un base fiable para desactivar los permisos que tenga asignados en caso de baja del usuario.
Evidencia de desarrollo: 1. Anexo 19: Matriz de Perfiles de Usuario.

Fuente: Elaboración propia de Investigador

Tabla N° 38:

Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.9.2.5 Revisión de los derechos de acceso de los usuarios, respecto a la Norma ISO 27001:2013 para el proceso de "Alta y Baja de Usuarios".

Objetivos de Control y Controles	A.9 Control de Acceso A.9.2 Gestión de acceso de los usuarios A.9.2.5 Revisión de los derechos de acceso de los usuarios
Observaciones Identificadas: 1. La Norma DIAMM S04 - Lineamientos generales de administración y seguridad para las Redes y Sistemas de la Organización en su punto 5.2 Control de Acceso indica que debe revisarse periódicamente los permisos para validar su uso, caso contrario se eliminaran, sin embargo no existe un criterio de comparación fiable para validar que permisos tiene asignados y deberían ser retirados.	
Acciones a ejecutar: 1. Desarrollar una matriz con los perfiles de usuario aplicables para determinar que aplicaciones, repositorios de información y con qué accesos físicos deberá contar el usuario al momento de su alta, con ello se eliminaría la asignación errónea de permisos al tomar como referencia un "usuario modelo", también esto eliminaría reproceso por modificación de permisos de usuarios, agilitaría su proceso de alta así como también sería un base fiable para desactivar los permisos que tenga asignados en caso de baja del usuario.	
Evidencia de desarrollo: 1. Anexo 19: Matriz de Perfiles de Usuario.	

Fuente: Elaboración propia de Investigador

Tabla N° 39:

Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.9.2.6 Eliminación o ajuste de los derechos de acceso, respecto a la Norma ISO 27001:2013 para el proceso de "Alta y Baja de Usuarios".

Objetivos de Control y Controles	A.9 Control de Acceso A.9.2 Gestión de acceso de los usuarios A.9.2.6 Eliminación o ajuste de los derechos de acceso
Observaciones Identificadas: 1. La Norma DIAMM S04 - Lineamientos generales de administración y seguridad para las Redes y Sistemas de la Organización en su punto 5.2 Control de Acceso, no hace referencia al retiro de permisos de acceso para todos los usuarios (solo detalla para personal de sistemas) y no tiene un criterio de validación para conocer que permisos tiene activos al momento de su baja, dejando abierta la posibilidad de quedar permisos abiertos para un usuario que ha sido dado de baja.	
Acciones a ejecutar: 1. Desarrollar una matriz con los perfiles de usuario aplicables para determinar que aplicaciones, repositorios de información y con qué accesos físicos deberá contar el usuario al momento de su alta, con ello se eliminaría la asignación errónea de permisos al tomar como referencia un "usuario modelo", también esto eliminaría reproceso por modificación de permisos de usuarios, agilitaría su proceso de alta así como también sería un base fiable para desactivar los permisos que tenga asignados en caso de baja del usuario.	
Evidencia de desarrollo: 1. Anexo 19: Matriz de Perfiles de Usuario.	

Fuente: Elaboración propia de Investigador

Tabla N° 40:

Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.9.3.1 Uso de la información secreta de autenticación, respecto a la Norma ISO 27001:2013 para el proceso de "Alta y Baja de Usuarios".

Objetivos de Control y Controles	A.9 Control de Acceso A.9.3 Responsabilidades del usuario A.9.3.1 Uso de la información secreta de autenticación
Observaciones Identificadas: 1. La Norma DIAMM S04 no detalla en su sección 4.6 Identificación y Autenticación de usuarios un estándar para claves seguras y/o controles de seguridad.	
Acciones a ejecutar: 1. Anexar a la Norma los controles que existen para salvaguardar la información de los usuarios (encriptación, PIN de seguridad, clave de Windows, respaldo de información, software antivirus, parches de seguridad, ente otros.).	

Evidencia de desarrollo: 1. Anexo 17: Controles de Seguridad.

Fuente: Elaboración propia de Investigador

Tabla N° 41:

Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.9.4.1 Restricción de acceso a sistemas y aplicaciones, respecto a la Norma ISO 27001:2013 para el proceso de "Alta y Baja de Usuarios".

Objetivos de Control y Controles	A.9 Control de Acceso A.9.4 Control de acceso a sistemas y aplicaciones A.9.4.1 Restricción de acceso a la información
Observaciones Identificadas: 1. El Procedimiento de Alta, Baja y Modificación de Usuarios (ENE 12 SI IS PR 001) en su punto Procedimiento de Alta, Baja y Modificación de Usuarios - 5.1.2 Alta de Usuarios - Análisis y Ejecución, cita que los permisos que se asignarán se tomarán de un usuario modelo, sin embargo existen casos en los cuales el usuario modelo tiene asignados erróneamente sus permisos y esta asignación errónea se sigue repitiendo.	
Acciones a ejecutar: 1. Desarrollar una matriz con los perfiles de usuario aplicables para determinar que aplicaciones, repositorios de información y con qué accesos físicos deberá contar el usuario al momento de su alta, con ello se eliminaría la asignación errónea de permisos al tomar como referencia un "usuario modelo", también esto eliminaría reproceso por modificación de permisos de usuarios, agilitaría su proceso de alta así como también sería un base fiable para desactivar los permisos que tenga asignados en caso de baja del usuario.	
Evidencia de desarrollo: 1. Anexo 19: Matriz de Perfiles de Usuario.	

Fuente: Elaboración propia de Investigador

Tabla N° 42:

Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.10.1.1 Política sobre el uso de controles criptográficos, respecto a la Norma ISO 27001:2013 para el proceso de "Alta y Baja de Usuarios".

Objetivos de Control y Controles	A.10 Criptografía A.10.1 Controles Criptográficos A.10.1.1 Política sobre el uso de controles criptográficos
Observaciones Identificadas: 1. La Norma DIAMM S04 no detalla en su sección 4.6 Identificación y Autenticación de usuarios un estándar para claves seguras y/o controles de seguridad.	
Acciones a ejecutar: 1. Anexar a la Norma los controles que existen para salvaguardar la información de los usuarios (encriptación, PIN de seguridad, clave de Windows, respaldo de información, software antivirus, parches de seguridad, ente otros.).	
Evidencia de desarrollo: 1. Anexo 17: Controles de Seguridad.	

Fuente: Elaboración propia de Investigador

Tabla N° 43:

Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.10.1.2 Gestión de claves, respecto a la Norma ISO 27001:2013 para el proceso de "Alta y Baja de Usuarios".

Objetivos de Control y Controles	A.10 Criptografía A.10.1 Controles Criptográficos A.10.1.2 Gestión de claves
Observaciones Identificadas: 1. La Norma DIAMM S04 no detalla en su sección 4.6 Identificación y Autenticación de usuarios un estándar para claves seguras y/o controles de seguridad.	
Acciones a ejecutar: 1. Anexar a la Norma los controles que existen para salvaguardar la información de los usuarios (encriptación, PIN de seguridad, clave de Windows, respaldo de información, software antivirus, parches de seguridad, ente otros.).	
Evidencia de desarrollo: 1. Anexo 17: Controles de Seguridad.	

Fuente: Elaboración propia de Investigador

Tabla N° 44:

Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones, respecto a la Norma ISO 27001:2013 para el proceso de "Alta y Baja de Usuarios".

Objetivos de Control y Controles	A.11 Seguridad física y ambiental A.11.2 Equipo A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones
Observaciones Identificadas: 1. El Procedimiento de Gestión de Activos de IT (ENE 10 SI IT PR 003) indica que debe contratarse seguros y garantías para precautelar el activo ante eventualidades como robos o daños, sin embargo no detalla los controles implementados para salvaguardar la información ante este tipo de eventos.	
Acciones a ejecutar: 1. Anexar a la Norma los controles que existen para salvaguardar la información de los usuarios (encriptación, PIN de seguridad, clave de Windows, respaldo de información, software antivirus, parches de seguridad, ente otros.).	
Evidencia de desarrollo: 1. Anexo 17: Controles de Seguridad.	

Fuente: Elaboración propia de Investigador

Tabla N° 45:

Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.11.2.7 Eliminación segura o reutilización del equipo, respecto a la Norma ISO 27001:2013 para el proceso de "Alta y Baja de Usuarios".

Objetivos de Control y Controles	A.11 Seguridad física y ambiental A.11.2 Equipo A.11.2.7 Eliminación segura o reutilización del equipo
Observaciones Identificadas: 1. Procedimiento de Alta, Baja y Modificación de Usuarios - 5.2.2 Baja de Usuarios - Análisis y Ejecución: No se incluye al momento de su ejecución el retiro de equipos asignados al personal. 2. Procedimiento de Gestión de Activos de IT, punto 3. Responsabilidades - Responsable de Sistemas de áreas: Cita la entrega y actualización del inventario, más no detalla retiro de equipos por bajas de usuario o bajas de equipos en el inventario por daño, robos y cualquier evento que afecte a los equipos/activos entregados.	
Acciones a ejecutar: 1. Agregar dentro del punto 5.2.2 en la política de Alta, Baja y Modificación de Usuarios el retiro de equipos (computadores, dispositivos móviles, tarjetas de	

acceso, token, radios VHF, módems) y cualquier elemento de propiedad de la empresa que le haya sido asignado al momento de su alta. 2. Agregar al Procedimiento de Gestión de Activos de IT dentro del punto 3. Responsabilidades - Responsable de Sistemas de área: las actividades de retiro de equipos por baja de usuarios y baja en el inventario por cualquier evento (robo, pérdida, daño) que afecte al desempeño de los activos asignados.
Evidencia de desarrollo: 1. Anexo 7: Extracto Política de Alta, Baja y Modificación de Usuarios, punto 5.2.2, inclusión actividad "Entrega y Retiro equipos". 2. Anexo 8: Extracto Procedimiento de Gestión de Activos de IT, 3. Responsabilidades - Responsable de Sistemas de área: "Actividades de retiro de equipo.

Fuente: Elaboración propia de Investigador

Tabla N° 46:

Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.12.2.1 Controles contra el malware, respecto a la Norma ISO 27001:2013 para el proceso de "Alta y Baja de Usuarios".

Objetivos de Control y Controles	A.12 Seguridad operacional A.12.2 Protección contra el malware A.12.2.1 Controles contra el malware
Observaciones Identificadas: 1. La Norma DIAMM S04 - Lineamientos generales de administración y seguridad para las Redes y Sistemas de la Organización en su punto 3.8, cita el especial cuidado que debe tener el personal de sistemas respecto a control de virus, pero no detalla los controles que existen para salvaguardar la información de los usuarios (encriptación, PIN de seguridad, clave de Windows, respaldo de información, software antivirus, parches de seguridad, ente otros.)	
Acciones a ejecutar: 1. Anexar a la Norma los controles que existen para salvaguardar la información de los usuarios (encriptación, PIN de seguridad, clave de Windows, respaldo de información, software antivirus, parches de seguridad, ente otros).	
Evidencia de desarrollo: 1. Anexo 17: Controles de Seguridad.	

Fuente: Elaboración propia de Investigador

Tabla N° 47:

Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.12.5.1 Instalación de software en sistemas operativos, respecto a la Norma ISO 27001:2013 para el proceso de "Alta y Baja de Usuarios".

Objetivos de Control y Controles	A.12 Seguridad operacional A.12.5 Control de software operativo A.12.5.1 Instalación de software en sistemas operativos
Observaciones Identificadas: 1. El Procedimiento de Gestión de Activos de IT (ENE 10 SI IT PR 003) no detalla un proceso de control para validar el buen uso de los activos, ni responsables para esta actividad.	
Acciones a ejecutar: 1. Detallar las actividades de control que debe efectuar el área de Sistemas sobre el buen uso de los activos, detallando revisiones periódicas de estado de los activos, control sobre el software instalado y el nivel de permisos de usuario (administrador).	
Evidencia de desarrollo: 1. Anexos: - Anexo 21: Extracto Procedimiento de Gestión de Activos de IT, 3. Responsabilidades - Responsable de Sistemas de área: "Control de Activos". - Anexo 14: Matriz de Software Estándar para Ecuador. - Anexo 15: Listado de perfiles de usuario (privilegios) para Ecuador.	

Fuente: Elaboración propia de Investigador

Tabla N° 48:

Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.12.6.2 Restricción en la instalación del software, respecto a la Norma ISO 27001:2013 para el proceso de "Alta y Baja de Usuarios".

Objetivos de Control y Controles	A.12 Seguridad operacional A.12.6 Gestión de vulnerabilidades técnicas A.12.6.2 Restricción en la instalación del software
Observaciones Identificadas: 1. El Procedimiento de Gestión de Activos de IT (ENE 10 SI IT PR 003) no detalla un proceso de control para validar el buen uso de los activos, ni responsables para esta actividad.	
Acciones a ejecutar: 1. Detallar las actividades de control que debe efectuar el área de Sistemas sobre el buen uso de los activos, detallando revisiones periódicas de estado de los activos,	

control sobre el software instalado y el nivel de permisos de usuario (administrador).
Evidencia de desarrollo: 1. Anexos: - Anexo 21: Extracto Procedimiento de Gestión de Activos de IT, 3. Responsabilidades - Responsable de Sistemas de área: "Control de Activos". - Anexo 14: Matriz de Software Estándar para Ecuador. - Anexo 15: Listado de perfiles de usuario (privilegios) para Ecuador.

Fuente: Elaboración propia de Investigador

Tabla N° 49:

Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.13.2.4 Acuerdos de confidencialidad o no divulgación, respecto a la Norma ISO 27001:2013 para el proceso de "Alta y Baja de Usuarios".

Objetivos de Control y Controles	A.13 Seguridad de las comunicaciones A.13.2 Transferencia de información A.13.2.4 Acuerdos de confidencialidad o no divulgación
Observaciones Identificadas: 1. El Procedimiento de Alta, Baja y Modificación de Usuarios (ENE 12 SI IS PR 001) en su punto Procedimiento de Alta, Baja y Modificación de Usuarios - 5.1.2 Alta de Usuarios - Análisis y Ejecución, cita que los permisos que se asignarán se tomarán de un usuario modelo, sin embargo existen casos en los cuales el usuario modelo tiene asignados erróneamente sus permisos y esta asignación errónea se sigue repitiendo, esto puede provocar una brecha en la confidencialidad de la información al asignar permisos a repositorios de información que no le corresponden al usuario. 2. No existe una sección donde se detalle el flujo para contacto interno ante incidentes de Seguridad y/o contacto externo, ante eventos que ameriten inclusión de autoridades (fraudes o delitos que atenten contra la información y/o activos de tecnología de la organización).	
Acciones a ejecutar: 1. Desarrollar una matriz con los perfiles de usuario aplicables para determinar que aplicaciones, repositorios de información y con qué accesos físicos deberá contar el usuario al momento de su alta, con ello se eliminaría la asignación errónea de permisos al tomar como referencia un "usuario modelo", también esto eliminaría reproceso por modificación de permisos de usuarios, agilitaría su proceso de alta así como también sería un base fiable para desactivar los permisos que tenga asignados en caso de baja del usuario. 2. Anexar a la Norma DIAMM S04 el flujo para reportar actividades que violen esta normativa así como eventos que puedan representar atentados a la seguridad de la	

información, pudiendo citarse que la Normativa Legal Vigente en Ecuador (COIP).
Evidencia de desarrollo: 1. Anexo 19: Matriz de Perfiles de Usuario. 2. Anexo 4: Flujograma de escalamiento y reporte de eventos que afecten a la Seguridad de la Información.

Fuente: Elaboración propia de Investigador

Tabla N° 50:

Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.16.1.1 Responsabilidades y procedimientos, respecto a la Norma ISO 27001:2013 para el proceso de "Alta y Baja de Usuarios".

Objetivos de Control y Controles	A.16 Gestión de incidentes de seguridad de la información A.16.1 Gestión de incidentes y mejoras en seguridad de la información A.16.1.1 Responsabilidades y procedimientos
Observaciones Identificadas: 1. No existe una sección donde se detalle el flujo para contacto interno ante incidentes de Seguridad y/o contacto externo, ante eventos que ameriten inclusión de autoridades (fraudes o delitos que atenten contra la información y/o activos de tecnología de la organización).	
Acciones a ejecutar: 1. Anexar a la Norma DIAMM S04 el flujo para reportar actividades que violen esta normativa así como eventos que puedan representar atentados a la seguridad de la información, pudiendo citarse que la Normativa Legal Vigente en Ecuador (COIP).	
Evidencia de desarrollo: 1. Anexo 4: Flujograma de escalamiento y reporte de eventos que afecten a la Seguridad de la Información.	

Fuente: Elaboración propia de Investigador

Tabla N° 51:

Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.16.1.2 Reporte de eventos de seguridad de la información, respecto a la Norma ISO 27001:2013 para el proceso de "Alta y Baja de Usuarios".

Objetivos de Control y Controles	A.16 Gestión de incidentes de seguridad de la información A.16.1 Gestión de incidentes y mejoras en seguridad de la información A.16.1.2 Reporte de eventos de seguridad de la información
Observaciones Identificadas: 1. No existe una sección donde se detalle el flujo para contacto interno ante incidentes de Seguridad y/o contacto externo, ante eventos que ameriten inclusión de autoridades (fraudes o delitos que atenten contra la información y/o activos de tecnología de la organización).	
Acciones a ejecutar: 1. Anexar a la Norma DIAMM S04 el flujo para reportar actividades que violen esta normativa así como eventos que puedan representar atentados a la seguridad de la información, pudiendo citarse que la Normativa Legal Vigente en Ecuador (COIP).	
Evidencia de desarrollo: 1. Anexo 4: Flujograma de escalamiento y reporte de eventos que afecten a la Seguridad de la Información.	

Fuente: Elaboración propia de Investigador

Tabla N° 52:

Acciones ejecutadas para cubrir los requerimientos aplicables al Control A.16.1.2 Informar sobre las debilidades en la seguridad de la información, respecto a la Norma ISO 27001:2013 para el proceso de "Alta y Baja de Usuarios".

Objetivos de Control y Controles	A.16 Gestión de incidentes de seguridad de la información A.16.1 Gestión de incidentes y mejoras en seguridad de la información A.16.1.3 Informar sobre las debilidades en la seguridad de la información
Observaciones Identificadas: 1. El Procedimiento de Alta, Baja y Modificación de Usuarios (ENE 12 SI IS PR 001) en su sección de Alta de Usuarios, no detalla el compromiso del usuario (interno/externo) para aportar a mejorar la Seguridad de la Información notificando sobre posibles debilidades que podría detectar.	
Acciones a ejecutar: 1. Agregar al Procedimiento de Alta, Baja y Modificación de Usuarios el compromiso de usuarios/proveedores respecto a informar sobre posibles	

debilidades en la Administración de la Seguridad de la Información de la organización.
Evidencia de desarrollo: 1. Anexo 22: Extracto Política de Alta, Baja y Modificación de Usuarios, inclusión actividad “Compromiso de los usuarios”.

Fuente: Elaboración propia de Investigador

3.3 Medición del tiempo del Proceso “Alta y Baja de Usuarios”

Para el cumplimiento de las observaciones identificadas durante la evaluación de los controles de la Norma ISO 27001:2013, se identificó que la “Matriz de Perfiles de Usuario” cubrió varios requisitos normativos, los cuales se detallan a continuación (Ver tabla N° 53):

Tabla N° 53:
Objetivos de Control y Controles donde la “Matriz de Perfiles de Usuario” cubrió los requisitos especificados.

Referencia	Objetivos de Control y controles
A.9	Control de Acceso
A.9.1	Requerimientos empresariales de control de acceso
A.9.1.2	Acceso a redes y servicios de redes
A.9	Control de Acceso
A.9.2	Gestión de acceso de los usuarios
A.9.2.1	Registro y cancelación de registro del usuario
A.9	Control de Acceso
A.9.2	Gestión de acceso de los usuarios
A.9.2.2	Provisión de acceso de usuario
A.9	Control de Acceso
A.9.2	Gestión de acceso de los usuarios
A.9.2.5	Revisión de los derechos de acceso de los usuarios
A.9	Control de Acceso
A.9.2	Gestión de acceso de los usuarios
A.9.2.6	Eliminación o ajuste de los derechos de acceso

Tabla N° 53:
Objetivos de Control y Controles donde la "Matriz de Perfiles de Usuario" cubrió los requisitos especificados (Continua).

Referencia	Objetivos de Control y controles
A.9	Control de Acceso
A.9.4	Control de acceso a sistemas y aplicaciones
A.9.4.1	Restricción de acceso a la información
A.13	Seguridad de las comunicaciones
A.13.2	Transferencia de información
A.13.2.4	Acuerdos de confidencialidad o no divulgación

Fuente: Elaboración propia de Investigador

Al desarrollar la ´"Matriz de Perfiles de Usuario" (Ver Anexo 19), se cumplió con las observaciones levantadas, sin embargo, provocó la modificación de los flujogramas de los subprocesos de "Alta de Usuarios" y "Baja de Usuarios"; estos cambios resultaron en la reducción de actividades y simplificación de estos subprocesos. A continuación se presentan los flujogramas modificados (Ver Figura N° 27 y Figura N° 28).

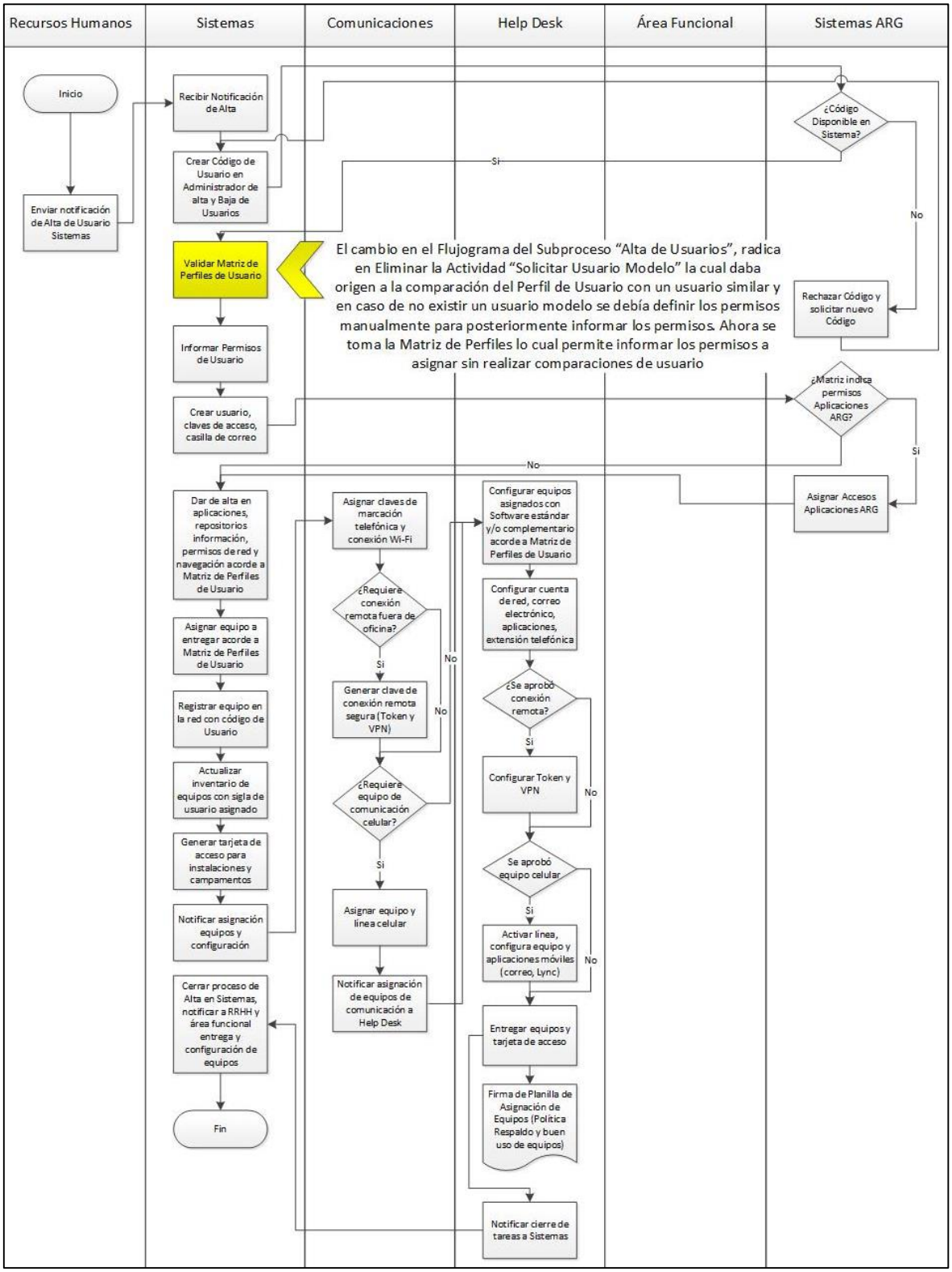


Figura N° 27: Diagrama de Flujo del Proceso de "Alta de Usuarios" actualizado luego de la implementación de la Matriz de Perfiles de Usuario.
Fuente: Elaboración propia del Investigador.

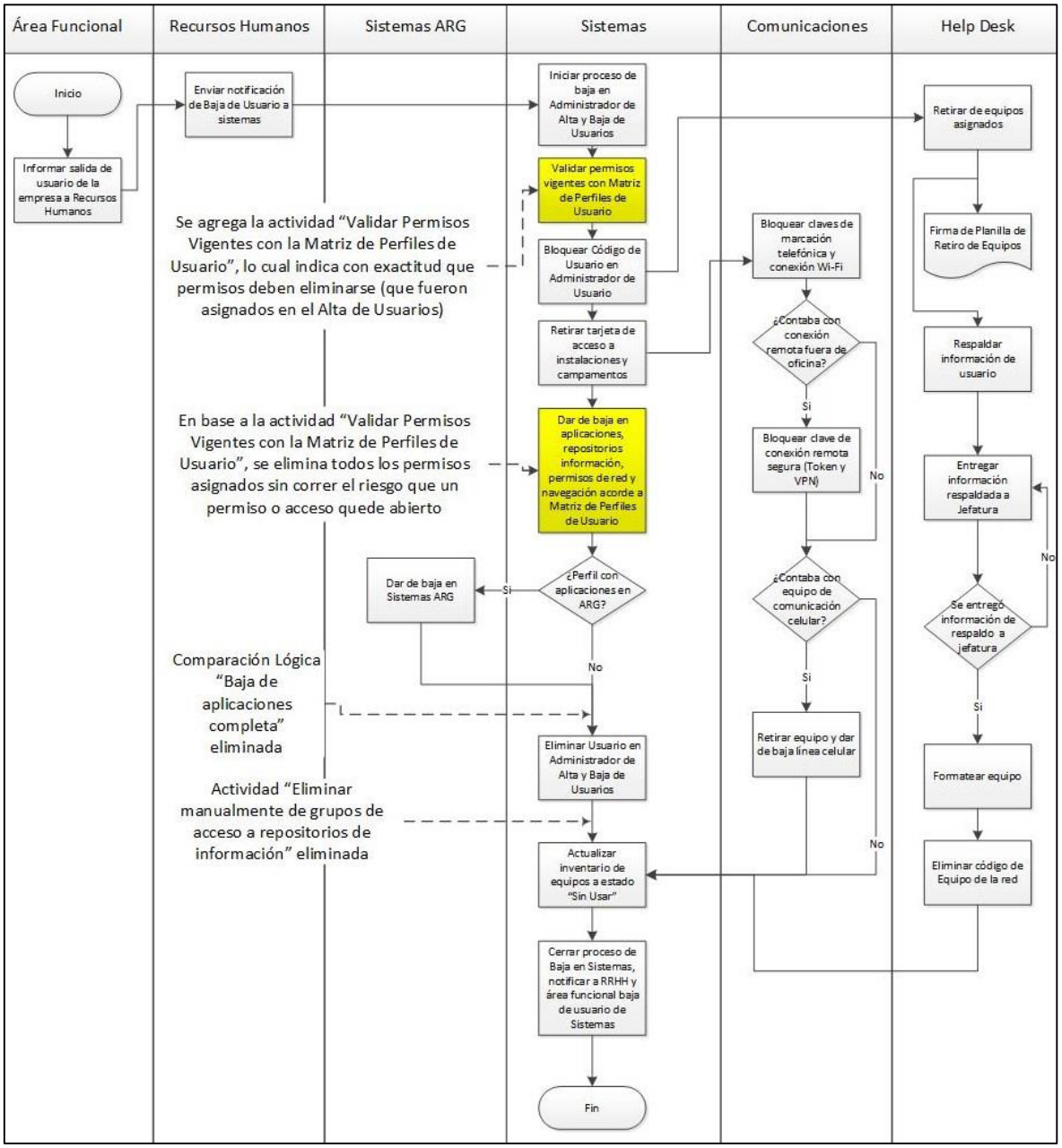


Figura N° 28: Diagrama de Flujo del Proceso de "Baja de Usuarios" actualizado luego de la implementación de Matriz de Perfiles de Usuario
Fuente: Elaboración propia del Investigador

El cambio en los subprocesos de "Alta de Usuarios" y "Baja de Usuarios", derivó que se aplique la medición de tiempos para conocer el impacto que estos cambios generaron en el tiempo de ejecución de los subprocesos en cuestión. Para ello, se utilizó el "Método de Registros de Datos Históricos" que permite evaluar cada subproceso antes y después del cambio aplicado.

Para la aplicación del método de medición del trabajo se siguieron los siguientes pasos:

3.3.1 Paso 1: Establecer el período de tiempo del que se desea obtener los datos históricos.

Para ello se definieron dos períodos de medición; el primer periodo fue desde 1 de enero del 2016 hasta el 31 de diciembre del 2016 (periodo en el cual no se ejecutaba cambios al flujograma de los subprocesos de “Alta de Usuarios” y “Baja de Usuarios”) y el segundo periodo fue desde el 1 de enero del 2017 hasta el 30 de abril del 2017 (periodo en el cual se implementó la “Matriz de Perfiles de Usuario” en los subprocesos de “Alta de Usuarios” y “Baja de Usuarios”). En la Figura N° 29 se detalla gráficamente la definición de los períodos de medición de tiempo y el tiempo de desarrollo de la “Matriz de Perfiles de Usuario”.

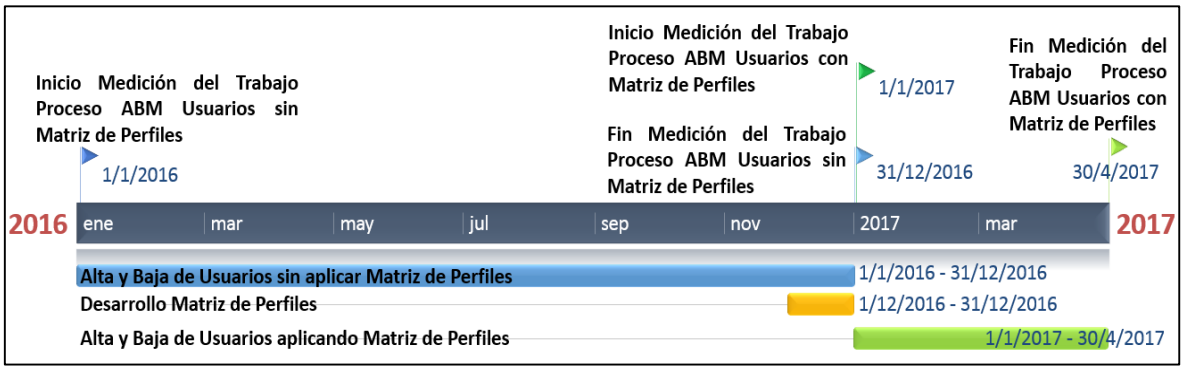


Figura N° 29: Período de Medición del Trabajo del Proceso de “Alta y Baja de Usuarios” antes y después de aplicar la Matriz de Perfiles de Usuario.
Fuente: Elaboración propia del Investigador

3.3.2 Paso 2: Recopilar los registros de datos históricos del período de tiempo a medir.

Los registros de datos históricos se obtuvieron del Sistema de Registro de Incidentes, el cual es la herramienta de Software que utiliza la organización para administrar el registro de incidentes (tickets de usuario) y controlar la gestión y solución de los mismos.

Esta herramienta permita gestionar la apertura de incidentes por parte de los usuarios, controlar el desarrollo, avance y solución del mismo hasta llegar al cierre de las solicitudes que se realizan al área de Sistemas. Dentro de esta herramienta se almacena la solicitud de asistencia del usuario, se lo clasifica por categorías (las categorías están previamente definidas por la Gerencia del área de Sistemas), se asigna prioridad de atención (alta, media y baja), se asigna un ingeniero de soporte para su atención, se registran las actividades que se realicen y se graba automáticamente el tiempo empleado para la ejecución y solución del ticket (entre los datos más relevantes que se pueden citar).

Además mediante esta herramienta de software, se pueden obtener métricas de atención al usuario, registrar y cuantificar las encuestas de satisfacción, así como validar que los SLA’s de atención están dentro de los parámetros contractuales.

Dentro del Sistema de Registro de Incidentes se seleccionaron los incidentes que están dentro de la Categoría “Alta de Usuarios” y “Baja de Usuarios”, cuyas fechas de ejecución están dentro del período de tiempo determinado en el paso 1. En la Figura N°

30, se puede observar a manera de ejemplo, la captura de pantalla del Sistema de Gestión de Incidentes, donde se muestra la ejecución de la selección de registros para el Subproceso de “Alta de Usuarios”, este mismo paso también se ejecutó para el subproceso de “Baja de Usuarios”.

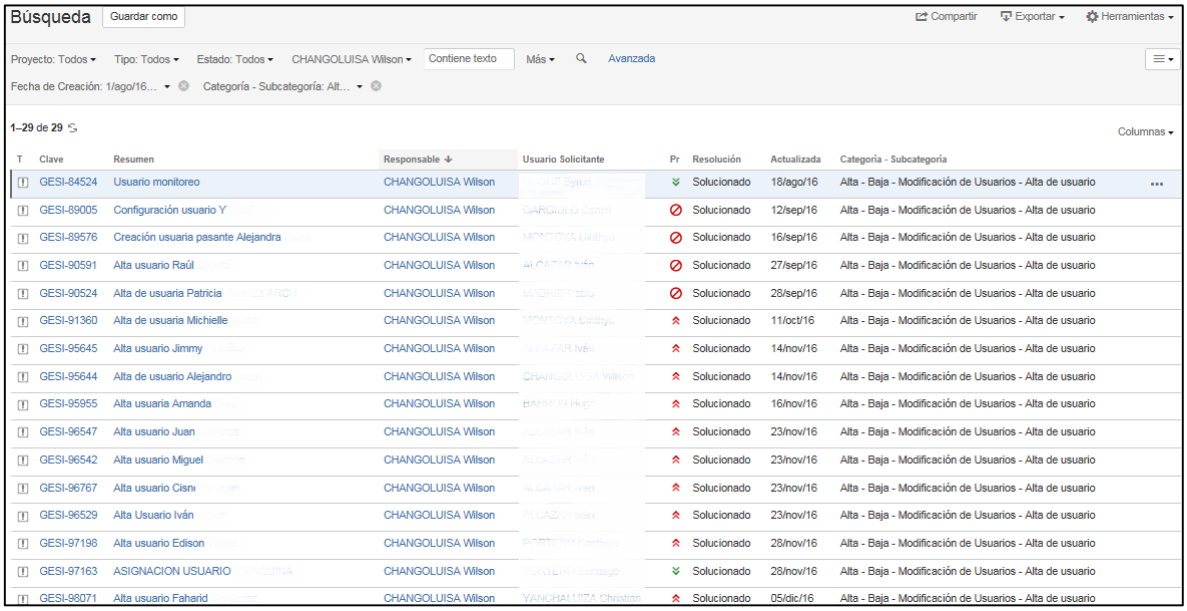


Figura N° 30: Pantalla con datos históricos del Subproceso de Alta de Usuarios obtenidos del Sistema de Gestión de Incidentes de la Empresa de Servicios de Consultoría para la Industria Petrolera. (Captura de Pantalla del Sistema de Gestión de Incidentes).
Nota: Nombres de usuarios se mantienen protegidos por confidencialidad de información de la empresa bajo estudio.
Fuente: Elaboración propia del Investigador.

3.3.3 Paso 3: Ordenar los registros de datos históricos:

Partiendo de los registros del Sistema de Gestión de Incidentes, se procedió a generar una matriz con cada incidente registrado para el subproceso de “Alta de Usuarios” (Ver Anexo 23) y una matriz con cada incidente registrado para el subproceso de “Baja de Usuarios” (Ver Anexo 24) y se organizaron los incidentes de cada subproceso en base a los siguientes criterios:

a) Ordenar cronológicamente los registros obtenidos, detallando los datos relevantes que servirán para realizar comparaciones de tiempo entre dos usuarios con los mismos permisos, al momento de ejecutar y completar el subproceso de “Alta de Usuarios” o “Baja de Usuarios” en diferentes lapsos de tiempo (Ver Tabla N° 54).

Tabla N° 54:
Extracto de registros históricos con datos relevantes obtenidos del Sistema de Gestión de Incidentes.

Usuario	Apellido Nombre	Tipo usuario	Cargo	Área	Empresa	Fecha inicio Alta	Fecha Fin Alta
YTEXAV	XXXX	Externo	Analista Químico	Operaciones	XXXX	29-ago-16	01-sep-16
YTERIV	XXXX	Externo	Analista Sistemas	Sistemas	XXXX	01-sep-16	05-sep-16
TECGAK	XXXX	Pasante	Pasante	Comercial	XXXX	01-sep-16	06-sep-16
YTEJEN	XXXX	Externo	Medico	Seguridad	XXXX	01-sep-16	06-sep-16
YTELIZ	XXXX	Externo	Abogada	Comercial	XXXX	02-sep-16	09-sep-16
TECCAI	XXXX	Pasante	Pasante	RRHH	XXXX	14-sep-16	21-sep-16
YTEKLO	XXXX	Externo	Analista Funcional	Impuestos	XXXX	13-sep-16	16-sep-16
YTEPPA	XXXX	Externo	Auditora ARCH	Impuestos	XXXX	16-sep-16	24-sep-16
YTEZAR	XXXX	Externo	Coord. Security	Security	XXXX	19-sep-16	27-sep-16
TECZUM	XXXX	Interno	Analista Comercial	Comercial	XXXX	03-oct-16	11-oct-16
YTERUX	XXXX	Externo	Auditor PWC	Impuestos	XXXX	24-oct-16	27-oct-16
YTEVEC	XXXX	Externo	Analista Sistemas	Impuestos	XXXX	25-oct-16	31-oct-16
YTEJIM	XXXX	Externo	Coord. Security	Security	XXXX	08-nov-16	14-nov-16
YTEDAZ	XXXX	Externo	Analista Sistemas	Sistemas	XXXX	14-nov-16	15-nov-16
YTEAMD	XXXX	Externo	Auditor Operaciones	Operaciones	XXXX	16-nov-16	16-nov-16
YTEBAL	XXXX	Externo	Operador Security	Security	XXXX	22-nov-16	23-nov-16
YTECIS	XXXX	Externo	Operador Security	Security	XXXX	22-nov-16	23-nov-16
YTEIVA	XXXX	Externo	Operador Security	Security	XXXX	22-nov-16	23-nov-16
YTEFMA	XXXX	Externo	Analista Sistemas	Impuestos	XXXX	05-dic-16	08-dic-16
TECCIB	XXXX	Interno	Ing. Reservorios	Reservorios	XXXX	07-dic-16	14-dic-16
YTESOU	XXXX	Externo	Auditor	Operaciones	XXXX	03-ene-17	03-ene-17
YTERUX	XXXX	Externo	Auditor	Impuestos	XXXX	04-ene-17	04-ene-17
TECGAE	XXXX	Interno	Técnico de Mant.	Mantenimiento	XXXX	05-ene-17	05-ene-17

Nota: Nombres de usuarios y empresas se mantienen protegidos por confidencialidad de información de la empresa bajo estudio.
Fuente: Elaboración propia del Investigador

La columna “Tipo usuario” a la que hace referencia la Tabla N° 54, corresponde a:

- Interno: Usuario que brinda sus servicios profesionales contratado directamente por la Empresa de Consultoría para la Industria Petrolera.
- Externo: Usuario que brinda sus servicios profesionales a través de una empresa y que esta a su vez brinda sus servicios a la Empresa de Consultoría para la Industria Petrolera. Esto se produce cuando se requiere de forma temporal el soporte puntual de un especialista en determinada área, o debido a auditorias que ordenan los órganos de control del Gobierno donde personal de estos organismos ingresan temporalmente a la empresa.
- Pasante: Usuario temporal (seis meses) que realiza sus prácticas pre-profesionales a modo de pasantías y es contratado directamente por la Empresa de Consultoría para la Industria Petrolera.

b) Establecer en base a la complejidad de los permisos que se le asignaron al usuario, una codificación para el perfil de usuario de la siguiente manera (Ver Tabla N° 55).

Tabla N° 55:
Codificación para el perfil de usuario acorde a su complejidad de permisos de acceso y aplicaciones.

Código Perfil de Usuario			
Título	**Usuario Básico**	**Usuario Intermedio**	**Usuario Avanzado**
Código	**1**	**2**	**3**
Accesos	- Usuario de Red - Correo Electrónico - Herramientas de Comunicación Colaborativa - Extensión Telefónica (Si amerita) - Navegación Internet (Si amerita)	- Permisos Usuario Básico - Acceso Intranet - Repositorio de Información General - Repositorios de información específica - Información SharePoint Ecuador - Token / VPN (Si amerita)	- Permisos Usuario Básico - Permisos Usuario Intermedio - Acceso ERP - SAP - Repositorios información específica ARG - SharePoint ARG - Aplicaciones ARG - Asignación equipos celulares - Aplicaciones móviles

Fuente: Elaboración propia del Investigador.

c) Unificar la codificación del tipo de perfil de usuario con el registro de datos históricos, con el fin de determinar la complejidad de las actividades a ejecutar para los subprocesos de “Alta de Usuarios” o “Baja de Usuarios” (Ver Tabla N° 56).

Tabla N° 56:
Extracto de la unificación registros históricos con clasificación tipo de perfil de usuario.

Usuario	Cargo	Fecha inicio Alta	Fecha Fin Alta	Código Perfil Usuario	Básico	Intermedio	Avanzado
YTEXAV	Analista Químico	29-ago-16	01-sep-16	1	X		
YTERIV	Analista Sistemas	01-sep-16	05-sep-16	2		X	
TECGAK	Pasante	01-sep-16	06-sep-16	2		X	
YTEJEN	Medico	01-sep-16	06-sep-16	1	X		
YTELIZ	Abogada	02-sep-16	09-sep-16	2		X	
TECCAI	Pasante	14-sep-16	21-sep-16	2		X	
YTEKLO	Analista Funcional	13-sep-16	16-sep-16	3			X
YTEPPA	Auditora ARCH	16-sep-16	24-sep-16	3			X
YTEZAR	Coord. Security	19-sep-16	27-sep-16	2		X	
TECZUM	Analista Comercial	03-oct-16	11-oct-16	3			X
YTERUX	Auditor PWC	24-oct-16	27-oct-16	3			X
YTEVEC	Analista Sistemas	25-oct-16	31-oct-16	3			X
YTEJIM	Coord. Security	08-nov-16	14-nov-16	2		X	
YTEDAZ	Analista Sistemas	14-nov-16	15-nov-16	2		X	
YTEAMD	Auditor	16-nov-16	16-nov-16	2		X	
YTEBAL	Operador Security	22-nov-16	23-nov-16	1	X		
YTECIS	Operador Security	22-nov-16	23-nov-16	1	X		
YTEIVA	Operador Security	22-nov-16	23-nov-16	1	X		
YTEFMA	Analista Sistemas	05-dic-16	08-dic-16	3			X
TECCIB	Ing. Reservorios	07-dic-16	14-dic-16	2		X	

Fuente: Elaboración propia del Investigador

d) Detallar las actividades que se identificaron en la etapa de levantamiento de los subprocesos de “Alta de Usuarios” y “Baja de Usuarios” y dividirlas para realizar la medición del trabajo. En la Tabla N° 57 se presenta un extracto de las primeras actividades identificadas para el subproceso de “Alta de Usuarios”. La identificación de actividades se basó en los flujogramas de cada subproceso antes y después de su modificación.

Tabla N° 57:

Extracto de actividades identificadas para el subproceso de "Alta de Usuarios".

Recibir Notificación Alta	Crear Siglas en ADM ABM Usuarios	Solicitar Usuario Modelo	Definir Usuario Modelo	Informar Permisos de Usuario a Aplicaciones	Crear usuario en AD (claves y correo)	Asignar Permisos Aplicaciones ARG	Alta en Aplicaciones ECU, permisos repositorios

Fuente: Elaboración propia del Investigador

A continuación, se listan todas las actividades que se identificaron para el subproceso de "Alta de Usuarios". En el Anexo 26, se presenta la matriz que contiene todas las actividades sin datos de usuarios para este subproceso:

- Recibir Notificación Alta.
- Crear Siglas en ADM ABM Usuarios.
- Solicitar Usuario Modelo.
- Definir Usuario Modelo.
- Informar Permisos de Usuario a Aplicaciones.
- Crear usuario en AD (claves y correo).
- Asignar Permisos Aplicaciones ARG.
- Alta en Aplicaciones ECU, permisos repositorios.
- Definir Equipos a asignar.
- Alta equipo en AD.
- Actualizar equipo en Inventario.

- Generar tarjeta acceso.
- Notificar asignación equipos.
- Asignar claves de marcación telefonía fija y Wi-Fi.
- Generar Clave de Conexión remota.
- Configurar equipos con Software.
- Configurar perfil usuario.
- Configurar Token y VPN.
- Configurar línea celular y aplicaciones.
- Entregar equipos y tarjeta de acceso.
- Notificar cierre y enviar reporte de equipos.
- Cerrar proceso de alta.

A continuación, se listan todas las actividades que se identificaron para el subproceso de "Baja de Usuarios". En el Anexo 27, se presenta la matriz que contiene todas las actividades sin datos de usuarios para este subproceso:

- Iniciar proceso de baja en ABM.
- Bloquear código de Usuario en ABM.
- Retirar equipos asignados.
- Entregar reporte de retiro de equipos.
- Respaldar información de usuario.
- Entregar respaldo a jefatura.
- Retirar tarjeta de acceso.
- Dar de baja en aplicaciones ECU.
- Dar de baja en aplicaciones ARG.

- Eliminar usuario en ABM.
- Eliminar manualmente de grupos y repositorios.
- Formatear equipo.
- Eliminar código equipo de la red.
- Bloquear claves de marcación telefónica y Wi-Fi.
- Bloquear clave de conexión remota.
- Retirar equipo celular.
- Dar de baja línea celular.
- Actualizar inventario de equipos.
- Cerrar el proceso de baja.

e) Unificar la matriz de registros y actividades; en la Tabla N° 58 se presenta un extracto de la unificación de registros de usuario, con su tipificación y actividades que se ejecutan para el subproceso de "Alta de Usuarios".

Tabla N° 58:
Extracto de unificación de registros y actividades identificadas para el subproceso de "Alta de Usuarios".

Usuario	Fecha inicio Alta	Fecha Fin Alta	Código Perfil Usuario	Básico	Intermedio	Avanzado	Recibir Notificación Alta	Crear Siglas en ADM ABM Usuarios	Solicitar Usuario Modelo
YTEXAV	29-ago-16	01-sep-16	1	X					
YTERIV	01-sep-16	05-sep-16	2		X				
TECGAK	01-sep-16	06-sep-16	2		X				
YTEJEN	01-sep-16	06-sep-16	1	X					
YTELIZ	02-sep-16	09-sep-16	2		X				
TECCAI	14-sep-16	21-sep-16	2		X				
YTEKLO	13-sep-16	16-sep-16	3			X			

Fuente: Elaboración propia del Investigador

La matriz completa se presenta en los Anexos 28 y 29 para cada subproceso.

3.3.4 Paso 4: Determinar si el tamaño de la muestra es significativa.

1. Se ejecutó el cálculo estadístico para determinar el valor que indique que la muestra sea significativa, utilizando la siguiente fórmula (Murray & Larry, 2009):

$$n = \frac{N * Z_{\propto}^{2} * p * q}{d^{2} * (N - 1) + Z_{\propto}^{2} * p * q}$$

Donde:

n = Representa el valor que demuestra que el tamaño de la muestra es significativa y el cual se debe calcular.

N = Representa el tamaño de la población finita que para el caso del subproceso de “Alta de Usuarios” tiene un total de 61 registros y para el subproceso de “Baja de Usuarios” tiene un total de 80 registros.

Z = Representa un valor correspondiente a la distribución de gauss (Tabla de valores estándar – Ver Anexo 25) para Zα igual a 0.05 cuyo valor es igual a 1,96; este valor representa el porcentaje de seguridad para el cálculo, que entes caso es del 95%.

p = Representa el valor de la proporción esperada (en este caso p = 0.5 (50%) lo cual maximiza el tamaño de la muestra al combinar con el valor de q).

q = Diferencia de proporción esperada que equivale a la resta de 1 – p (en este caso 1 – 0,5 = 0,5).

d = Precisión o error que se estima cometer, donde el autor recomienda utilizar el valor del 5%, es decir d = 0,05.

Los valores para el cálculo de valores de muestra significativa se presentan en la Tabla N° 59:

Tabla N° 59:
Cálculo de muestra de población significativa para los subprocesos de "Alta de Usuarios" y "Baja de Usuarios".

Alta de Usuarios		**Baja de Usuarios**	
Parámetro	**Valor**	**Parámetro**	**Valor**
Z	61	Z	80
p	50	p	50
q	5	q	5
s	95	s	95
n	**53**	**n**	**67**

Nota. Los valores de n se los redondea a su inmediato superior como indican los autores (Murray & Larry, 2009).
Fuente: Elaboración propia de Investigador.

Partiendo de los registros obtenidos y los datos que se extrajeron del Sistema de Gestión de Incidentes, se tomó el 100% de los datos de las actividades que se ejecutaron para los subprocesos de "Alta de Usuarios" y "Baja de Usuarios", cubriendo con ello el valor significativo que se calculó estadísticamente.

3.3.5 Paso 5: Ejecutar el proceso de cálculo.

Contando con los registros de datos históricos del Sistema de Gestión de Incidentes, se procede a completar la Matriz de Registro de tiempos de los subprocesos de “Alta de Usuarios” y “Baja de Usuarios” ejecutando los siguientes pasos:

- Ordenar los registros por Tipo de usuario, considerando que la asignación de permisos difiere mucho del perfil que se requiere habilitar.
- Registrar el tiempo dedicado a ejecutar cada actividad de cada subproceso (“Alta de Usuario” o “Baja de Usuario”).
- Medición total del tiempo dedicado para completar los subprocesos (“Alta de Usuario” o “Baja de Usuario”).
- Calcular la media, desviación estándar de los datos y el coeficiente de variación de los tiempos registrados.
- Identificar las actividades cuyo tiempo de ejecución representa un pico en el histograma de ejecución del proceso.

A continuación se presenta los cálculos realizados para cada subproceso.

3.3.5.1 Subproceso de “Alta de Usuarios” antes de realizar cambios en el flujograma:

Se tomaron cuarenta y siete (47) registros del Sistema de Gestión de incidentes y se los organizó en las veinte y dos (22) actividades que se ejecutan según lo indica el Flujograma del subproceso y para cada una se registró el tiempo en la Matriz (Ver Anexo 30). Se totalizó el tiempo empleado por cada registro según el tipo de usuario (Ver Figura N° 31).

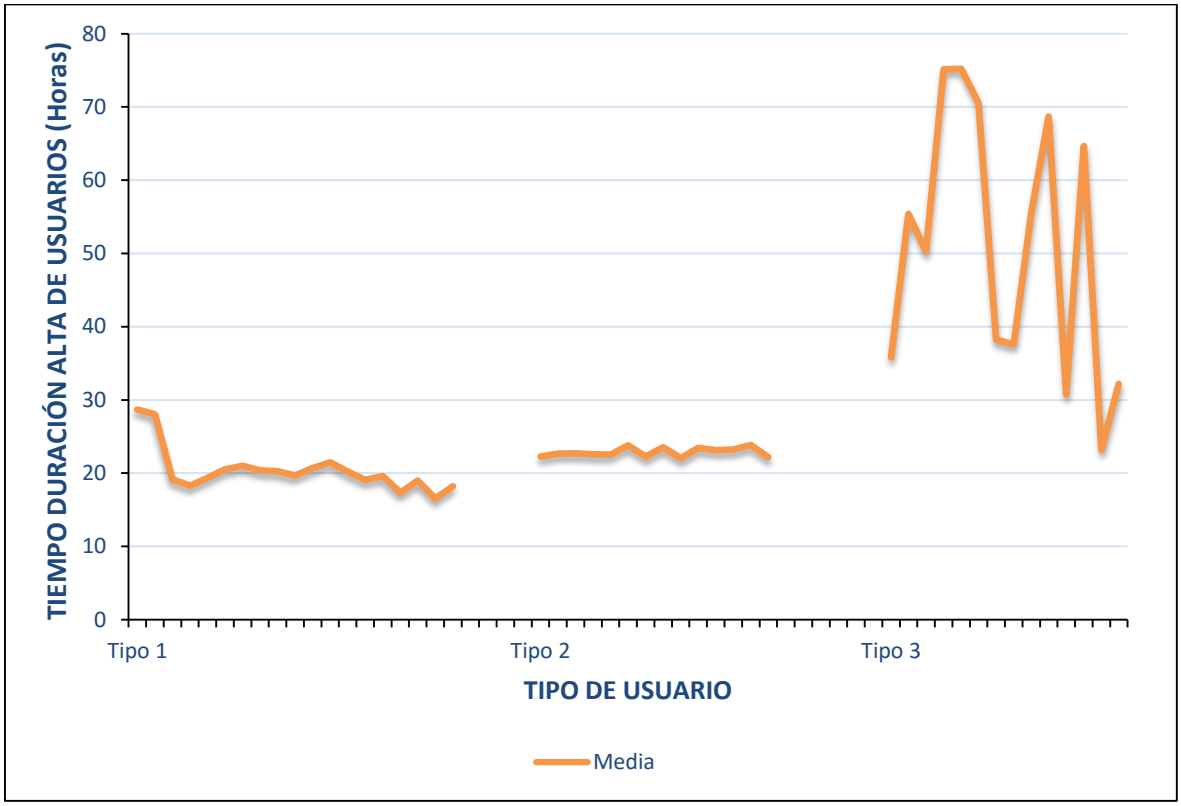


Figura N° 31: Tiempo registrado para culminar el subproceso de "Alta de Usuarios" medido en horas antes de realizar cambios en el Flujograma.
Fuente: Elaboración propia del Investigador.

Se realizó el cálculo de la Media y desviación estándar de cada actividad para los cuarenta y siete registros divididos por el tipo de usuario (Ver Figuras N° 32 a la Figura N° 34).

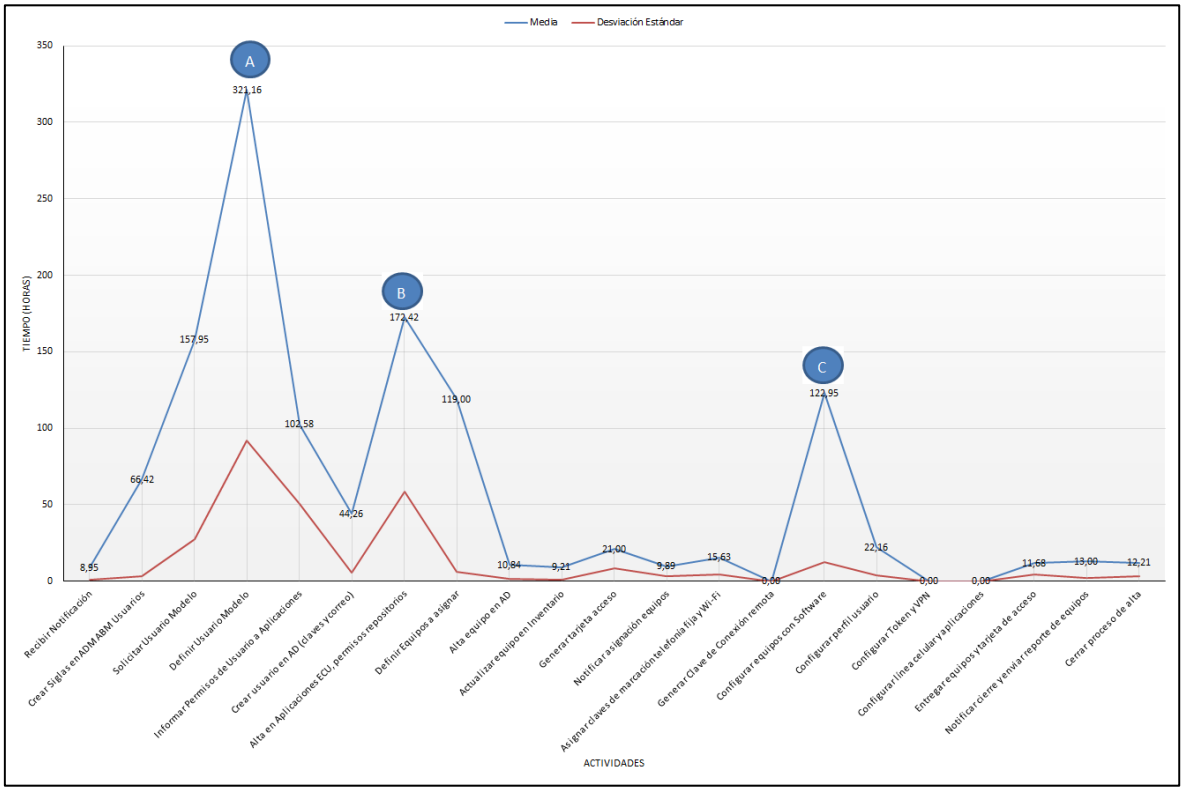


Figura N° 32: Tiempo registrado para culminar el subproceso de “Alta de Usuarios” para usuarios de Tipo 1, medido en horas antes de realizar cambios en el Flujograma
Fuente: Elaboración propia del Investigador.

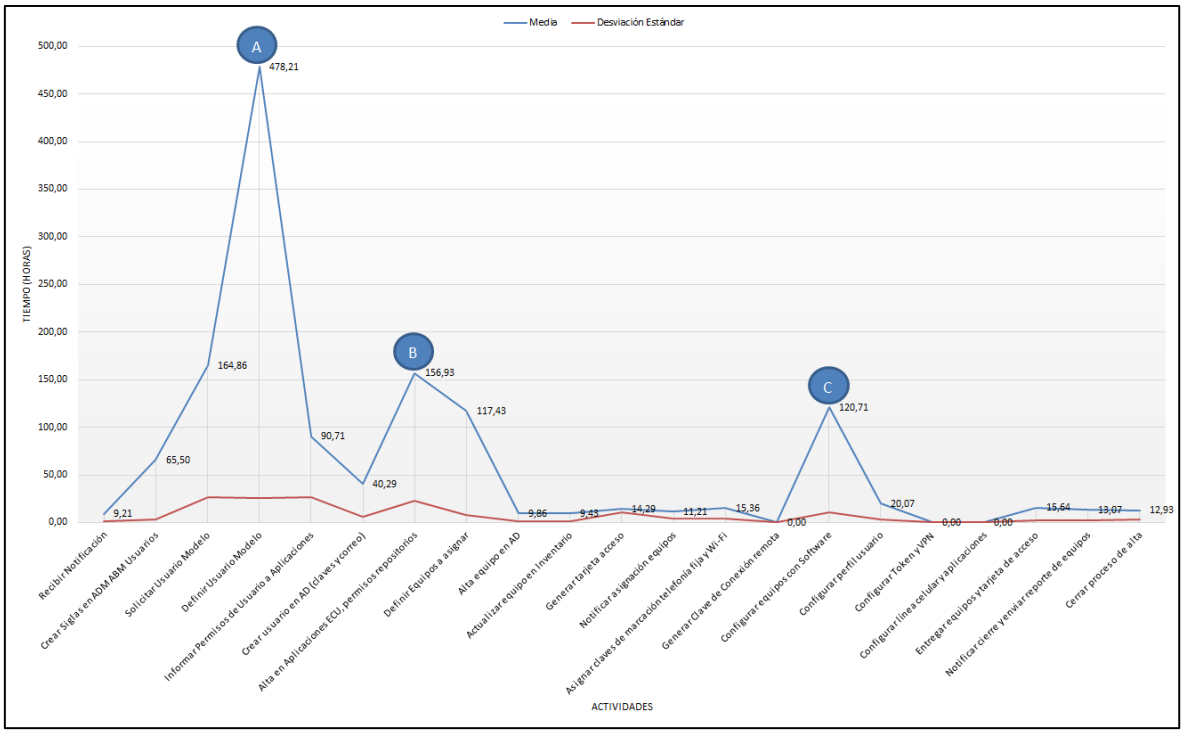


Figura N° 33: Tiempo registrado para culminar el subproceso de “Alta de Usuarios” para usuarios de Tipo 2, medido en horas antes de realizar cambios en el Flujograma.
Fuente: Elaboración propia del Investigador.

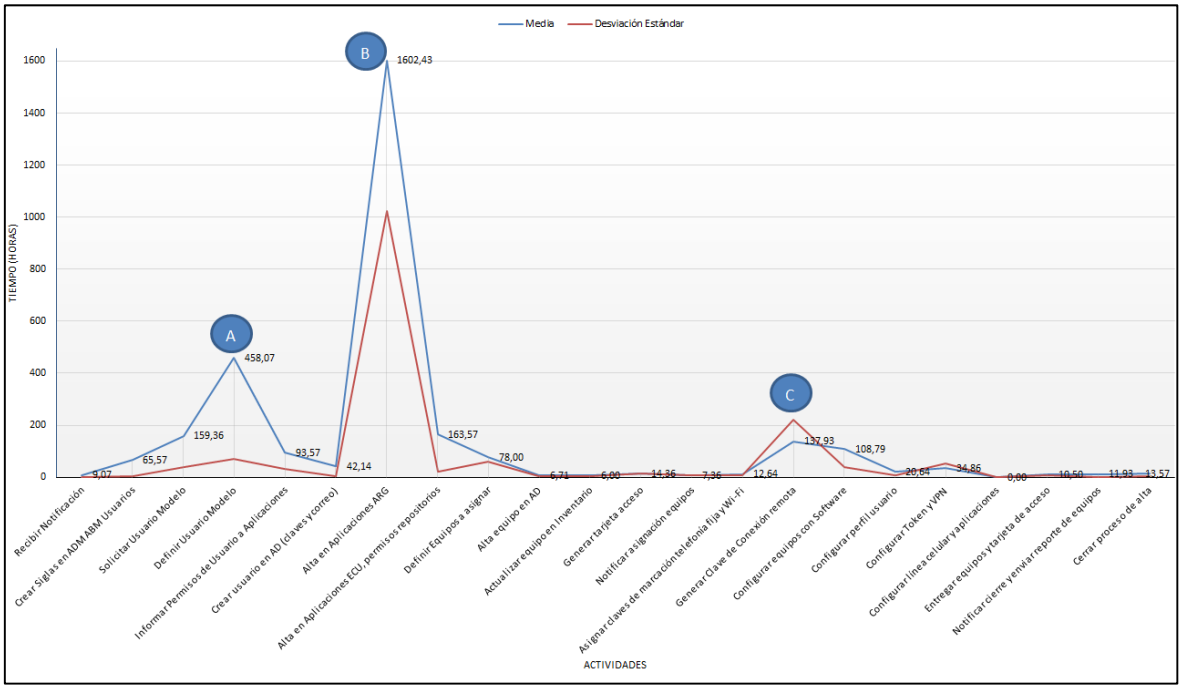


Figura N° 34: Tiempo registrado para culminar el subproceso de "Alta de Usuarios" para usuarios de Tipo 3, medido en horas antes de realizar cambios en el Flujograma.
Fuente: Elaboración propia del Investigador.

En las Figuras N°32, N° 33 y N° 34 se resaltan las actividades de mayor duración para cada tipo de usuario y su porcentaje de ejecución en tiempo respecto a todo el subproceso de "Alta de Usuarios", las cuales se detallan en la Tabla N° 60:

Tabla N° 60:
Identificación de actividades de mayor duración para cada tipo de usuario antes de aplicar cambios en el flujograma del Subproceso de "Alta de Usuarios".

Tipo	Identificador	Actividad	% del tiempo dentro del subproceso de Alta de Usuarios
Tipo 1	A	Definir Usuario modelo	26,24%
	B	Alta en aplicaciones ECU, permisos repositorios	14,09%
	C	Configurar equipos con software	10,04%
Tipo 2	A	Definir Usuario modelo	35,01%
	B	Alta en aplicaciones ECU, permisos repositorios	11,49%
	C	Configurar equipos con software	8,83%
Tipo 3	A	Definir Usuario modelo	14,98%
	B	Alta aplicaciones ARG	52,41%
	C	Generar clave de conexión remota	4,51%

Fuente: Elaboración propia de Investigador.

Por último, se presenta la dispersión de los datos en base al cálculo del Coeficiente de Variación para cada Tipo de Usuario (Ver Figura N° 35).

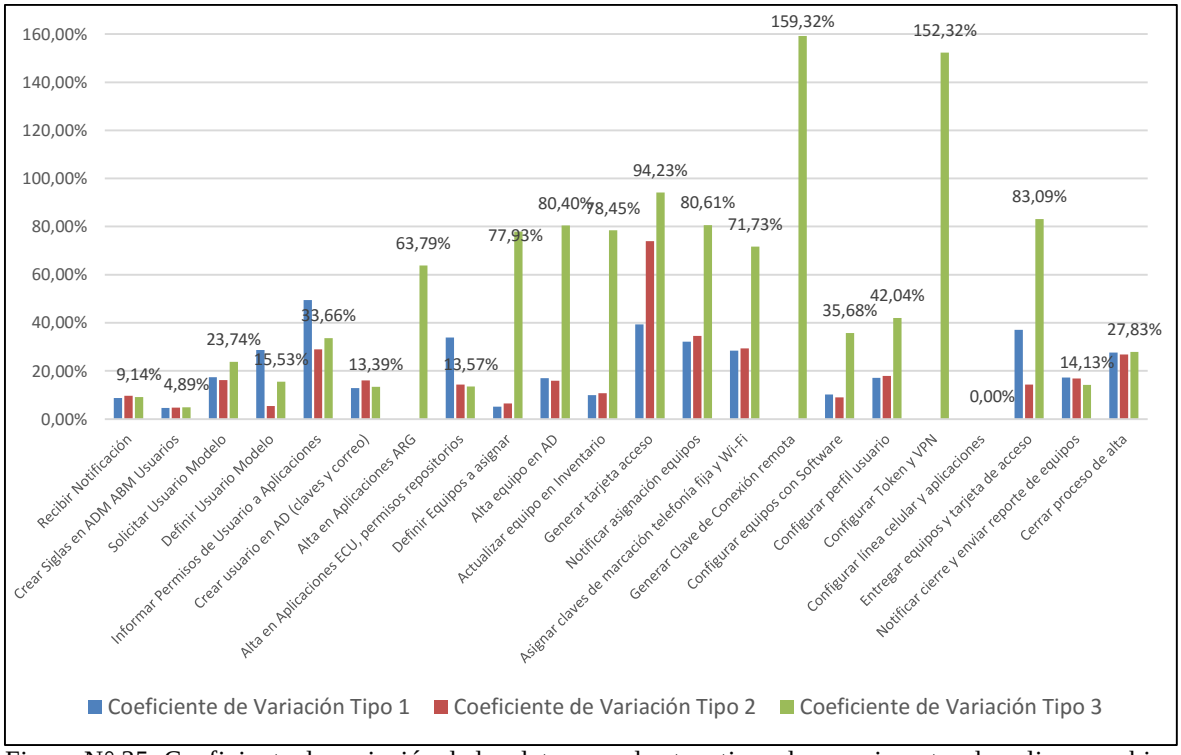


Figura N° 35: Coeficiente de variación de los datos para los tres tipos de usuario antes de aplicar cambios en el flujograma del Subproceso de Alta de Usuarios.
Fuente: Elaboración propia del Investigador.

Como se observa en la Figura N° 35, existen registros con un valor de cero (0), esto es debido a que existen actividades que no se ejecutan para todo tipo de usuario como:

- El alta de aplicaciones ARG no es obligatoria para todos los usuarios, solo puede requerir un acceso puntual.
- La tarjeta de acceso no se asigna a todo el personal, solo a personal propio y en campamentos a personal de supervisión.
- El Token y VPN solo se asigna para usuarios internos y que harán uso de equipos portátiles.

- Usuarios externos que ingresan por trabajos puntuales a los cuales no se les asigna equipos ya que trabajan con sus propias computadoras, entre las razones más relevantes.

3.3.5.2 Subproceso de “Alta de Usuarios” después de realizar cambios en el flujograma.

Se tomaron catorce (14) registros del Sistema de Gestión de incidentes, de los cuales se dividió en las veinte y dos (22) actividades que se ejecutaban según lo indica el Flujograma del subproceso y para cada una se registró el tiempo en la Matriz (Ver Anexo 30) se totalizó el tiempo empleado por cada registro para culminar el subproceso dividido por el tipo de usuario (Ver Figura N° 36).

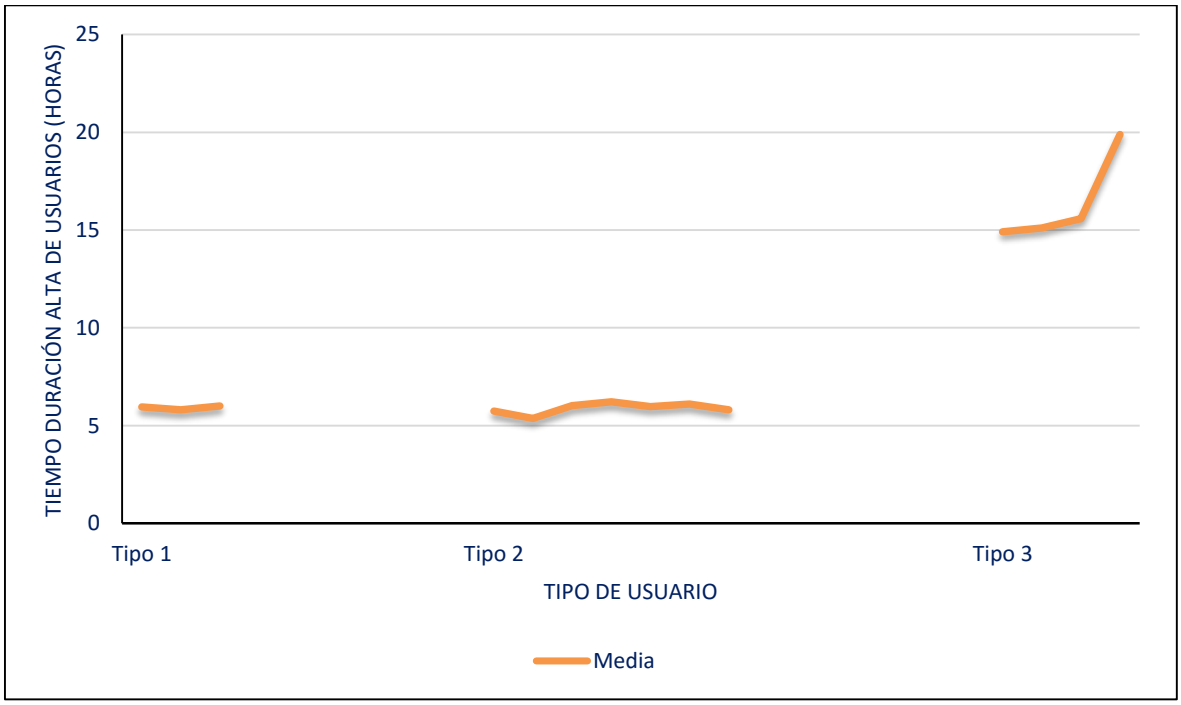


Figura N° 36: Tiempo registrado para culminar el subproceso de “Alta de Usuarios” medido en horas después de realizar cambios en el Flujograma.
Fuente: Elaboración propia del Investigador.

Se realizó el cálculo de la Media y desviación estándar de cada actividad para los catorce registros divididos por el tipo de usuario (Ver Figuras N° 37 a la Figura N° 39).

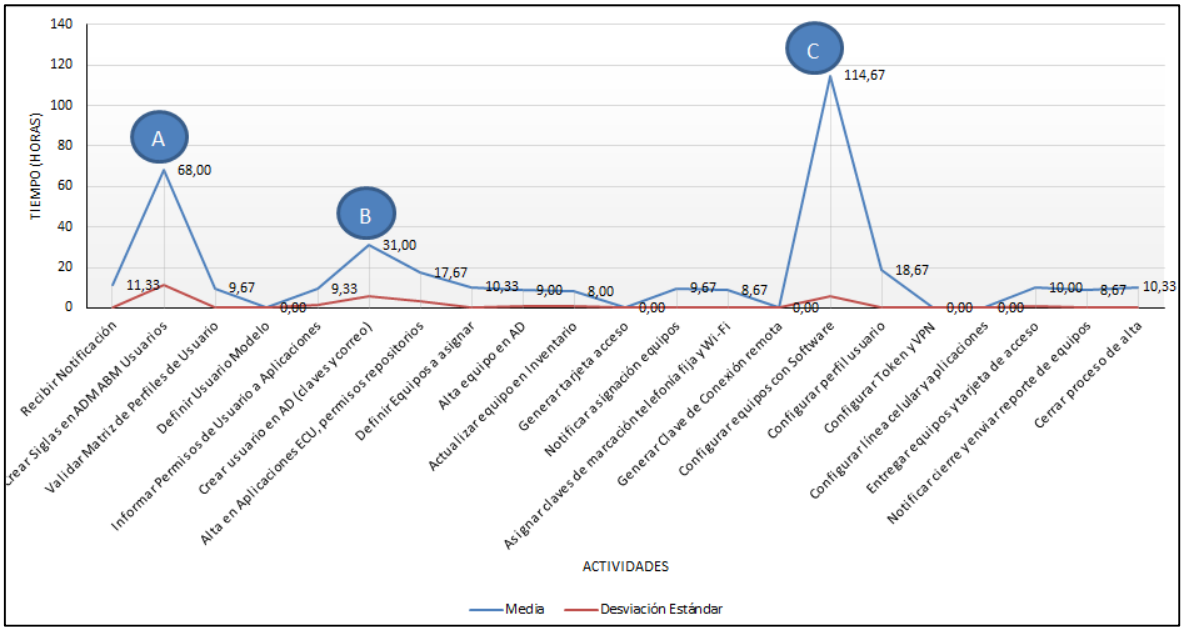


Figura N° 37: Tiempo registrado para culminar el subproceso de "Alta de Usuarios" para usuarios de Tipo 1, medido en horas después de realizar cambios en el Flujograma.
Fuente: Elaboración propia del Investigador.

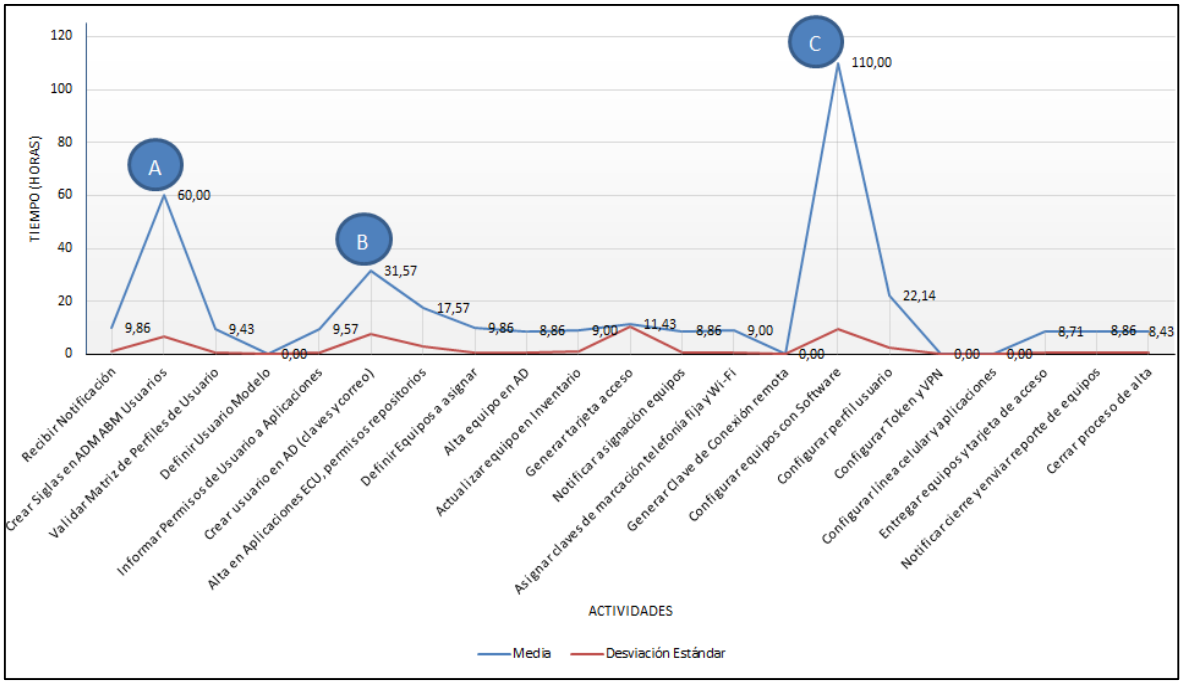


Figura N° 38: Tiempo registrado para culminar el subproceso de "Alta de Usuarios" para usuarios de Tipo 2, medido en horas después de realizar cambios en el Flujograma.
Fuente: Elaboración propia del Investigador.

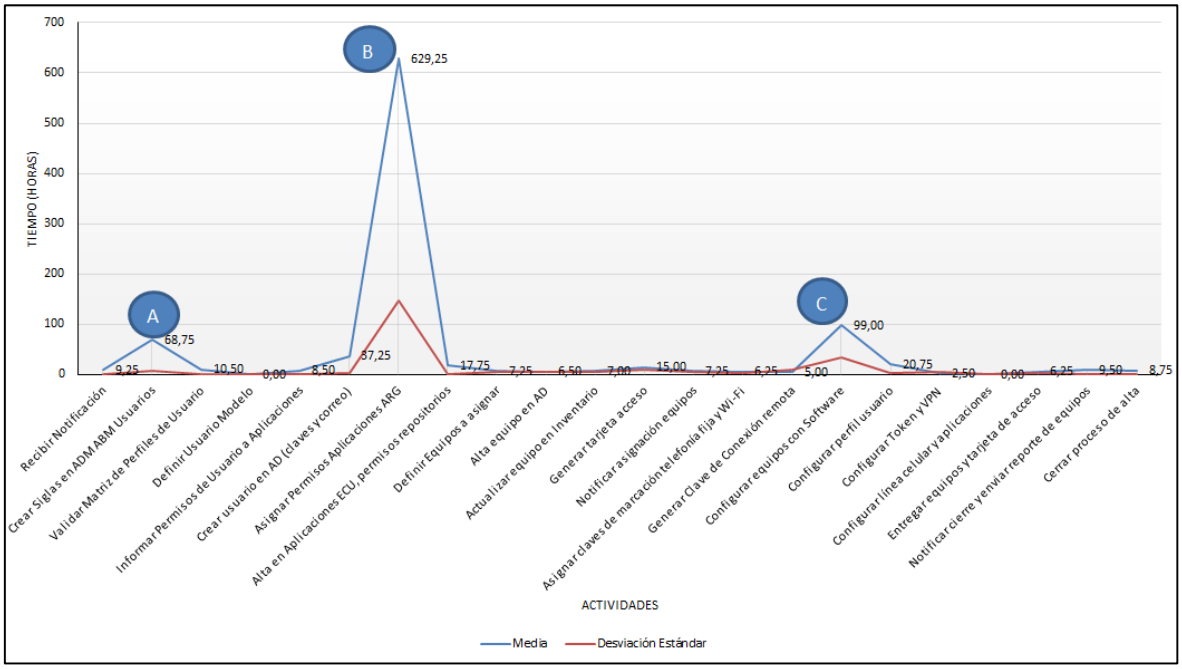


Figura N° 39: Tiempo registrado para culminar el subproceso de "Alta de Usuarios" para usuarios de Tipo 3, medido en horas después de realizar cambios en el Flujograma.
Fuente: Elaboración propia del Investigador.

En las Figuras N°37, N° 38 y N° 39 se resaltan las actividades de mayor duración para cada tipo de usuario y su porcentaje de ejecución en tiempo respecto a todo el subproceso de "Alta de Usuarios", las cuales se detallan en la Tabla N° 61:

Tabla N° 61:
Identificación de actividades de mayor duración para cada tipo de usuario después de aplicar cambios en el flujograma del Subproceso de "Alta de Usuarios".

Tipo	Identificador	Actividad	% del tiempo dentro del subproceso de Alta de Usuarios
Tipo 1	A	Crear Siglas en ADM ABM Usuarios	19,15%
	B	Crear usuario en AD (claves y correo)	8,73%
	C	Configurar equipos con Software	32,30%
Tipo 2	A	Crear Siglas en ADM ABM Usuarios	16,99%
	B	Crear usuario en AD (claves y correo)	8,94%
	C	Configurar equipos con Software	31,14%
Tipo 3	A	Crear Siglas en ADM ABM Usuarios	7,00%
	B	Asignar Permisos Aplicaciones ARG	64,06%
	C	Configurar equipos con Software	10,08%

Fuente: Elaboración propia de Investigador.

Por último, se puede validar también la dispersión de los datos en base al cálculo del Coeficiente de Variación para cada Tipo de Usuario (Ver Figura N° 40).

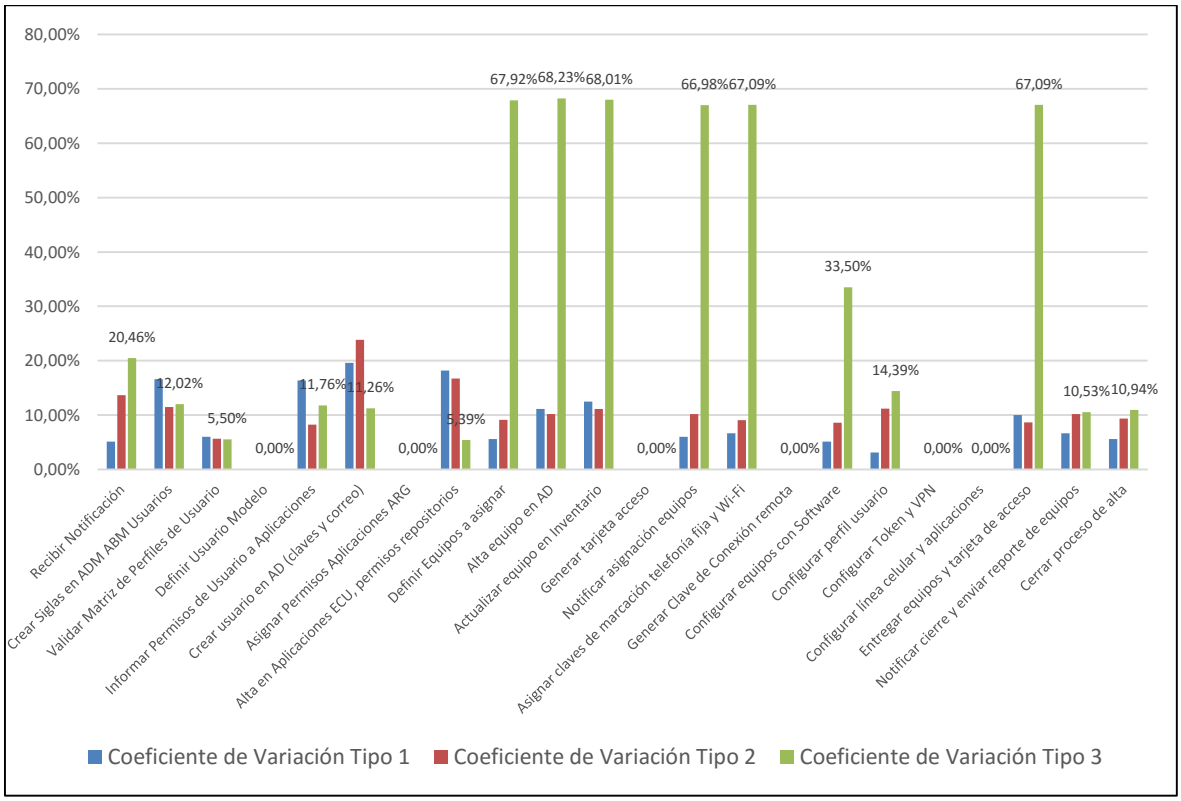


Figura N° 40: Coeficiente de variación de los datos para los tres tipos de usuario después de aplicar cambios en el Flujograma del Subproceso de Alta de Usuarios.
Fuente: Elaboración propia del Investigador.

Partiendo de los valores presentados en las Tablas N° 60 y N° 61, se realiza la comparativa de las mismas, considerando las actividades cuyo tiempo de ejecución representa el mayor porcentaje dentro del subproceso de alta, y esta se presenta en la Tabla N° 62.

Tabla N° 62:

Comparación de actividades de mayor duración para cada tipo de usuario antes y después de aplicar cambios en el flujograma del subproceso "Alta de Usuarios".

Tipo	Identificador	Actividad	Antes Cambio Flujo: % del tiempo dentro del subproceso de Alta de Usuarios	Después Cambio Flujo: % del tiempo dentro del subproceso de Alta de Usuarios
Tipo 1	A	Definir Usuario modelo	26,24%	2,72%
	B	Alta en aplicaciones ECU, permisos repositorios	14,09%	4,98%
	C	Configurar equipos con software	10,04%	32,30%
Tipo 2	A	Definir Usuario modelo	35,01%	2,67%
	B	Alta en aplicaciones ECU, permisos repositorios	11,49%	4,98%
	C	Configurar equipos con software	8,83%	31,15%
Tipo 3	A	Definir Usuario modelo	14,98%	1,96%
	B	Alta aplicaciones ARG	52,41%	64,06%
	C	Generar clave de conexión remota	4,51%	0,51%

Fuente: Elaboración propia de Investigador.

Considerando los resultados de la Tabla N° 62, se puede observar que la actividad "Definir Usuario Modelo" por su porcentaje en el tiempo de ejecución, fue identificada como una de las tres actividades que mayor tiempo demandaba para completar el subproceso de "Alta de Usuarios" antes de su cambio en el flujograma; al ser reemplazada con la actividad "Validar Matriz de Perfiles de Usuario", este porcentaje disminuye en un 89,63% para usuarios de Tipo 1; 92,37% para usuarios del tipo 2 y 86,91% para usuarios de Tipo 3. Esto genera que el tiempo total de ejecución del subproceso se reduzca y por ende que el porcentaje de demanda de tiempo por actividad varíe y se redistribuya.

Así también existen actividades cuyo porcentaje de demanda de tiempo sobresale respecto al resto (aunque su tiempo medido no se haya incrementado), pero esto se debe además de la reducción en el tiempo de ejecución completa del subproceso, a que estas

actividades son tareas manuales como lo es “Configurar equipos con Software desde cero” y de las cuales su tiempo no se enfocó para reducción.

3.3.5.3 Subproceso de “Baja de Usuarios” antes de realizar cambios en el flujograma.

Se tomaron cincuenta y ocho (58) registros del Sistema de Gestión de incidentes, de los cuales se dividió en las diez y nueve (19) actividades que se ejecutaban según lo indica el flujograma del subproceso y para cada una se registró el tiempo en la Matriz (Ver Anexo 31) totalizando el tiempo empleado por cada registro para culminar el subproceso dividido por el tipo de usuario (Ver Figura N° 41).

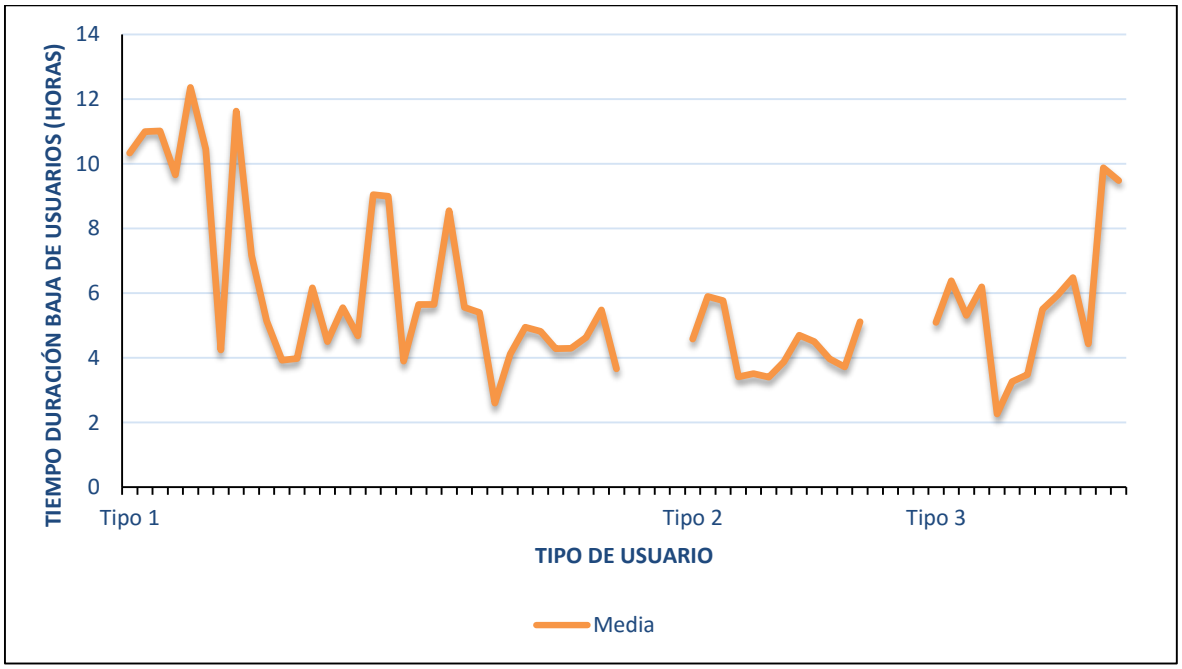


Figura N° 41: Tiempo registrado para culminar el subproceso de “Baja de Usuarios” medido en horas antes de realizar cambios en el Flujograma.
Fuente: Elaboración propia del Investigador.

Se realizó el cálculo de la Media y desviación estándar de cada actividad para los cincuenta y ocho registros divididos por el tipo de usuario (Ver Figuras N° 42 a la Figura N° 44).

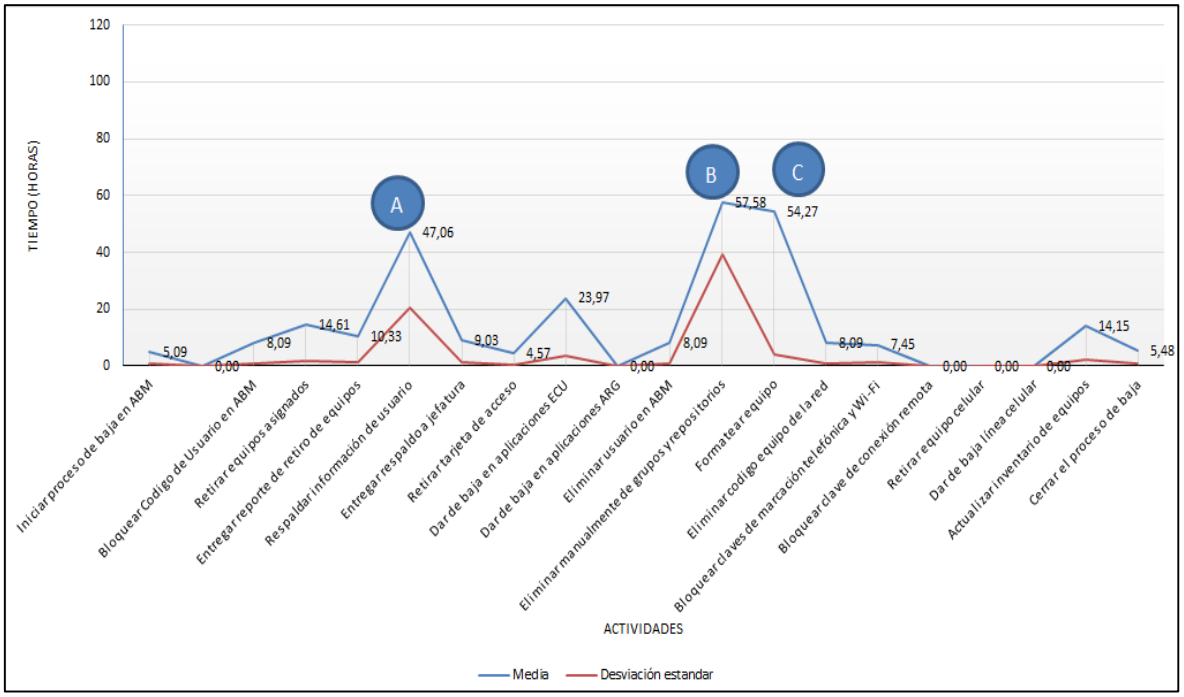


Figura N° 42: Tiempo registrado para culminar el subproceso de "Baja de Usuarios" para usuarios de Tipo 1, medido en horas antes de realizar cambios en el Flujograma.
Fuente: Elaboración propia del Investigador.

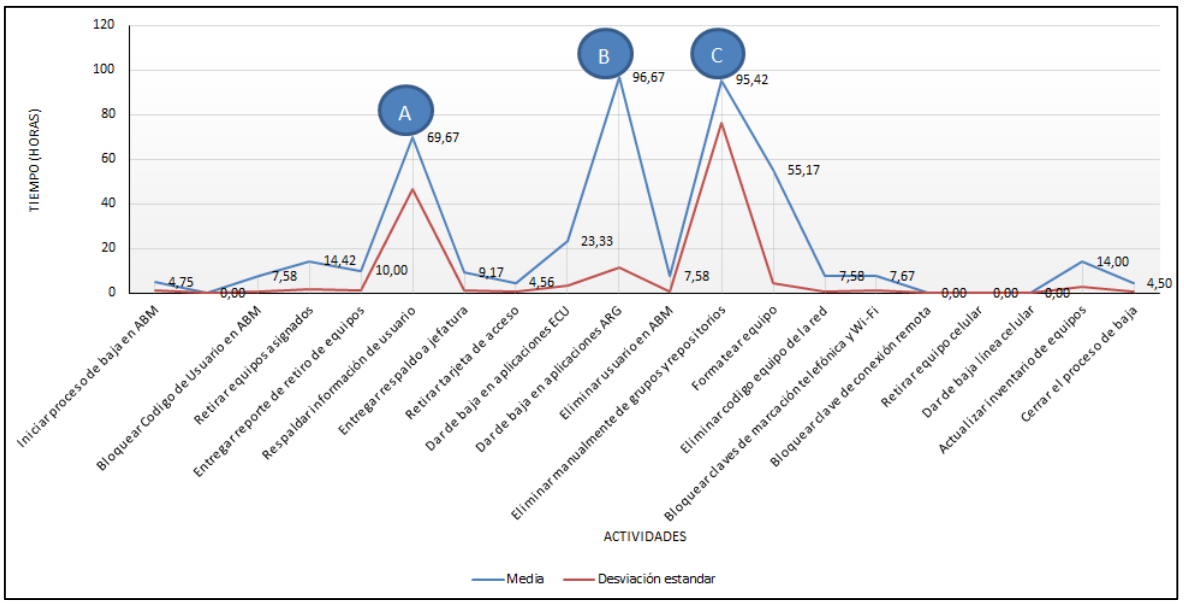


Figura N° 43: Tiempo registrado para culminar el subproceso de "Baja de Usuarios" para usuarios de Tipo 2, medido en horas antes de realizar cambios en el Flujograma.
Fuente: Elaboración propia del Investigador.

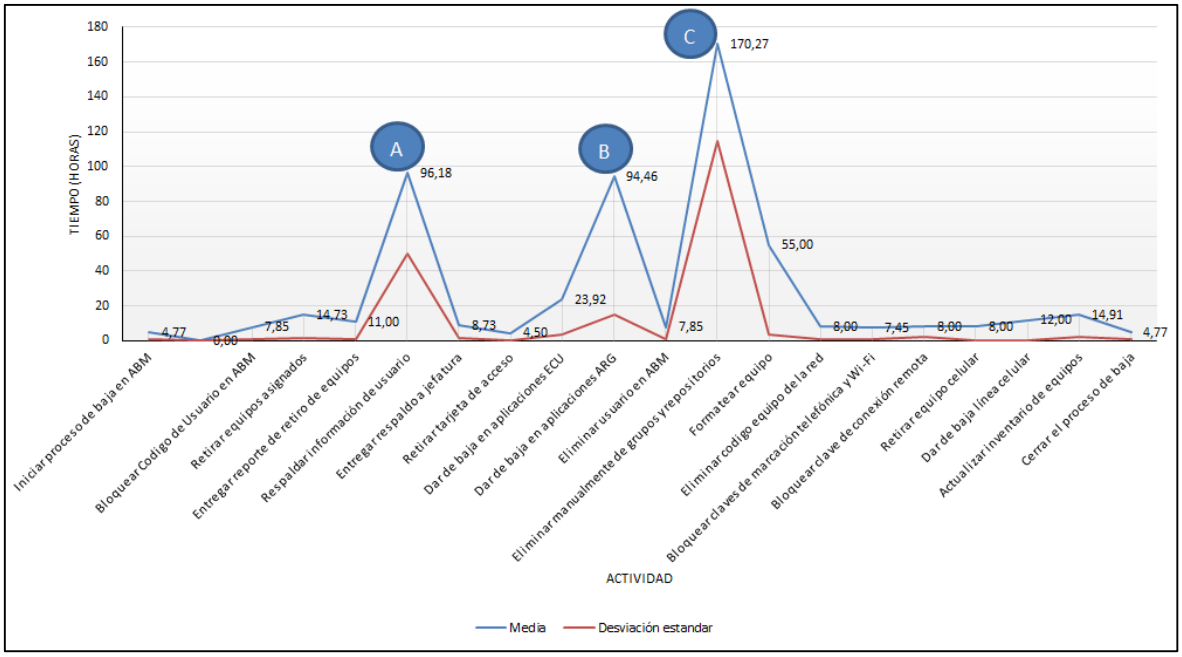


Figura N° 44: Tiempo registrado para culminar el subproceso de "Baja de Usuarios" para usuarios de Tipo 3, medido en horas antes de realizar cambios en el Flujograma.
Fuente: Elaboración propia del Investigador.

En las Figuras N°42, N° 43 y N° 44 se resaltan las actividades de mayor duración para cada tipo de usuario y su porcentaje de ejecución en tiempo respecto a todo el subproceso de "Baja de Usuarios", las cuales se detallan en la Tabla N° 63:

Tabla N° 63:
Identificación de actividades de mayor duración para cada tipo de usuario antes de aplicar cambios en el flujograma del Subproceso de "Baja de Usuarios".

Tipo	Identificador	Actividad	% del tiempo dentro del subproceso de Baja de Usuarios
Tipo 1	A	Respaldar información de usuario	16,28%
	B	Eliminar manualmente grupos y repositorios	21,21%
	C	Formatear equipo	19,99%
Tipo 2	A	Respaldar información de usuario	16,06%
	B	Dar de baja aplicaciones ARG	22,29%
	C	Eliminar manualmente grupos y repositorios	22,00%
Tipo 3	A	Respaldar información de usuario	17,00%
	B	Dar de baja aplicaciones ARG	19,74%
	C	Eliminar manualmente grupos y repositorios	30,11%

Fuente: Elaboración propia de Investigador.

Por último, se puede validar también la dispersión de los datos en base al cálculo del Coeficiente de Variación para cada Tipo de Usuario (Ver Figura N° 45).

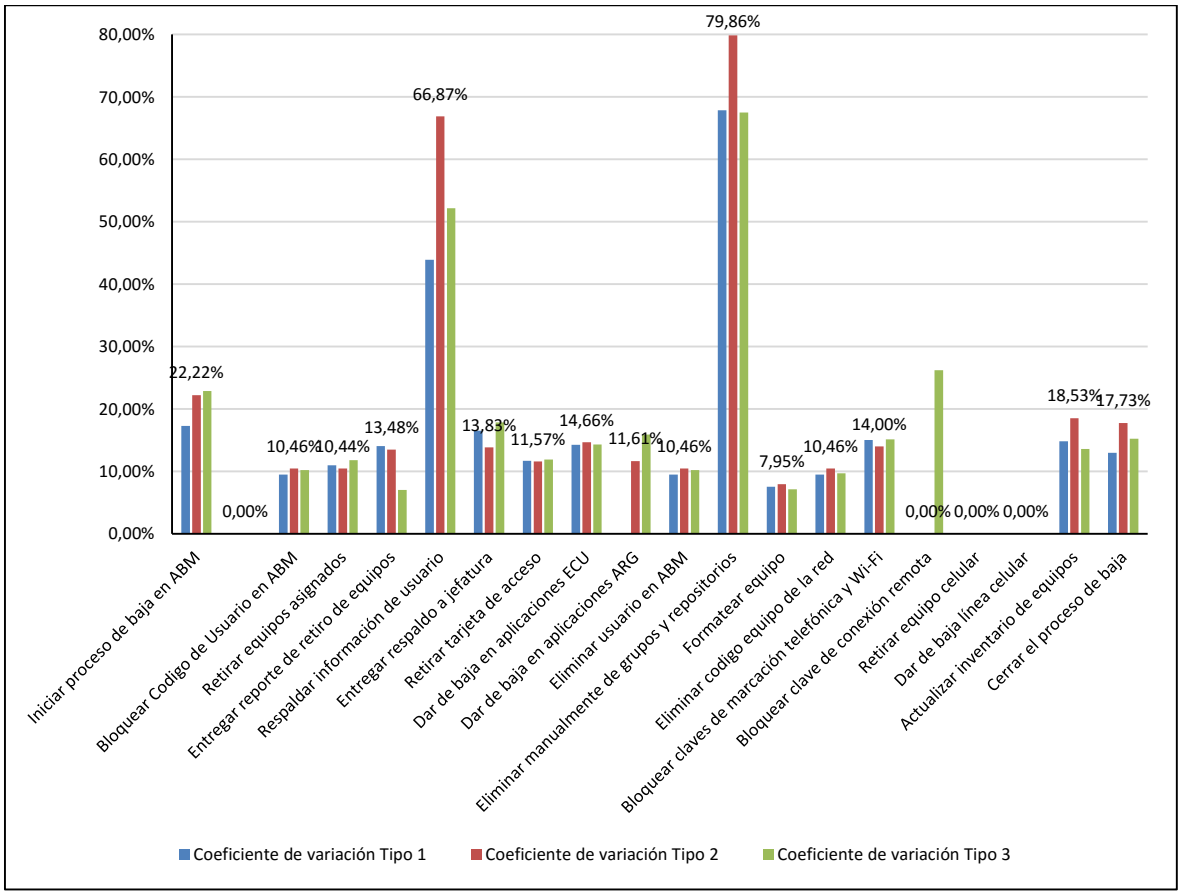


Figura N° 45: Coeficiente de variación de los datos para los tres tipos de usuario antes de aplicar cambios en el Flujograma del Subproceso de Baja de Usuarios.
Fuente: Elaboración propia del Investigador.

Como se observa en la Figura N° 45, existen registros con un valor de cero (0), esto es debido a que existen actividades que no se ejecutan para todo tipo de usuario:

- El retiro de la tarjeta de acceso no ejecuta para todo el personal, ya que no es asignada a todos los usuarios, solo a personal propio y en campamentos a personal de supervisión.

- Usuarios externos que ingresan por trabajos puntuales a los cuales no se les asigna equipos ya que trabajan con sus propias computadoras, no se les puede retirar estos equipos, entre las razones más relevantes.

3.3.5.4 Subproceso de “Baja de Usuarios” después de realizar cambios en el flujograma.

Se tomaron veinte y dos (22) registros del Sistema de Gestión de incidentes, de los cuales se dividió en las diecinueve (19) actividades que se ejecutaban según lo indica el Flujograma del subproceso y para cada una se registró el tiempo en la Matriz (Ver Anexo 31) totalizando el tiempo empleado por cada registro para culminar el subproceso dividido por el tipo de usuario (Ver Figura N° 46).

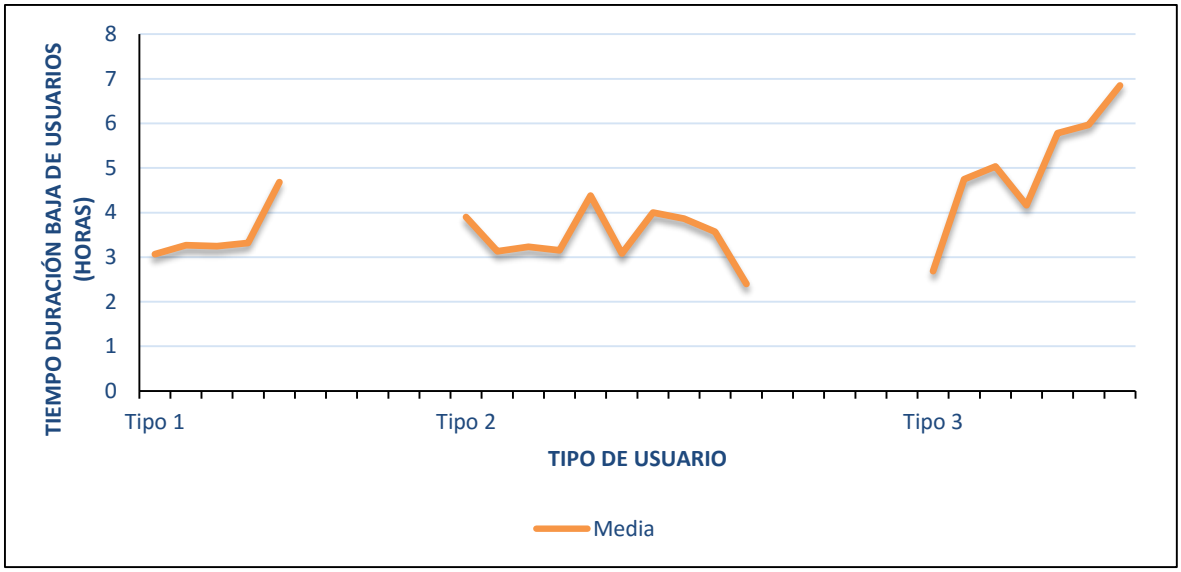


Figura N° 46: Tiempo registrado para culminar el subproceso de “Baja de Usuarios” medido en horas después de realizar cambios en el Flujograma.
Fuente: Elaboración propia del Investigador.

Se realizó el cálculo de la Media y desviación estándar de cada actividad para los diecinueve registros divididos por el tipo de usuario (Ver Figuras N° 47 a la Figura N° 49).

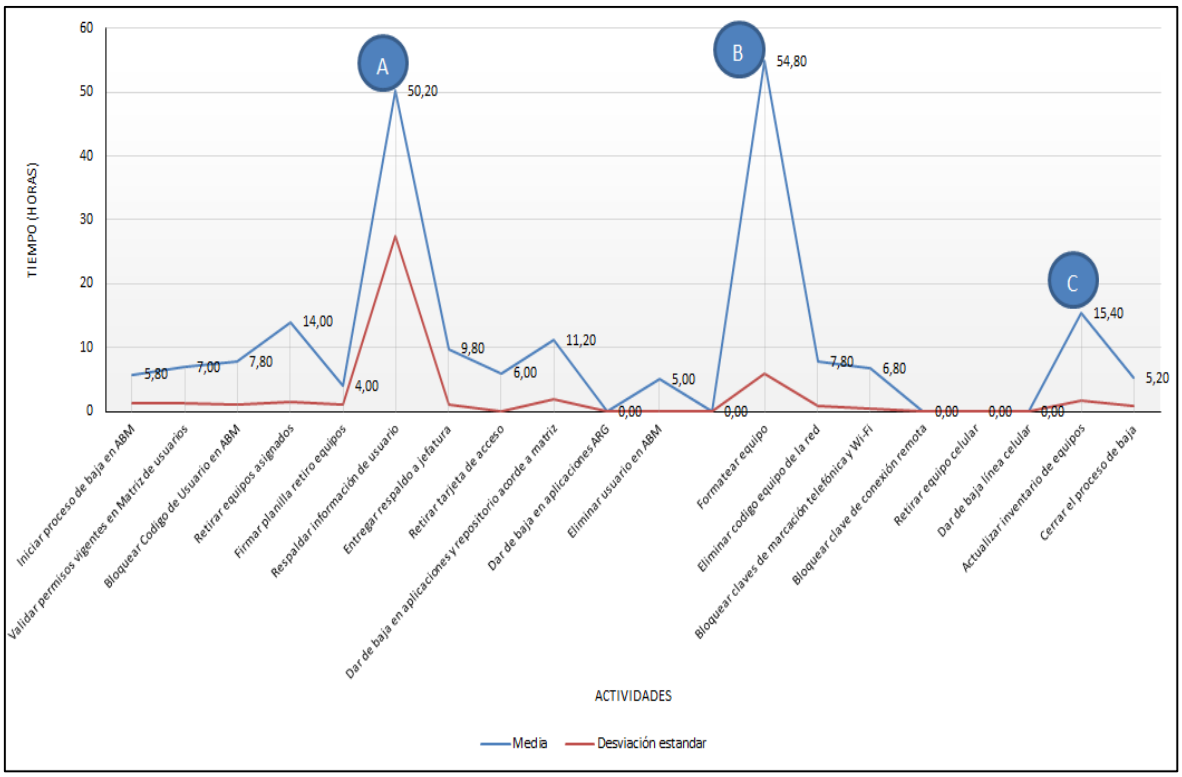


Figura N° 47: Tiempo registrado para culminar el subproceso de “Baja de Usuarios” para usuarios de Tipo 1, medido en horas después de realizar cambios en el Flujograma.
Fuente: Elaboración propia del Investigador.

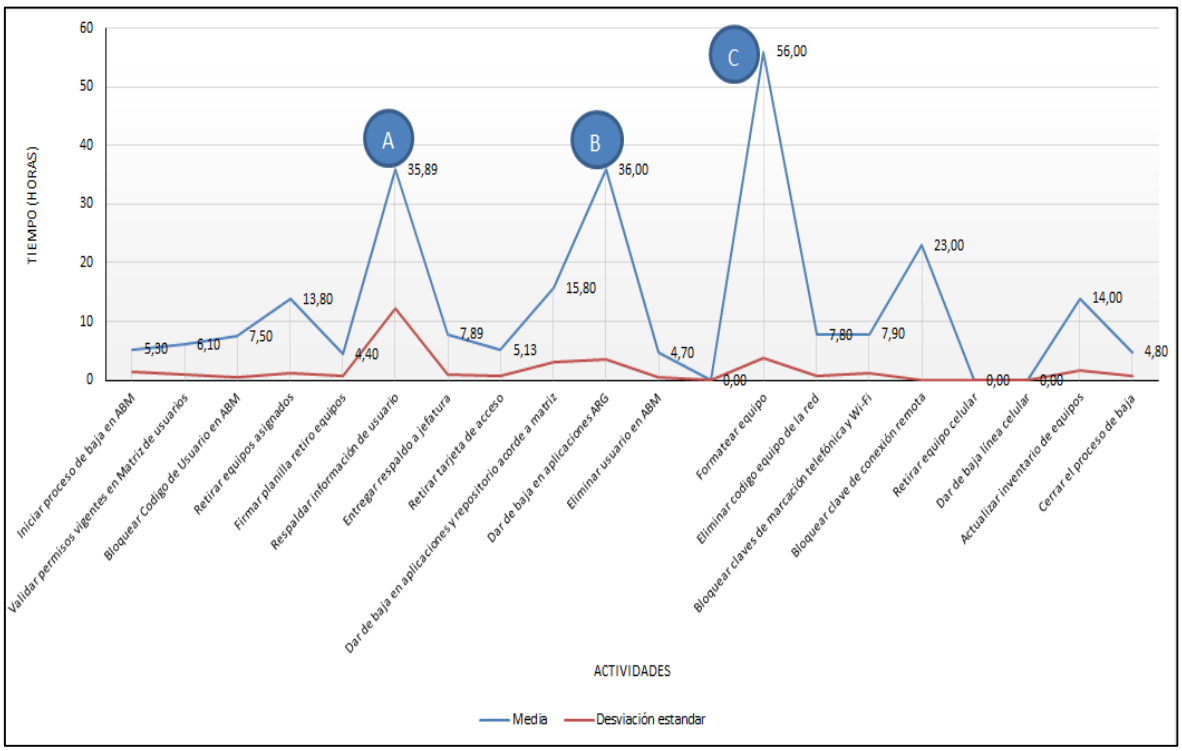


Figura N° 48: Tiempo registrado para culminar el subproceso de “Baja de Usuarios” para usuarios de Tipo 2, medido en horas después de realizar cambios en el Flujograma.

Fuente: Elaboración propia del Investigador.

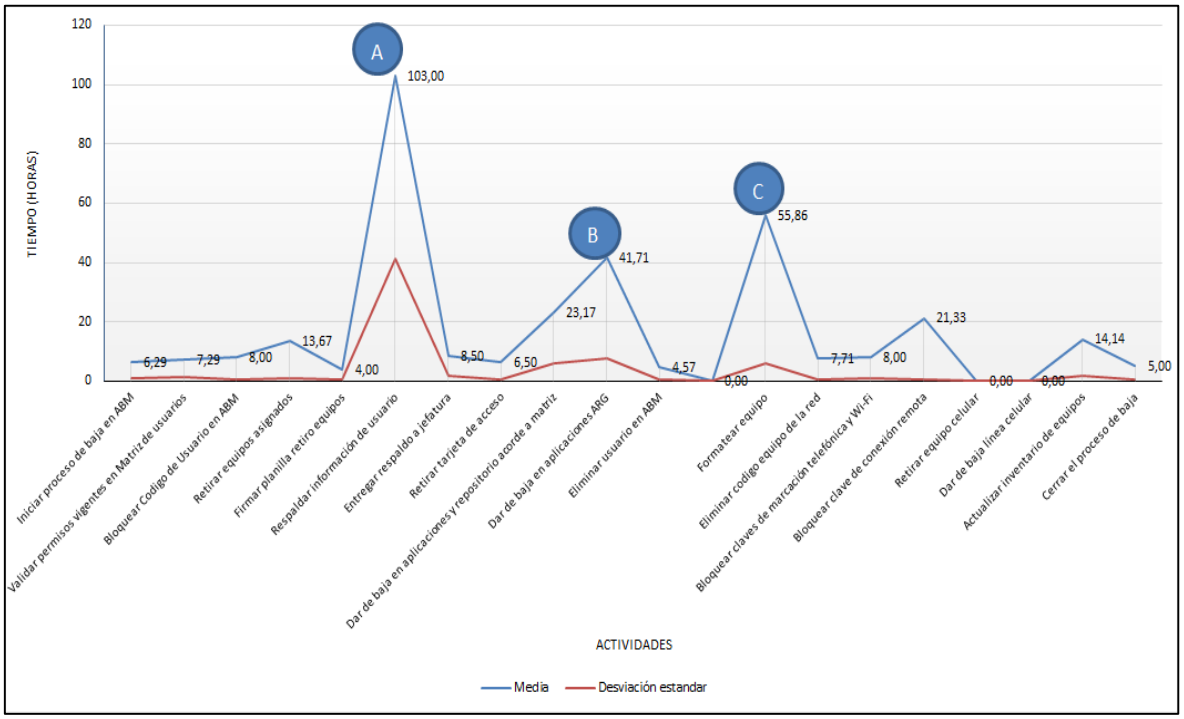


Figura N° 49: Tiempo registrado para culminar el subproceso de "Baja de Usuarios" para usuarios de Tipo 3, medido en horas después de realizar cambios en el Flujograma.
Fuente: Elaboración propia del Investigador.

En las Figuras N°47, N° 48 y N° 49 se resaltan las actividades de mayor duración para cada tipo de usuario y su porcentaje de ejecución en tiempo respecto a todo el subproceso de "Baja de Usuarios", las cuales se detallan en la Tabla N° 64:

Tabla N° 64:
Identificación de actividades de mayor duración para cada tipo de usuario después de aplicar cambios en el flujograma del Subproceso de "Baja de Usuarios".

Tipo	Identificador	Actividad	% del tiempo dentro del subproceso de Baja de Usuarios
Tipo 1	A	Respaldar información de usuario	24,36%
	B	Formatear equipo	26,60%
	C	Actualizar inventario de equipos	7,47%
Tipo 2	A	Respaldar información de usuario	15,50%
	B	Dar de baja aplicaciones ARG	6,91%
	C	Formatear equipo	26,88%
Tipo 3	A	Respaldar información de usuario	29,23%
	B	Dar de baja aplicaciones ARG	13,81%
	C	Formatear equipo	18,49%

Fuente: Elaboración propia de Investigador.

Por último, se puede validar también la dispersión de los datos en base al cálculo del Coeficiente de Variación para cada Tipo de Usuario (Ver Figura N° 50).

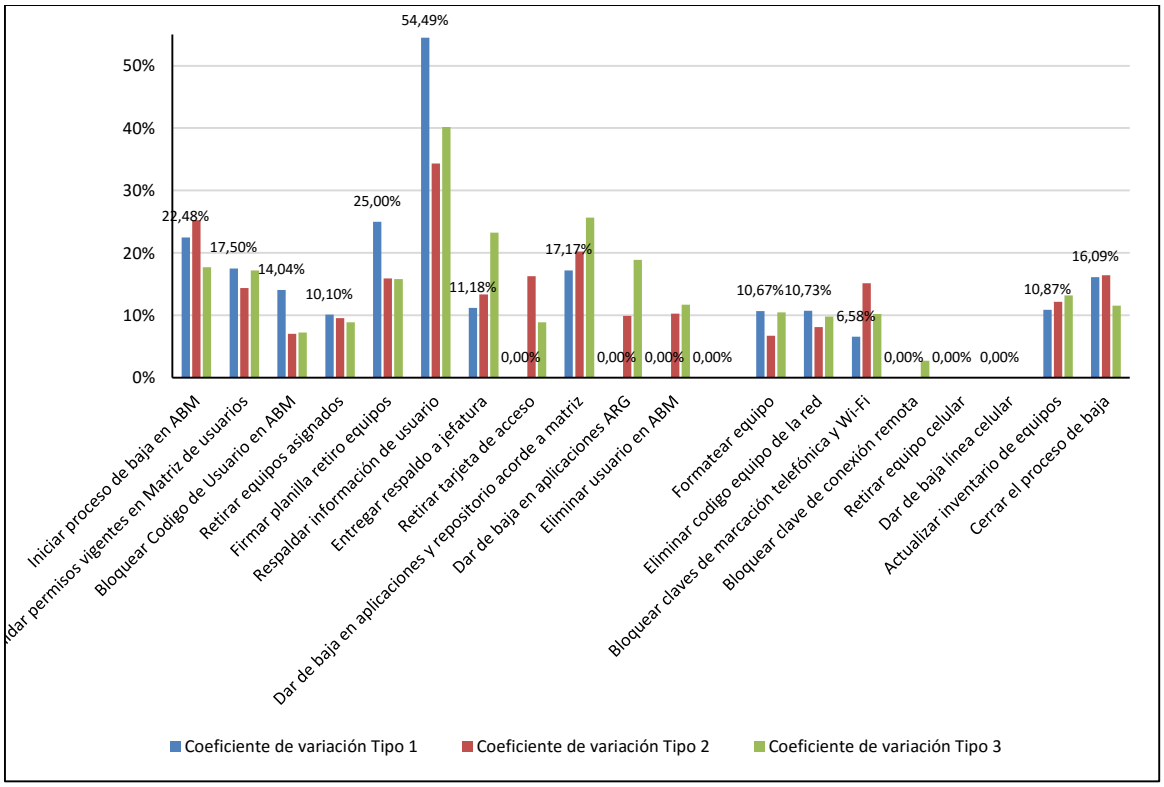


Figura N° 50: Coeficiente de variación de los datos para los tres tipos de usuario después de aplicar cambios en el Flujograma del Subproceso de Baja de Usuarios.
Fuente: Elaboración propia del Investigador.

Partiendo de los valores presentados en las Tablas N° 63 y N° 64, se realiza la comparativa de las mismas, considerando las actividades cuyo tiempo de ejecución representa el mayor porcentaje dentro del subproceso de baja, y esta se presenta en la Tabla N° 65.

Tabla N° 65:

Comparación de actividades de mayor duración para cada tipo de usuario antes y después de aplicar cambios en el flujograma del subproceso "Baja de Usuarios".

Tipo	Identificador	Actividad	Antes Cambio Flujo: % del tiempo dentro del subproceso de Baja de Usuarios	Después Cambio Flujo: % del tiempo dentro del subproceso de Baja de Usuarios
Tipo 1	A	Respaldar información de usuario	16,28%	24,36%
	B	Eliminar manualmente grupos y repositorios	21,21%	5,43%
	C	Formatear equipo	19,99%	26,60%
Tipo 2	A	Respaldar información de usuario	16,06%	15,50%
	B	Dar de baja aplicaciones ARG	22,29%	6,91%
	C	Eliminar manualmente grupos y repositorios	22,00%	7,58%
Tipo 3	A	Respaldar información de usuario	17,00%	29,23%
	B	Dar de baja aplicaciones ARG	19,74%	13,81%
	C	Eliminar manualmente grupos y repositorios	30,11%	6,57%

Fuente: Elaboración propia de Investigador.

Considerando los resultados de la Tabla N° 62, se puede observar que la actividad "Eliminar manualmente grupos y repositorios" por su porcentaje en el tiempo de ejecución, fue identificada como una de las tres actividades que mayor tiempo demandaba para completar el subproceso de "Baja de Usuarios" antes de su cambio en el flujograma; al ser reemplazada con la actividad "Dar de baja en aplicaciones y repositorio acorde a matriz", este porcentaje disminuye en un 74,40% para usuarios de Tipo 1; 65,55% para usuarios del tipo 2 y 78,18% para usuarios de Tipo 3. Esto genera que el tiempo total de ejecución del subproceso se reduzca y por ende que el porcentaje de demanda de tiempo por actividad varíe y se redistribuya.

Así también existen actividades cuyo porcentaje de demanda de tiempo sobresale respecto al resto (aunque su tiempo medido no se haya incrementado), pero esto se debe además de a la reducción en el tiempo de ejecución completa del subproceso, a que estas

actividades son tareas manuales como lo es “Respaldar información del usuario y Formatear equipo” y de las cuales su tiempo no se enfocó para reducción.

3.3.6 Paso 6: Presentar y evaluar los resultados.

Una vez ejecutados los cálculos sobre la matriz de registros de tiempos, se puede resumir los resultados obtenidos en la Tabla N° 66 para el subproceso de “Alta de Usuarios”:

Tabla N° 66:
Presentación de resultados y variación en los indicadores del subproceso de “Alta de Usuario”.

Tipo Usuario	Indicadores	Sin cambios en el flujograma	Ejecutados cambios en el flujograma	% de Reducción
Tipo 1	Media (Ejecutar alta - horas)	20,39	5,92	70,99%
	Desviación Estándar	3,07	0,10	96,61%
	Coeficiente de Variación	15,07%	1,76%	Aceptable
Tipo 2	Media (Ejecutar alta - horas)	22,76	5,89	74,14%
	Desviación Estándar	0,64	0,28	55,64%
	Coeficiente de Variación	2,80%	4,80%	Aceptable
Tipo 3	Media (Ejecutar alta - horas)	50,95	16,37	67,87%
	Desviación Estándar	17,97	2,36	86,88%
	Coeficiente de Variación	35,27%	14,41%	Aceptable

Nota: El Nivel de aceptabilidad del coeficiente de variación hasta un valor de 7% se considera confiable, del 8% al 14% se considera aceptable, del 15% al 20% se considera de precisión regular y sobre el 20% no se considera confiable.
Fuente: Elaboración propia de Investigador.

De similar forma, una vez ejecutados los cálculos sobre la matriz de registros de tiempos, se puede resumir los resultados obtenidos en la Tabla N° 67 para el subproceso de “Baja de Usuarios”:

Tabla N° 67:
Presentación de resultados y variación en los indicadores del subproceso de "Baja de Usuario"

Tipo Usuario	Indicadores	Sin cambios en el flujograma	Ejecutados cambios en el flujograma	% de Reducción
Tipo 1	Media (Ejecutar alta - horas)	4,52	3,52	22,26%
	Desviación Estándar	0,89	0,66	26,17%
	Coeficiente de Variación	19,73%	18,74%	Aceptable
Tipo 2	Media (Ejecutar alta - horas)	7,23	3,47	51,97%
	Desviación Estándar	2,04	0,58	71,59%
	Coeficiente de Variación	28,27%	16,72%	Aceptable
Tipo 3	Media (Ejecutar alta - horas)	7,97	5,03	36,88%
	Desviación Estándar	3,44	1,36	60,45%
	Coeficiente de Variación	43,10%	27,01%	Aceptable

Nota: El Nivel de aceptabilidad del coeficiente de variación hasta un valor de 7% se considera confiable, del 8% al 14% se considera aceptable, del 15% al 20% se considera de precisión regular y sobre el 20% no se considera confiable.
Fuente: Elaboración propia de Investigador.

Como se lo puede visualizar en las Tablas N° 66 y Tabla N° 67, existe una reducción en el tiempo para completar los subprocesos de "Alta de Usuarios" y "Baja de Usuarios", la dispersión de los datos se reduce, concluyendo que la modificación en el flujograma partiendo de la implementación de la Matriz de Perfiles, permitió reducir el tiempo de ejecución de los dos subprocesos, para "Alta de Usuarios" en un 71,00% y para "Baja de Usuarios" en un 37,04%.

3.4 Resultados de la Investigación

3.4.1 Cumplimiento de Objetivos de Control y Controles Aplicables.

Una vez completadas las acciones a ejecutar para cumplir los objetivos de control de la Norma ISO 27001:2013, se cubrió con las observaciones identificadas, lo cual permitió cumplir el 100% de los objetivos de control que especifica la Norma y dentro de las cuales figuraban cuarenta y cuatro (44) requisitos aplicables para el proceso de "Alta y Baja de Usuarios".

En la Tabla N° 68 se muestra el porcentaje de cumplimiento que se efectuó desde diciembre del 2016 hasta marzo del 2017 para llegar a cubrir el 100% de los objetivos de control y controles que cita la Norma ISO 27001:2013.

Tabla N° 68:
Porcentaje de cumplimiento de objetivos de control y controles para el proceso de "Alta y Baja de Usuarios"

Período	Número Total de Requisitos Aplicables	Número de Requisitos que Cumple	Número de Requisitos que No Cumple	Número de Requisitos que Cumple Parcialmente	% Cumplimiento
Diciembre 2016	44	15	8	21	65%
Marzo 2017	44	44	0	0	100%

Fuente: Elaboración propia del Investigador.

3.4.2 Reducción de Re-procesos por modificación de permisos de usuario.

En la Tabla N° 69 se muestra el número total de altas de usuario, bajas de usuario y modificación de usuarios dividido en los dos períodos de investigación, donde se puede evidenciar la reducción en el número de re procesos, una vez aplicada la "Matriz de perfiles de usuario" como acción de mejora ejecutada.

Tabla N° 69:
Altas, bajas y modificaciones (reproceso) de usuario para el periodo Enero 2016 Abril 2017.

Período	Número Total de Altas	Número Total de Bajas	Número Total de Modificaciones	# Reproceso / (# Altas + # Bajas)
Enero 2016 - Diciembre 2016	47	58	92	1,07
Enero 2017 – Abril 2017	14	22	8	0,25

Fuente: Elaboración propia del Investigador.

3.4.3 Mejora de Tiempos en la ejecución de cada subproceso.

En la Figura N° 51 se presenta la reducción del tiempo en la ejecución del subproceso de "Alta de Usuarios", el cual demuestra una disminución en la ejecución completa del ciclo del subproceso.

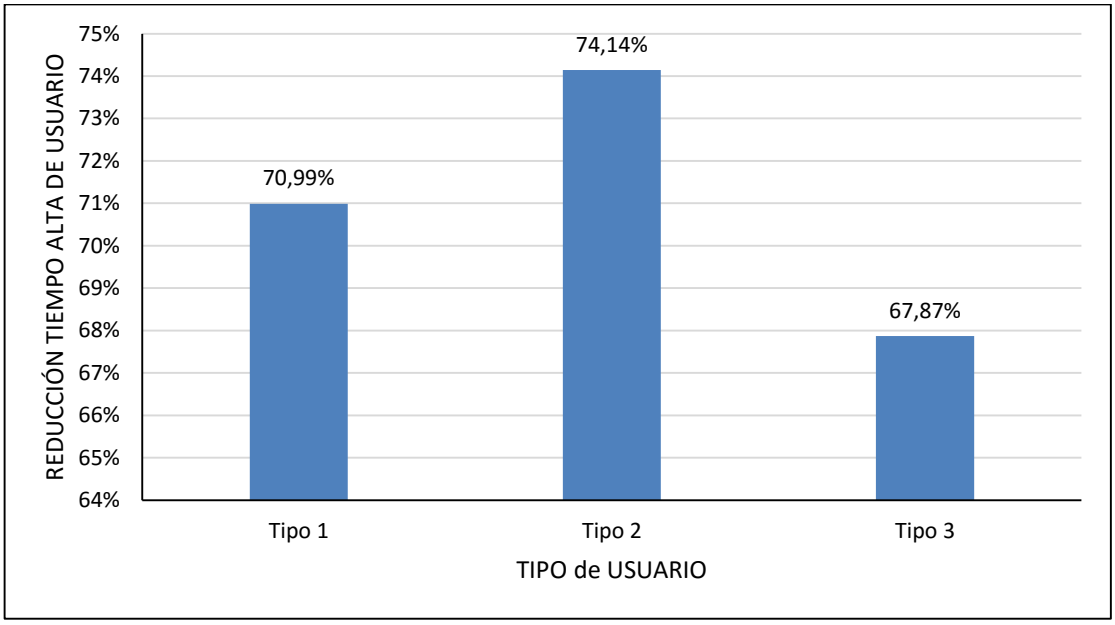


Figura N° 51: Porcentaje de reducción de tiempo en el subproceso de “Alta de Usuarios”.
Fuente: Elaboración propia del Investigador.

En la Figura N° 52 se presenta la reducción del tiempo en la ejecución del subproceso de “Alta de Usuarios”, el cual demuestra una disminución en la ejecución completa del ciclo del subproceso.

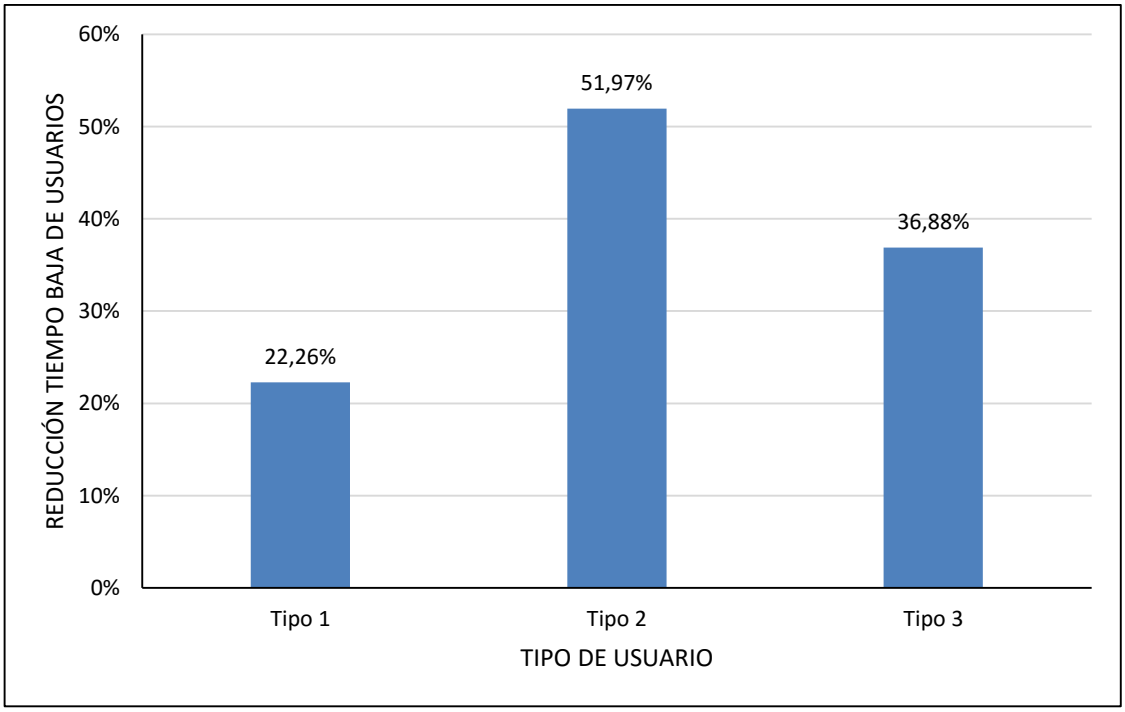


Figura N° 52: Porcentaje de reducción de tiempo en el subproceso de “Baja de Usuarios”.
Fuente: Elaboración propia del Investigador.

CAPÍTULO 4: ANÁLISIS DE RESULTADOS

Partiendo de los resultados de la investigación, se procede a analizar los mismos para validar que se cumplieron los objetivos planteados para el presente estudio, para ello se analiza:

- Cumplimiento de Objetivos de Control y Controles Aplicables respecto a la Norma ISO 27001:2013.
- Reducción de re procesos en la ejecución de los subprocesos de “Alta de Usuarios” y “Baja de Usuarios”.
- Mejora de Tiempos en la ejecución de los subprocesos de “Alta de Usuarios” y “Baja de Usuarios”.

4.1 Cumplimiento de Objetivos de Control y Controles Aplicables respecto a la Norma ISO 27001:2013.

En las Figuras N° 53 y Figura N° 54 se muestra el avance de cumplimiento que se efectuó mensualmente hasta llegar a cubrir el 100% de los objetivos en el mes de marzo del 2017, partiendo de los resultados que presentó el análisis de objetivos de cumplimiento realizado al inicio del presente estudio.

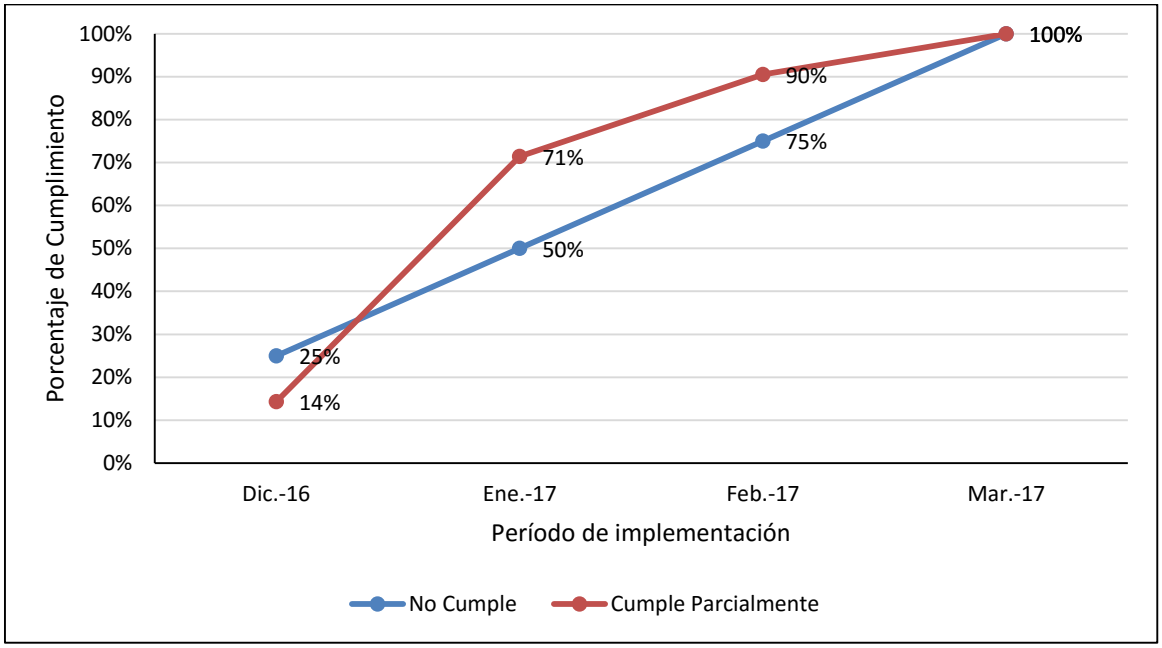


Figura N°53: Porcentaje de cumplimiento de objetivos mensual (Diciembre 2016 – Marzo 2017).
Fuente: Elaboración propia del Investigador.

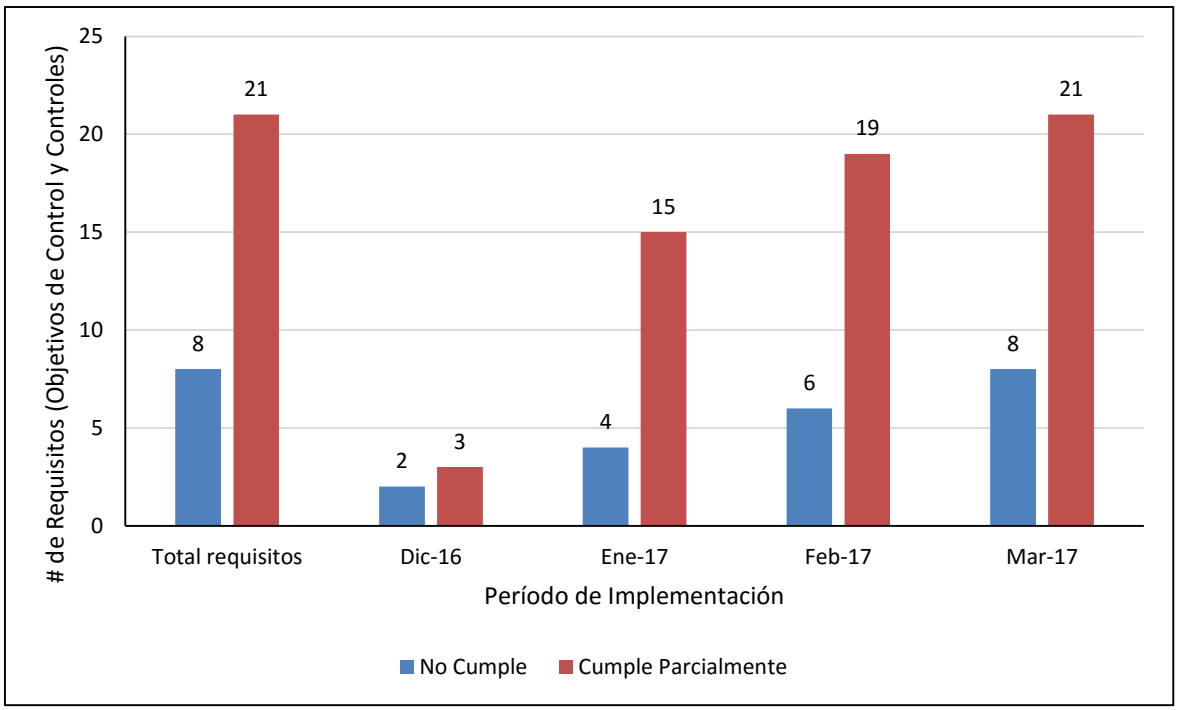


Figura N°54: Avance mensual de cumplimiento de objetivos de Control y Controles de la Norma ISO 27001:2013 (Diciembre 2016 – Marzo 2017).
Fuente: Elaboración propia del Investigador.

4.2 Reducción de Re-procesos en la ejecución de los subprocesos de "Alta de Usuarios" y "Baja de Usuarios".

La Figura N° 55 presenta el número de Altas y Bajas de Usuario ejecutadas para el período "Enero 2016 – Abril 2017" y los re-procesos efectuados en ese período de tiempo por asignación errónea de permisos. Se puede observar la evolución de Alta y Baja de usuarios, una vez aplicados los objetivos de control y controles de la Norma ISO 27001:2013, en el período "Enero 2017 – Abril 2017", mostrando una tendencia de reducción de re procesos.

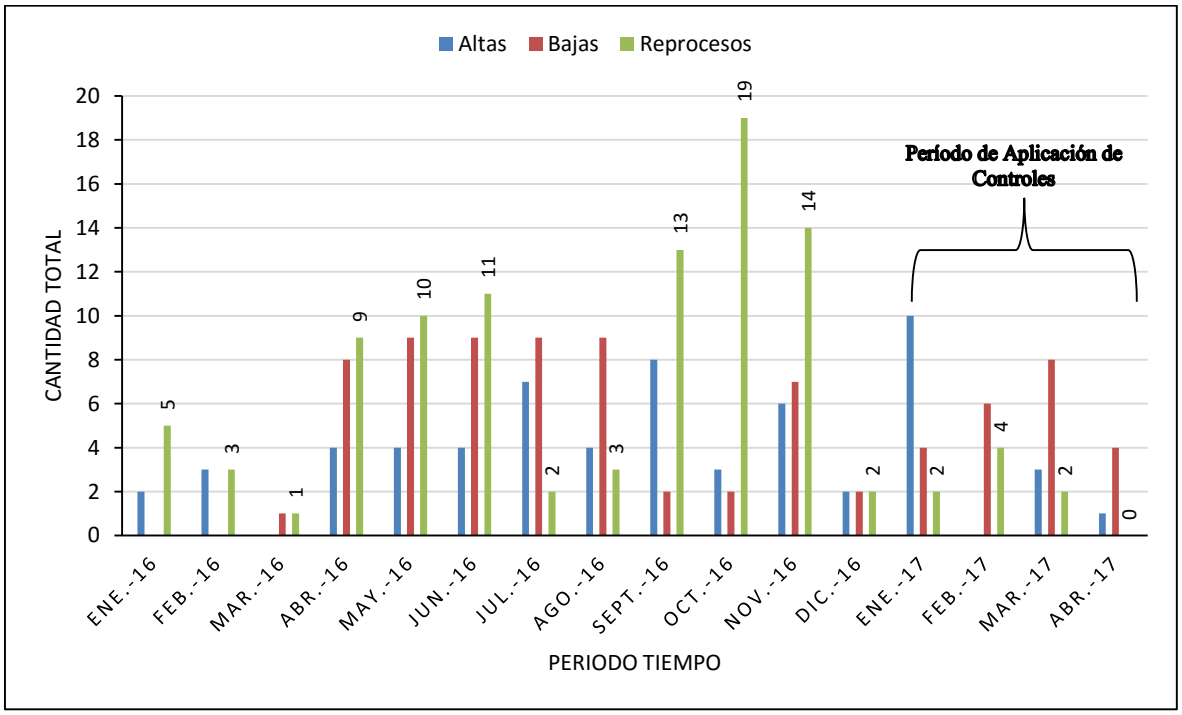


Figura N° 55: Número de Altas, Bajas y Modificación de usuarios para el período Agosto 2016 – Abril 2017.
Fuente: Elaboración propia del Investigador.

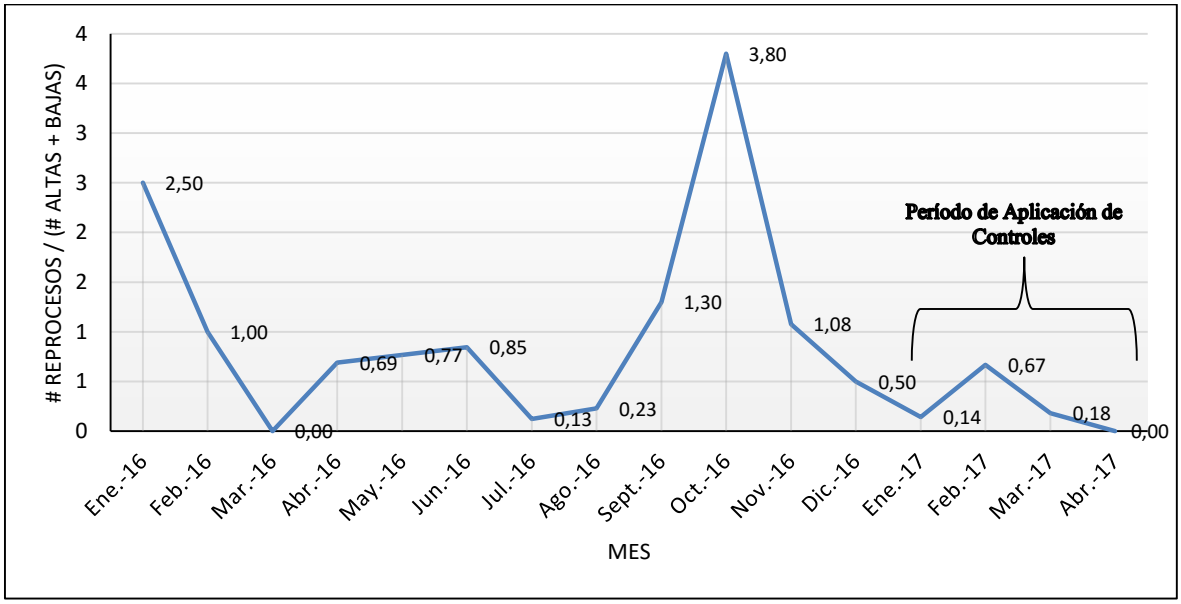


Figura N° 56: Reproceso en permisos de usuario por asignación errónea o permisos adicionales en el período Enero 2016 – Abril 2017.
Fuente: Elaboración propia del Investigador.

La Figura N° 56 muestra la evolución mensual de “Reproceso” frente al número de “Alta de Usuarios” y “Bajas de usuario”. La Media del valor de re procesos del período “Enero 2016 – Diciembre 2016” es de 1,07; mientras que la Media de valor de re procesos del período “Enero 2017 – Abril 2017” es de 0,25. Con la aplicación de los objetivos de control y controles de la Norma ISO 27001:2013 se logró una reducción del 76,84% de re procesos.

En la Tabla N° 70 se presenta el detalle del número de altas de usuario, bajas de usuario por cambio de permisos, asignación de nuevos permisos y modificación de accesos; de los cuales se calcula el costo por hora dedicado ($ 19,50 USD), permitiendo comprobar que existe un reducción de $ 44,14 USD mensuales desde Enero del 2017 y con esta tendencia se tendría un ahorro de $ 497,25 USD para el período Enero 2017 a Diciembre 2017.

Tabla N° 70:

Análisis de re procesos expresado en tiempo y costo para el período Enero 2016 – Abril 2017.

Mes	*# Altas*	*# Bajas para nuevo permiso*	*Tiempo baja (horas)*	*# Asignación nuevos permisos*	*Tiempo permisos (horas)*	*# Modificación Accesos*	*Tiempo accesos (horas)*	*Esfuerzo total en horas por re proceso*	*Esfuerzo total en USD*
Ene-16	2	0	0	0	0	5	2,5	2,5	$ 48,75
Feb-16	3	0	0	0	0	3	1,5	1,5	$ 29,25
Mar-16	0	1	1	1	2	0	0	3	$ 58,50
Abr-16	4	2	2	2	4	7	3,5	9,5	$ 185,25
May-16	4	1	1	1	2	9	4,5	7,5	$ 146,25
Jun-16	4	1	1	1	2	10	5	8	$ 156,00
Jul-16	7	0	0	1	2	1	0,5	2,5	$ 48,75
Ago-16	4	0	0	0	0	3	1,5	1,5	$ 29,25
Sept-16	8	0	0	2	4	11	5,5	9,5	$ 185,25
Oct-16	3	0	0	5	10	14	7	17	$ 331,50
Nov-16	6	0	0	3	6	11	5,5	11,5	$ 224,25
Dic-16	2	0	0	2	4	0	0	4	$ 78,00
Ene-17	10	0	0	1	2	1	0,5	2,5	$ 48,75
Feb-17	0	0	0	4	8	0	0	8	$ 156,00
Mar-17	3	1	1	2	4	0	0	5	$ 97,50
Abr-17	1	2	2	0	0	0	0	2	$ 39,00
Total	**61**	**8**	**8**	**25**	**50**	**75**	**37,5**	**95,5**	**$ 1.862,25**
Promedio mensual total	3,81	0,50		1,56		4,69			$ 116,39
Promedio mensual Ene.2016 - Dic.2016	3,92	0,42		1,50		6,17			$ 126,75
Promedio mensual Ene.2017 - Abr.2017	3,50	0,75		1,75		0,25			$ 85,31

Nota. Esfuerzo total calculado por re procesos y expresado en horas y dólares. Informes de Gestión de Incidentes de Help Desk. (2016). Registros de Alta y Baja de Usuarios. Ecuador: Empresa de Consultoría para la Industria Petrolera.

4.3 Mejora de Tiempos en la ejecución de los subprocesos de "Alta de Usuarios" y "Baja de Usuarios".

La Figura N° 57 presenta la reducción del tiempo (considerando la media y desviación estándar) en la ejecución del subproceso de "Alta de Usuarios", el cual demuestra una disminución en la Media del Tiempo Total del ciclo del subproceso para cada tipo de usuario:

- Tipo 1: 70,99%
- Tipo 2: 74,14%
- Tipo 3: 67,87%

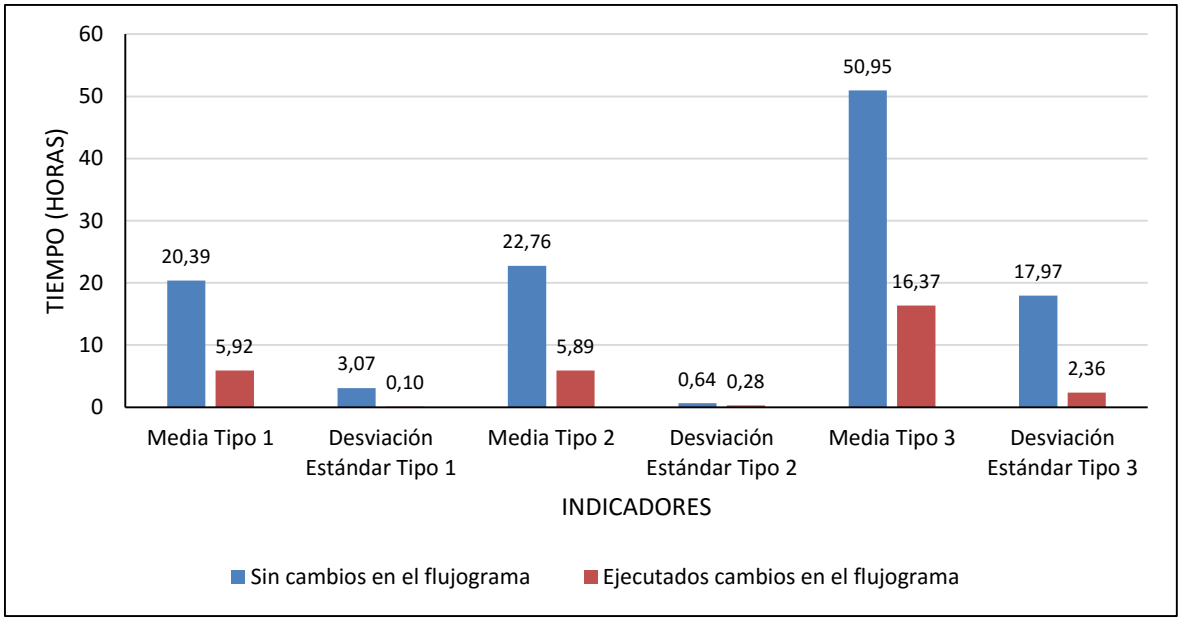


Figura N° 57: Media del tiempo de ejecución del subproceso de "Alta de Usuarios" (Tiempo en horas).
Fuente: Elaboración propia del Investigador.

En resumen, para el subproceso de "Alta de Usuarios" se redujo un 71,00 % del tiempo de ejecución del subproceso.

La Figura N° 58 presenta la reducción del tiempo (considerando la media y desviación estándar) en la ejecución del subprocesos de “Baja de Usuarios”, el cual demuestra una disminución en la Media del Tiempo Total del ciclo del subproceso para cada tipo de usuario:

- Tipo 1: 22,26%
- Tipo 2: 51,97%
- Tipo 3: 36,88%

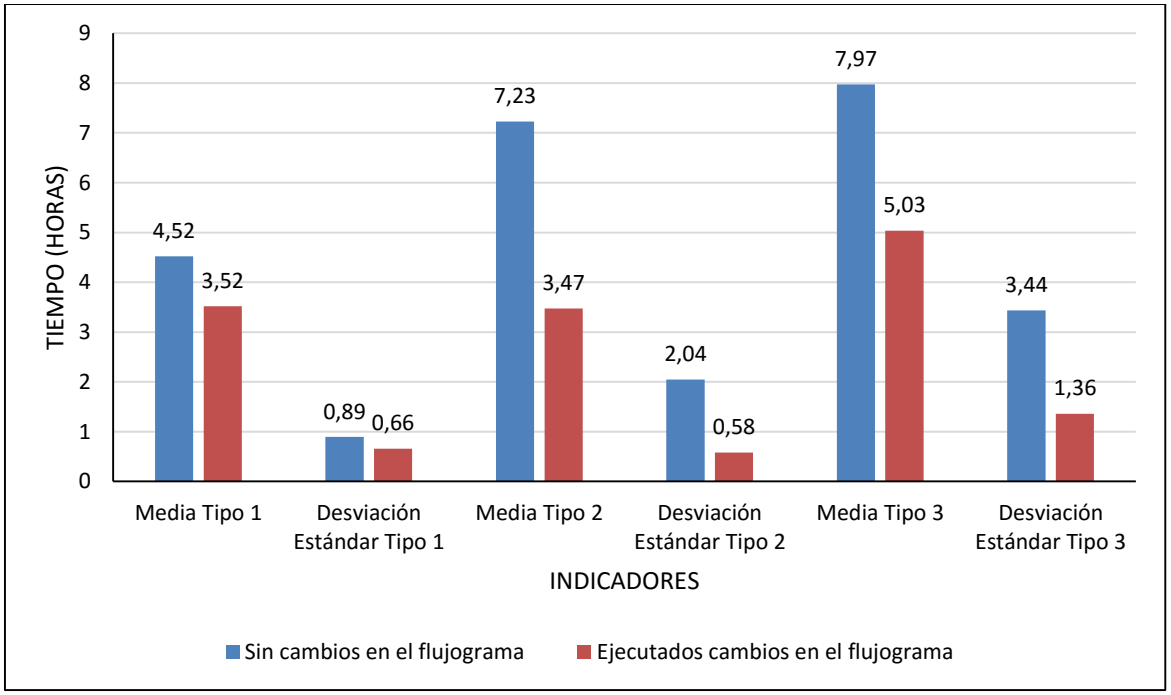


Figura N° 58: Media del tiempo de ejecución del subproceso de “Baja de Usuarios” (Tiempo en horas).
Fuente: Elaboración propia del Investigador.

En resumen, para el subproceso de “Baja de Usuarios” se redujo un 37,04 % del tiempo de ejecución del subproceso.

CAPÍTULO 5: CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES.

La optimización de la Gestión de Seguridad de la Información para el Proceso de "Alta y Baja de Usuarios" permitió reducir el valor promedio de re procesos en un 76,84 % lo cual transformado en USD se convierte en $ 44,14 mensuales, esto mediante la implementación de los requisitos aplicables de la Norma ISO 27001:2013 para una empresa de Consultoría para la Industria Petrolera.

El diagnóstico de la situación actual del proceso de "Alta y Baja de Usuarios", basado en la Norma ISO 27001:2013 permitió identificar cuarenta y cuatro (44) objetivos de control y controles aplicables de los cuales: se cumplía con quince (15) controles, no se cumplía con nueve (9) controles y se cumplía parcialmente con veinte y uno (21) controles, sobre los cuales se aplicaron las acciones de mejora para cubrir estos requisitos aplicables a una empresa de consultoría para la Industria Petrolera.

Optimizar el desempeño del proceso de "Alta y Baja de Usuarios" mediante el desarrollo e implementación de requisitos aplicables de la norma ISO 27001:2013, además de reducir el porcentaje de re procesos en un 76,84%, permitió realizar reducción de tiempos promedio para el subproceso de "Alta de Usuarios" en un 71% y para el subproceso de "Baja de Usuarios" en un 37,04%, mediante el Estudio del Tiempo aplicado a una empresa de consultoría para la Industria Petrolera.

La implementación de objetivos de control y controles respecto a la Norma ISO 27001:2013, permitió encontrar diferencias entre los subprocesos de “Alta de Usuarios” y “Baja de Usuarios” partiendo de los flujogramas corporativos, respecto a la ejecución de estos subprocesos en Ecuador, esto permitió modificar los mismos para optimizarlos acorde a las necesidades y recursos locales de la Empresa de Consultoría para la Industria Petrolera.

Utilizar el método de Medición del Tiempo mediante Registros Históricos, permitió desarrollar herramientas como la Matriz de Registro de Tiempos basada en el Registro de Control de Tiempos que cita este método, sobre la misma se pudo detallar actividades que intervienen en el flujo de los subprocesos, categorizar por tipos de usuario, generar cálculos parciales por cada registro o sección (tipos de usuario); facilitando la observación de los datos y el análisis del tiempo de ciclo para proponer mejoras en las actividades de los dos subprocesos para una empresa de consultoría para la Industria Petrolera

La optimización de re procesos en una empresa de consultoría para la Industria Petrolera aplicando los objetivos de control y controles aplicables de la Norma ISO, permitió identificar las actividades que mayor tiempo dentro del ciclo demandaban, para el subproceso de “Alta de Usuarios” la actividad “Definir usuario modelo” utilizaba un 25,41% del tiempo total del ciclo y para el subproceso de “Baja de Usuarios” la actividad “Eliminar manualmente grupos y repositorios” utilizaba un 24,54% del tiempo total del ciclo.

El conocimiento técnico sobre herramientas (hardware / software), así como dominar el proceso en estudio, ayudó a entender sobre la ejecución y recursos que intervienen dentro del proceso de “Alta y Baja de Usuarios”, permitiendo mediante ello plantear y aplicar cambios que aportaron a optimizar la reducción de re procesos en un 76,84% y reducir el

tiempo de ejecución de los dos subprocesos a partir de la aplicación de la Matriz de Perfiles de Usuario.

5.2 RECOMENDACIONES.

Se recomienda aplicar el diagnóstico de situación actual a los procesos colaterales con los que interactúa el proceso de “Alta y Baja de Usuarios”, lo que permitiría optimizar estos procesos (Proceso de Respaldo de Información y Proceso de Recuperación y Restauración de Información), que si bien en este estudio se citan como requisitos aplicables, profundizar en su estudio permitiría definir si los procesos se efectúan de manera óptima o se pueden aplicar mejoras que aporten a reducir tiempos de ejecución en su ejecución.

Mantener el nivel de control implementado en el proceso de “Alta y Baja de Usuarios” y evaluarlo periódicamente es recomendable, con el fin de validar que los cambios aplicados continúan aportando a la optimización del proceso y conseguir la estabilidad del proceso respecto a tiempo de ejecución.

Programar auditorías externas al proceso de “Alta y Baja de Usuario” para continuar validando la eficacia de los controles aplicados.

Ampliar el ajuste de Normativas Corporativas a los requisitos locales en el resto de procesos que intervienen en la gestión de IT, ya que los mismos no podrían ser aplicables en su totalidad o de forma correcta, esto debido a la diferencia entre matriz y una filial respecto a recursos humanos, presupuesto, normativas legales, entre otros.

Para realizar un Estudio de Tiempo se recomienda, iniciar con la validación de la data a utilizar para asegurar que el relevamiento de información cuente con datos confiables y actualizados; evitando que su registro demande mayor esfuerzo para el investigador que el objetivo principal en estudio.

BIBLIOGRAFÍA

Asociación de la Industria de las Telecomunicaciones. (Abril de 2013). *ANSI/TIA-942-A 1*. Arlington, Estados Unidos: Asociación de la Industria de las Telecomunicaciones.

Automatas ORG. (2 de Marzo de 2006). *SISTEMAS SCADA.* Obtenido de SISTEMAS SCADA: http://automatas.org/redes/scadas.htm

Automatización e Integración Tecnológica Argentina - AIT. (22 de Julio de 2015). *Sistemas SCADA y su importancia.* Obtenido de Sistemas SCADA y su importancia: https://www.ait.com.ar/blog/sistemas-scada-importancia

Check Point Software Technologies Ltd. (20 de Diciembre de 2016). *Creación de una política de seguridad de Firewall fuerte*. Obtenido de Creación de una política de seguridad de Firewall fuerte: https://sc1.checkpoint.com/documents/R76/CP_R76_Firewall_WebAdmin/92703.htm

Cisco Systems. (2004). Topology Diagram with Both Network Devices and End Systems. En C. Systems, *Cisco Internetwork Troublshooting* (pág. 40). Silicon Valley: Cisco Systems Inc.

Cisco Systems. (20 de Diciembre de 2016). *Tipos de Autenticación para Dispositivos Inalámbricos.* Obtenido de Tipos de Autenticación para Dispositivos Inalámbricos:

http://www.cisco.com/c/en/us/td/docs/routers/access/wireless/software/guide/SecurityAuthenticationTypes.html#wp1002608

Criollo, R. G. (2005). *Estudio del Trabajo - Ingeniería de Métodos y Medición del Trabajo.* México: McGraw-Hill Interamericana.

Departamento de Defensa de los Estados Unidos. (20 de Diciembre de 2016). *Servicio de Defensa - Manual de Operaciones del Programa Nacional de Seguridad Industrial*. Obtenido de Marcas Equivalente Extranjeras: http://web.archive.org/web/20061209205925/http://www.dss.mil/isec/appendixb.htm

EDIWORLD. (2016). Seguridad, el desafío informático del 2016. *COMPUTERWORLD ECUADOR*, 36.

Empresa de Consultoría para la Industria Petrolera. (4 de Mayo de 2012). Manual de Procedimiento para el Alta, Baja y Modificación de Usuarios. Buenos Aires, Buenos Aires, Argentina.

Empresa de Consultoría para la Industria Petrolera. (2016). *Informes de Gestión de Incidentes de Help Desk – Registros de Alta y Baja de Usuarios.* Quito: Empresa de Consultoría para la Industria Petrolera.

Empresa de Consultoría para la Industria Petrolera. (2016). *Informes de Gestión de Incidentes de Help Desk – Registros de modificaciones a usuarios.* Quito: Empresa de Consultoría para la Industria Petrolera.

Empresa de Consultoría para la Industria Petrolera. (20 de Noviembre de 2016). *Intranet Empresa de Consultoría para la Industria Petrolera*. Obtenido de Organigrama Empresarial: htttp://www.intra.ot

Empresa de Consultoría para la Industria Petrolera. (5 de Octubre de 2016). Manual para Automatización y Monitoreo de Estaciones. Quito, Pichincha, Ecuador.

Empresa de Consultoría para la Industria Petrolera. (20 de Julio de 2016). Protección de Información. Buenos Aires, Buenos Aires, Argentina. Obtenido de Protección de Información: http://www.intra.ot/

Empresa de Consultoría para la Industria Petrolera. (28 de Noviembre de 2016). *Sistema Normativo.* Obtenido de Procedimientos para el Área de Sistemas: http://intra.ot/SistemaNormativo/

Ingeniería Dric - IDRIC. (20 de Diciembre de 2016). *Gestión de Usuarios en el Active Directory.* Obtenido de Gestión de Usuarios en el Active Directory: http://manageengine.mx/active-directory-manager/gestion-usuarios-active-directory.html

ITpreneurs. (2014). Biblioteca de Infraestructura de Tecnologías de Información. En ITpreneurs, *Manual de inducción para certificación en Fundamentos de ITIL V3* (pág. 43). Ecuador: New Horizons.

Level 3. (6 de Octubre de 2016). 8° Foro Level 3. *Tecnología y Negocios XAAS*. Quito, Pichincha, Ecuador: Level 3.

Microsoft. (20 de Diciembre de 2016). *Windows Server- Administración de usuarios.* Obtenido de Windows Server- Administración de usuarios: https://technet.microsoft.com/es-es/library/dd861336(v=ws.11).aspx

Ministerio de Justicia, Derechos Humanos y Cultos del Ecuador. (2014). *Código Orgánico Integral Penal.* Quito: Gráficas Ayerve C. A.

Murray, S. R., & Larry, S. J. (2009). *Estadística.* México D.F.: McGraw-Hill.

Organización Internacional de Normalización. (2014). ISO/IEC 27000. En ISO, *Tecnología de la Información - Técnicas de Seguridad - Administración de Sistemas de Seguridad de la Información - Información General y Vocabulario* (pág. v). Suiza: Organización Internacional de Normalización.

Organización Internacional de Normalización. (2014). ISO/IEC 27001:2013. En O. I. Normalización, *Tecnología de la Información – Técnicas de Seguridad – Sistema de Administración de Seguridad de la Información – Requisitos* (pág. v). Suiza: Organización Internacional de Normalización.

Organización Internacional de Normalización. (2015). *Norma Internacional ISO 9001:2015*. Ginebra: Organización Internacional de Normalización - Grupo ISO/TC 176.

PGP Corporation. (6 de Octubre de 2016). Tecnología y Negocios XAAS - Usabilidad versus Seguridad. *Usabilidad versus Seguridad*. Quito, Pichincha, Ecuador: Level 3.

Rockwell Automation. (20 de Diciembre de 2016). *Terminales gráficos PanelView 5500*. Obtenido de Terminales gráficos PanelView 5500: http://literature.rockwellautomation.com/3F4E7ADC-DE1D-4E01-B178-ED4ED7F1EED8/FinalDownload/DownloadId-E1CCEF8005F0CAE0BACBD600BB305403/3F4E7ADC-DE1D-4E01-B178-ED4ED7F1EED8/idc/groups/literature/documents/pp/2715-pp001_-en-p.pdf

ANEXOS

ANEXO 1: ISO 27001: 2013 – Objetivos de Control y Controles.

A.5	**Políticas de Seguridad de la Información**	
A.5.1	**Gestión de la dirección para seguridad de la información**	
Objetivo:	Proporcionar gestión de dirección y apoyo para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones pertinentes	
A.5.1.1	Políticas de Seguridad de la Información	***Control***
		Grupo de políticas de seguridad de la información definidas, aprobadas por la dirección, publicadas y comunicadas a todos los empleados y terceras partes
A.5.1.2	Revisión de Políticas de Seguridad de la Información	***Control***
		Las políticas de seguridad de la información se revisarán en intervalos previstos o si se producen cambios significativos para garantizar su idoneidad, suficiencia y efectividad
A.6	**Organización de Seguridad de la información**	
A.6.1	**Organización Interna**	
Objetivo:	Establecer un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización	
A.6.1.1	Roles y responsabilidades de Seguridad de la información	***Control***
		Todas las responsabilidades de seguridad de la información serán definidas y asignadas
A.6.1.2	Discriminación de obligaciones	***Control***
		Las funciones en conflicto y las áreas de responsabilidad deben ser segregados para reducir las oportunidades de modificación no autorizada o no intencional o mal uso de los activos de la organización
A.6.1.3	Contacto con autoridades	***Control***
		Se mantendrán contactos apropiados con las autoridades pertinentes
A.6.1.4	Contacto con grupos especiales de interés	***Control***
		Se mantendrán contactos apropiados con grupos de interés especial u otros foros especializados de seguridad y asociaciones profesionales.
A.6.1.5	Seguridad de la información en Administración de Proyectos	***Control***
		La seguridad de la información se abordará en la gestión del proyecto, independientemente del tipo de proyecto
A.6.2	**Dispositivos móviles y teletrabajo**	
Objetivo:	Asegurar la seguridad de teletrabajo y uso de dispositivos móviles	
A.6.2.1	Política para dispositivos móviles	***Control***
		Se adoptará una política y medidas de seguridad de apoyo para gestionar el riesgo introducido por el uso de dispositivos móviles

A.6.2.2	Teletrabajo	***Control***
		Se aplicará una política y medidas de seguridad de apoyo para proteger la información accesible, procesada o almacenada en los sitios de teletrabajo
A.7	**Seguridad de los recursos humanos**	
A.7.1	**Antes del empleo**	
Objetivo:	Asegurar que los empleados y los contratistas entiendan sus responsabilidades y sean adecuados para los roles para los cuales son considerados	
A.7.1.1	Proyección	***Control***
		Los controles de verificación de antecedentes de todos los candidatos para el empleo se llevarán a cabo de conformidad con las leyes, reglamentos y ética pertinentes y serán proporcionales a los requerimientos de la empresa, la clasificación de la información a ser ingresada y los riesgos percibidos
A.7.1.2	Términos y condiciones de empleo	***Control***
		Los acuerdos contractuales con los empleados y contratistas deberán establecer sus responsabilidades y la de la organización en materia de seguridad de la información
A.7.2	**Durante el empleo**	
Objetivo:	Asegurar que los empleados y contratistas conozcan y cumplan sus responsabilidades de seguridad de la información	
A.7.2.1	Administración de responsabilidades	***Control***
		La administración requerirá que todos los empleados y contratistas apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización
A.7.2.2	Sensibilización, educación y formación en materia de seguridad de la información	***Control***
		Todos los empleados de la organización y, en su caso, los contratistas recibirán una educación y capacitación apropiadas sobre la concienciación y actualizaciones regulares en las políticas y procedimientos de la organización, según sea relevante para su función de trabajo
A.7.2.3	Procesos disciplinarios	***Control***
		Habrá un proceso disciplinario formal y de comunicación para tomar acciones contra los empleados que han cometido una violación de la seguridad de la información
A.7.3	**Terminación y cambio de empleo**	
Objetivo:	Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo	
A.7.3.1		***Control***

	Terminación o cambio de responsabilidades laborales	Las responsabilidades y deberes de seguridad de la información que permanezcan vigentes después de la terminación o cambio de empleo serán definidos, comunicados al empleado o contratista y puestos en vigor
A.8	**Gestión de activos**	
A.8.1	**Responsabilidad de los activos**	
Objetivo:	Identificar los activos de la organización y definir las responsabilidades de protección apropiadas	
A.8.1.1	Inventario de activos	***Control***
		Información asociada a los activos deberán ser identificada, elaborada y mantenida en un inventario
A.8.1.2	Propiedad de activos	***Control***
		Los activos serán registrados y mantendrán en el inventario
A.8.1.3	Uso aceptable de activos	***Control***
		Las reglas para el uso aceptable de la información y de los activos asociados con las instalaciones de procesamiento de información e información deben ser identificadas, documentadas e implementadas
A.8.1.4	Regreso de activos	***Control***
		Todos los empleados y usuarios de partes externas devolverán todos los activos de la organización en su poder al finalizar su empleo, contrato o acuerdo
A.8.2	**Clasificación de la Información**	
Objetivo:	Asegurar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organización	
A.8.2.1	Clasificación de la información	***Control***
		La información se clasificará en términos de requisitos legales, valor, criticidad y sensibilidad a la divulgación o modificación no autorizada
A.8.2.2	Etiquetado de información	***Control***
		Se elaborará y aplicará un conjunto adecuado de procedimientos para el etiquetado de la información de conformidad con el esquema de clasificación de información adoptado por la organización
A.8.2.3	Manejo de activos	***Control***
		Los procedimientos para el manejo de los activos se desarrollarán e implementarán de acuerdo con el esquema de clasificación de información adoptado por la organización
A.8.3	**Manejo de Medios**	
Objetivo:	Para evitar la divulgación, modificación, eliminación o destrucción no autorizadas de la información almacenada en los medios	
A.8.3.1	Gestión de medios extraíbles	***Control***

		Se aplicarán procedimientos para la gestión de medios extraíbles de conformidad con el esquema de clasificación adoptado por la organización
A.8.3.2	Eliminación de medios	***Control***
		Los medios deben ser eliminados de manera segura cuando ya no se requiera, usando procedimientos formales
A.8.3.3	Transferencia de medios físicos	***Control***
		Los medios que contengan información deberán estar protegidos contra el acceso no autorizado, el mal uso o la corrupción durante el transporte
A.9	**Control de Acceso**	
A.9.1	**Requerimientos empresariales de control de acceso**	
Objetivo:	Limitar el acceso a la información e instalaciones de procesamiento de la información	
A.9.1.1	Política de Control de Acceso	***Control***
		Se establecerá, documentará y revisará una política de control de acceso basada en los requisitos de seguridad empresarial y de información
A.9.1.2	Acceso a redes y servicios de redes	***Control***
		Los usuarios sólo tendrán acceso a la red y a los servicios de red que hayan sido específicamente autorizados a utilizar
A.9.2	**Gestión de acceso de los usuarios**	
Objetivo:	Garantizar el acceso de los usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios	
A.9.2.1	Registro y cancelación de registro del usuario	***Control***
		Se llevará a cabo un proceso formal de registro y cancelación de registro de usuarios para habilitar la asignación de derechos de acceso
A.9.2.2	Provisión de acceso de usuario	***Control***
		Proceso formal de provisión de acceso de usuario será implementado para asignar o revocar derechos de acceso para todo tipo de usuario a todos los sistemas y servicios
A.9.2.3	Gestión de derechos de acceso privilegiados	***Control***
		La asignación y el uso de los derechos de acceso privilegiados serán restringidos y controlados
A.9.2.4	Gestión de la información de autenticación secreta de los usuarios	***Control***
		La asignación de información secreta de autenticación se controlará mediante un proceso de gestión formal
A.9.2.5	Revisión de los derechos de acceso de los usuarios	***Control***
		Los propietarios de activos deberán revisar los derechos de acceso de los usuarios a intervalos regulares
A.9.2.6		***Control***

	Eliminación o ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y usuarios de partes externas a las instalaciones de procesamiento de información e información se eliminarán al finalizar su empleo, contrato o acuerdo, o ajustarse al cambiar
A.9.3	**Responsabilidades del usuario**	
Objetivo:	Responsabilizar a los usuarios por la protección de su información de autenticación	
A.9.3.1	Uso de la información secreta de autenticación	***Control***
		El usuario deberá seguir las prácticas de la organización en el uso de la información de autenticación secreta
A.9.4	**Control de acceso a sistemas y aplicaciones**	
Objetivo:	Prevenir el acceso no autorizado a sistemas y aplicaciones	
A.9.4.1	Restricción de acceso a la información	***Control***
		El acceso a la información y las funciones del sistema de aplicación se restringirán de conformidad con la política de control de acceso
A.9.4.2	Procedimientos de conexión segura	***Control***
		Cuando así lo exija la política de control de acceso, el acceso a sistemas y aplicaciones se controlará mediante un procedimiento seguro de conexión
A.9.4.3	Sistema de gestión de contraseñas	***Control***
		Los sistemas de gestión de contraseñas deben ser interactivos y garantizar contraseñas de calidad
A.9.4.4	Uso de programas de utilidad privilegiada	***Control***
		El uso de programas de utilidad que podrían ser capaces de anular los controles del sistema y aplicación debe ser restringido y controlado estrictamente
A.9.4.5	Control de acceso al código fuente del programa	***Control***
		Acceso al código fuente del programa debe ser restringido
A.10	**Criptografía**	
A.10.1	**Controles Criptográficos**	
Objetivo:	Asegurar un uso adecuado y efectivo de la criptografía para proteger la confidencialidad, autenticidad e integridad de la información	
A.10.1.1	Política sobre el uso de controles criptográficos	***Control***
		Se elaborará y aplicará una política sobre el uso de los controles criptográficos para la protección de la información
A.10.1.2	Gestión de claves	***Control***
		Se desarrollará y aplicará una política sobre el uso, la protección y la duración de las claves criptográficas durante todo su ciclo de vida
A.11	**Seguridad física y ambiental**	
A.11.1	**Áreas seguras**	

Objetivo:	Evitar accesos físicos no autorizados, daños e interferencias a las instalaciones de procesamiento de información e información de la organización	
A.11.1.1	Seguridad perimetral física	***Control***
		Se definirán perímetros de seguridad y utilizarán para proteger las áreas que contengan información sensible o crítica e instalaciones de procesamiento de información
A.11.1.2	Controles físicos de entrada	***Control***
		Las zonas seguras deben estar protegidas por controles de entrada apropiados para garantizar que sólo el personal autorizado tenga acceso
A.11.1.3	Asegurar oficinas, cuartos e instalaciones	***Control***
		Seguridad física para oficinas, cuartos y facilidades deben ser diseñadas y aplicadas
A.11.1.4	Protección contra las amenazas externas y ambientales	***Control***
		Protección física contra desastres naturales, ataques maliciosos o accidentes deben ser diseñados y aplicados
A.11.1.5	Trabajo en áreas seguras	***Control***
		Procedimientos para trabajar en áreas seguras debe ser diseñado y aplicado
A.11.1.6	Zonas de entrega y carga	***Control***
		Los puntos de acceso, tales como las áreas de entrega / carga y otros puntos en los que personas no autorizadas puedan entrar en las instalaciones, serán controlados y, de ser posible, aislados de las instalaciones de procesamiento de información para evitar el acceso no autorizado
A.11.2	**Equipo**	
Objetivo:	Evitar pérdidas, daños, robo o compromiso de los activos e interrupción de las operaciones de la organización	
A.11.2.1	Ubicación de equipos y protección	***Control***
		Los equipos deberán estar situados y protegidos para reducir el riesgo de amenazas ambientales y las oportunidades de acceso no autorizado
A.11.2.2	Utilidades de apoyo	***Control***
		El equipo debe estar protegido contra fallas de energía y otras interrupciones causadas por fallas en los servicios de apoyo
A.11.2.3	Seguridad de cableado	***Control***
		Los cables de energía y telecomunicaciones que transporten datos o servicios de información de apoyo deberán estar protegidos contra intercepciones, interferencias o daños
A.11.2.4	Mantenimiento de equipo	***Control***
		El equipo debe mantenerse correctamente para asegurar su continua disponibilidad e integridad

A.11.2.5	Eliminación de activos	***Control***
		Equipos, información o software no deben ser extraídos fuera del sitio sin autorización previa
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	***Control***
		La seguridad se aplicará a los activos fuera de sitio teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización
A.11.2.7	Eliminación segura o reutilización del equipo	***Control***
		Todos los elementos del equipo que contengan medios de almacenamiento deberán ser verificados para asegurar que los datos sensibles y el software bajo licencia hayan sido eliminados o sobrescritos de forma segura antes de su eliminación o reutilización
A.11.2.8	Equipo desatendido de usuario	***Control***
		Los usuarios deberán asegurarse de que el equipo desatendido tiene la protección adecuada
A.11.2.9	Política de escritorio y pantalla limpia	***Control***
		Se adoptará una política de escritorio limpio de papeles y medios de almacenamiento extraíbles y una política de pantalla limpia para las instalaciones de procesamiento de información
A.12	**Seguridad operacional**	
A.12.1	**Procedimientos y responsabilidades operacionales**	
Objetivo:	Asegurar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información	
A.12.1.1	Procedimientos operativos documentados	***Control***
		Los procedimientos operativos deberán documentarse y ponerse a disposición de todos los usuarios que los necesiten
A.12.1.2	Gestión del cambio	***Control***
		Los cambios en la organización, los procesos de negocio, las instalaciones de procesamiento de información y los sistemas que afectan a la seguridad de la información deben ser controlados
A.12.1.3	Gestión de la capacidad	***Control***
		El uso de los recursos será monitoreado, ajustado y realizarán proyecciones de los requerimientos futuros de capacidad para asegurar el desempeño del sistema requerido
A.12.1.4	Separación de entornos de desarrollo, prueba y operación	***Control***
		Los entornos de desarrollo, prueba y operación deben estar separados para reducir el riesgo de acceso no autorizado o cambios en el entorno operacional
A.12.2	**Protección contra el malware**	

Objetivo:	Garantizar que la información y las instalaciones de procesamiento de información estén protegidas contra el malware	
A.12.2.1	Controles contra el malware	***Control***
		Se implementarán controles de detección, prevención y recuperación para proteger contra el malware, combinados con el conocimiento apropiado del usuario
A.12.3	**Copia de seguridad**	
Objetivo:	Proteger contra la perdida de información	
A.12.3.1	Copia de seguridad de información	***Control***
		Copias de seguridad de la información, software e imágenes del sistema se tomarán y probarán periódicamente de acuerdo con una política de respaldo acordada
A.12.4	**Registro y monitoreo**	
Objetivo:	Para registrar eventos y generar evidencia	
A.12.4.1	Registro de sucesos	***Control***
		Registros de eventos que registran actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información deberán ser realizados, mantenidos y revisados regularmente
A.12.4.2	Protección del registro de información	***Control***
		Registros de instalaciones y registros de información estarán protegidos contra la manipulación y acceso no autorizado
A.12.4.3	Registros del administrador y del operador	***Control***
		Las actividades del administrador del sistema y del operador del sistema deberán ser registradas y los registros protegidos y revisados periódicamente
A.12.4.4	Sincronización de reloj	***Control***
		Los relojes de todos los sistemas de procesamiento de información relevantes dentro de una organización o dominio de seguridad se sincronizarán con una única fuente de tiempo de referencia
A.12.5	**Control de software operativo**	
Objetivo:	Asegurar la integridad de los sistemas operativos	
A.12.5.1	Instalación de software en sistemas operativos	***Control***
		Se implementarán procedimientos para controlar la instalación de software en sistemas operativos
A.12.6	**Gestión de vulnerabilidades técnicas**	
Objetivo:	Evitar la explotación de vulnerabilidades técnicas	
A.12.6.1		***Control***

	Gestión de vulnerabilidades técnicas	La información sobre las vulnerabilidades técnicas de los sistemas de información que se utilicen se obtendrá oportunamente, se evaluará la exposición de la organización a dichas vulnerabilidades y se adoptarán medidas apropiadas para abordar el riesgo asociado
A.12.6.2	Restricción en la instalación del software	***Control***
		Normas que rigen la instalación de software por parte de los usuarios se establecerán e implementarán
A.12.7	**Consideraciones sobre la auditoría de los sistemas de información**	
Objetivo:	Minimizar el impacto de las actividades de auditoría en los sistemas operativos	
A.12.7.1	Controles de auditoría de sistemas de información	***Control***
		Los requisitos de auditoría y las actividades que impliquen la verificación de los sistemas operativos se planificarán y acordarán cuidadosamente para minimizar las interrupciones en los procesos de negocio
A.13	**Seguridad de las comunicaciones**	
A.13.1	**Gestión de la seguridad de la red**	
Objetivo:	Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información	
A.13.1.1	Controles de red	***Control***
		La red será gestionada y controlada para proteger la información en sistemas y aplicaciones
A.13.1.2	Seguridad de los servicios de red	***Control***
		Los mecanismos de seguridad, los niveles de servicios y los requisitos de gestión de todos los servicios de red se identificarán e incluirán en los acuerdos de servicios de red, ya se trate de servicios internos o subcontratado
A.13.1.3	Segregación en redes	***Control***
		Los grupos de servicios de información, usuarios y sistemas de información se segregarán en redes
A.13.2	**Transferencia de información**	
Objetivo:	Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa	
A.13.2.1	Políticas y procedimientos de transferencia de información	***Control***
		Se establecerán políticas, procedimientos y controles de transferencia formal para proteger la transferencia de información mediante el uso de todo tipo de medios de comunicación
A.13.2.2	Acuerdos sobre transferencia de información	***Control***
		Acuerdos deberán abordar la transferencia segura de información comercial entre la organización y las partes externas
A.13.2.3	Mensajería electrónica	***Control***
		La información relacionada con la mensajería electrónica estará debidamente protegida

A.13.2.4	Acuerdos de confidencialidad o no divulgación	***Control***
		Los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de protección de la organización serán identificados, revisados y documentados periódicamente
A.14	**Adquisición, desarrollo y mantenimiento de sistemas**	
A.14.1	**Requisitos de seguridad de los sistemas de información**	
Objetivo:	Asegurar que la seguridad de la información es una parte integral del sistema de información a lo largo de todo el ciclo de vida. Esto incluye también los requisitos para los sistemas de información que proporcionan servicios a través de redes públicas	
A.14.1.1	Análisis y especificaciones de requisitos de seguridad de la información	***Control***
		Los requisitos relacionados con la seguridad de la información se incluirán en los requisitos para nuevos sistemas de información o mejoras en los sistemas de información existentes
A.14.1.2	Asegurar servicios de aplicación en redes públicas	***Control***
		La información involucrada en los servicios de aplicación que pasa por redes públicas estará protegida contra actividad fraudulenta, disputa contractual, divulgación y modificación no autorizada
A.14.1.3	Protección de transacciones de servicios de aplicaciones	***Control***
		La información involucrada en las transacciones de servicios de aplicación estará protegida para evitar la transmisión incompleta, el enrutamiento erróneo, la alteración no autorizada de mensajes, la divulgación no autorizada, la duplicación o reproducción no autorizada de mensajes
A.14.2	**Seguridad en procesos de desarrollo y soporte**	
Objetivo:	Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida del desarrollo de los sistemas de información	
A.14.2.1	Política de desarrollo seguro	***Control***
		Se establecerán y aplicarán reglas para el desarrollo de software y sistemas a los desarrollos dentro de la organización
A.14.2.2	Procedimientos de control de cambios del sistema	***Control***
		Los cambios en los sistemas dentro del ciclo de vida del desarrollo se controlarán mediante el uso de procedimientos formales de control de cambios
A.14.2.3	Revisión técnica de aplicaciones tras cambios en la plataforma operativa	***Control***
		Cuando se cambien las plataformas operativas, las aplicaciones críticas de negocio serán revisadas y probadas para asegurar que no haya impacto adverso en las operaciones de la organización o en la seguridad
A.14.2.4		***Control***

	Restricciones a los cambios en los paquetes de software	Las modificaciones a los paquetes de software deberán ser rechazadas, limitadas a los cambios necesarios y todos los cambios deberán ser estrictamente controlados
A.14.2.5	Principios seguros de ingeniería de sistemas	***Control***
		Los principios para la ingeniería de sistemas seguros se establecerán, documentarán, se mantendrán y se aplicarán a cualquier esfuerzo de implementación del sistema de información
A.14.2.6	Entorno de desarrollo seguro	***Control***
		La Organización establecerá y protegerá apropiadamente los entornos de desarrollo seguro para los esfuerzos de desarrollo e integración del sistema que abarquen todo el ciclo de desarrollo del sistema
A.14.2.7	Desarrollo subcontratado	***Control***
		La organización supervisará y monitoreará la actividad de desarrollo de sistemas subcontratado
A.14.2.8	Pruebas de seguridad del sistema	***Control***
		Las pruebas de funcionalidad de seguridad se llevarán a cabo durante el desarrollo
A.14.2.9	Pruebas de aceptación del sistema	***Control***
		Se establecerán programas de pruebas de aceptación y criterios relacionados para los nuevos sistemas de información, actualizaciones y nuevas versiones
A.14.3	**Datos de prueba**	
Objetivo:	Para garantizar la protección de los datos utilizados para las pruebas	
A.14.3.1	Protección de datos de prueba	***Control***
		Los datos de prueba se seleccionarán cuidadosamente, se protegerán y se controlarán
A.15	**Relaciones con proveedores**	
A.15.1	**Seguridad de la información en las relaciones con proveedores**	
Objetivo:	Asegurar la protección de los activos de la organización a los que pueden acceder los proveedores	
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	***Control***
		Requisitos de seguridad de la información para mitigar el riesgo asociado con el acceso del proveedor a los activos de la organización serán acordados con el proveedor y documentados
A.15.1.2	Abordar la seguridad dentro de los acuerdos de proveedores	***Control***
		Todos los requerimientos relevantes de seguridad de la información serán establecidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI para la información de la organización

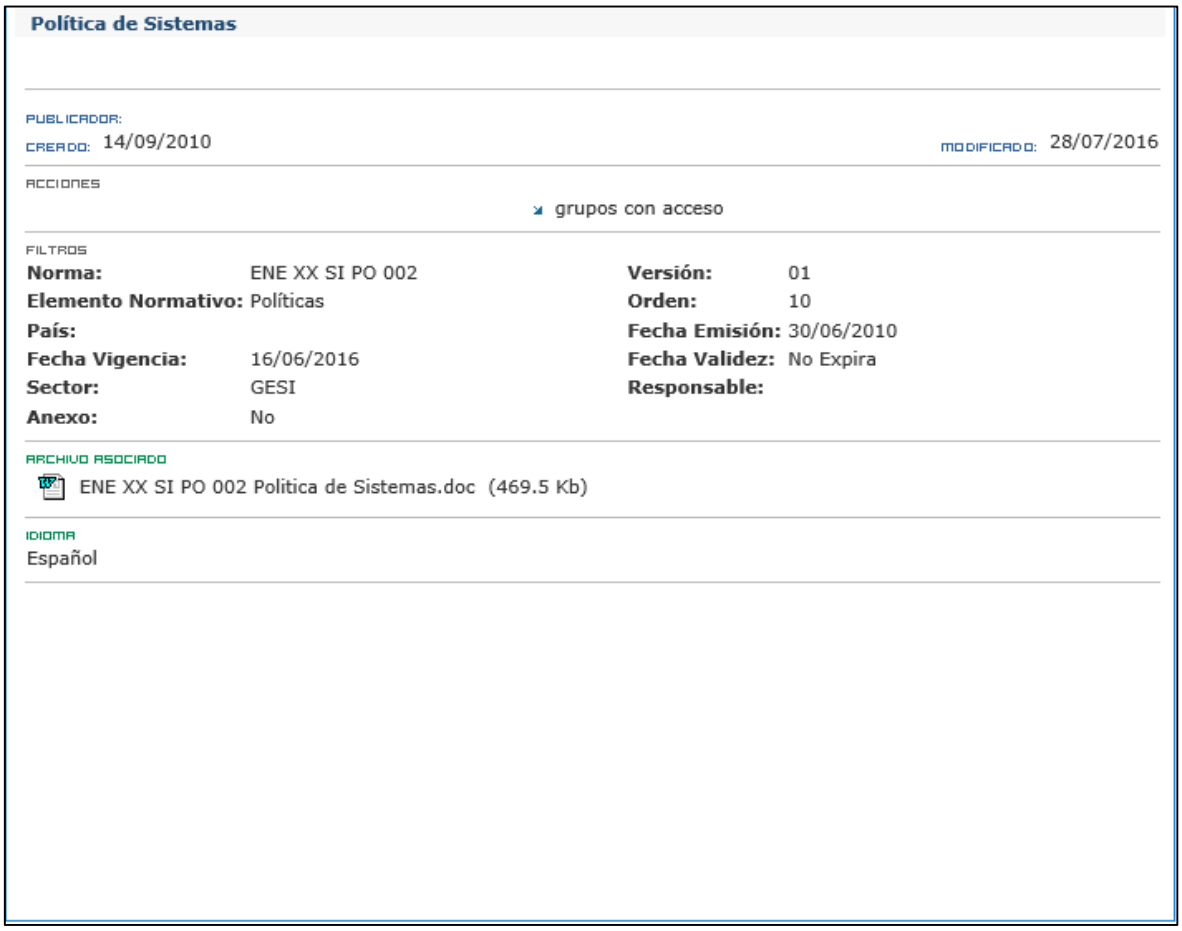
A.15.1.3	Cadena de suministro de tecnología de la información y comunicación	***Control***
		Los acuerdos con proveedores incluirán requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información, las comunicaciones y la cadena de suministro de productos
A.15.2	**Gestión de la entrega de servicios de proveedores**	
Objetivo:	Mantener un nivel de acuerdo de seguridad de la información y prestación de servicios en línea con los acuerdos de proveedores	
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	***Control***
		Las organizaciones deben monitorear, revisar y auditar regularmente la prestación de servicios del proveedor
A.15.2.2	Gestión de cambios en los servicios de proveedores	***Control***
		Los cambios en la prestación de servicios por parte de los proveedores, incluido el mantenimiento, mejora de las políticas, procedimientos y controles de seguridad de la información existentes; se administrarán teniendo en cuenta la criticidad de la información comercial, los sistemas, procesos implicados y la reevaluación de los riesgos
A.16	**Gestión de incidentes de seguridad de la información**	
A.16.1	**Gestión de incidentes y mejoras en seguridad de la información**	
Objetivo:	Asegurar un enfoque coherente y efectivo para la gestión de incidentes de seguridad de la información, incluyendo la comunicación sobre eventos y debilidades de seguridad	
A.16.1.1	Responsabilidades y procedimientos	***Control***
		Gestión de responsabilidades y procedimientos para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información
A.16.1.2	Reporte de eventos de seguridad de la información	***Control***
		Los eventos de seguridad de la información deben ser reportados a través de canales de administración apropiados tan pronto como sea posible
A.16.1.3	Informar sobre las debilidades en la seguridad de la información	***Control***
		Los empleados y contratistas que utilicen los sistemas y servicios de información de la organización deberán tomar nota de cualquier falla observada o presunta debilidad de seguridad de la información en sistemas o servicios
A.16.1.4	Evaluación y decisión sobre los eventos de seguridad de la información	***Control***
		Se evaluarán los eventos de seguridad de la información y se decidirá si se van a clasificar como incidentes de seguridad de la información
A.16.1.5		***Control***

	Respuesta a incidentes de seguridad de la información	Se responderá a los incidentes de seguridad de la información de conformidad con los procedimientos documentados
A.16.1.6	Aprender de los incidentes de seguridad de la información	***Control***
		Los conocimientos obtenidos del análisis y resolución de incidentes de seguridad de la información se utilizarán para reducir la probabilidad o el impacto de futuros incidentes
A.16.1.7	Recolección de pruebas	***Control***
		La organización deberá definir y aplicar procedimientos para la identificación, recolección, adquisición y conservación de la información, que puedan servir como prueba
A.17	**Aspectos de la seguridad de la información en la gestión de la continuidad del negocio**	
A.17.1	**Continuidad de la seguridad de la información**	
Objetivo:	La continuidad de la seguridad de la información se integrará en los sistemas de gestión de continuidad del negocio	
A.17.1.1	Planificación de la continuidad de la seguridad de la información	***Control***
		La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo: durante una crisis o un desastre
A.17.1.2	Implementación de la continuidad de la seguridad de la información	***Control***
		La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad para la seguridad de la información durante una situación adversa
A.17.1.3	Verificar, revisar y evaluar la continuidad de la seguridad de la información	***Control***
		La organización verificará el control de continuidad de seguridad de la información establecido y aplicado, a intervalos regulares a fin de asegurar que sean válidos y eficaces durante situaciones adversas
A.17.2	**Redundancias**	
Objetivo:	Asegurar la disponibilidad de instalaciones de procesamiento de información	
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	***Control***
		Las instalaciones de procesamiento de la información se implementarán con una redundancia suficiente para satisfacer los requisitos de disponibilidad
A.18	**Cumplimiento**	
A.18.1	**Cumplimiento de las exigencias legales y contractuales**	
Objetivo:	Para evitar infracciones legales, estatutarias, reglamentarias u obligaciones contractuales relacionadas con la seguridad de la información y de cualquier requerimiento de seguridad	
A.18.1.1		***Control***

	Identificación de la legislación aplicable y requisitos contractuales	Todos los requisitos legislativos, regulatorios y contractuales relevantes, y el enfoque de la organización para cumplir con estos requisitos deberán ser identificados, documentados y actualizados explícitamente para cada sistema de información y la organización
A.18.1.2	Derechos de propiedad intelectual	***Control***
		Se aplicarán procedimientos adecuados para garantizar el cumplimiento de los requisitos legislativos, regulatorios y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados
A.18.1.3	Protección de registros	***Control***
		Los registros estarán protegidos contra la pérdida, destrucción, falsificación, acceso y liberación no autorizada, de conformidad con los requisitos legislativos, regulatorios, contractuales y comerciales
A.18.1.4	Privacidad y protección de información de identificación personal	***Control***
		Se garantizará la privacidad y la protección de la información de identificación personal, según se requiera en la legislación y la regulación pertinentes donde sea aplicable
A.18.1.5	Regulación de los controles criptográficos	***Control***
		Los controles criptográficos se utilizarán de conformidad con todos los acuerdos, leyes y regulaciones pertinentes
A.18.2	**Revisión de seguridad de la información**	
Objetivo:	Asegurar que la seguridad de la información sea implementada y operada de acuerdo con las políticas y procedimientos de la organización	
A.18.2.1	Revisión independiente de la seguridad de la información	***Control***
		El enfoque de la organización para administrar la seguridad de la información y su implementación (es decir, objetivos de control, controles, procesos de políticas y procedimientos para la seguridad de la información) será revisado independientemente a intervalos planificados o cuando ocurran cambios significativos
A.18.2.2	Cumplimiento de las políticas y estándares de seguridad	***Control***
		Los administradores revisarán periódicamente el cumplimiento del procesamiento de información y los procedimientos dentro de su área de responsabilidad con las políticas de seguridad adecuadas, estándares y cualquier otro requisito de seguridad
A.18.2.3		***Control***

	Revisión del cumplimiento técnico	Los sistemas de información se revisarán periódicamente para verificar el cumplimiento de las políticas y normas de seguridad de la información de la organización

ANEXO 2: Extracto Política de Sistemas (MAR 17 SI PO 002) actualizada.



Política de Sistemas

PUBLICADOR:

CREADO: 14/09/2010 MODIFICADO: 28/07/2016

ACCIONES

grupos con acceso

FILTROS

Norma:	ENE XX SI PO 002	**Versión:**	01
Elemento Normativo:	Políticas	**Orden:**	10
País:		**Fecha Emisión:**	30/06/2010
Fecha Vigencia:	16/06/2016	**Fecha Validez:**	No Expira
Sector:	GESI	**Responsable:**	
Anexo:	No		

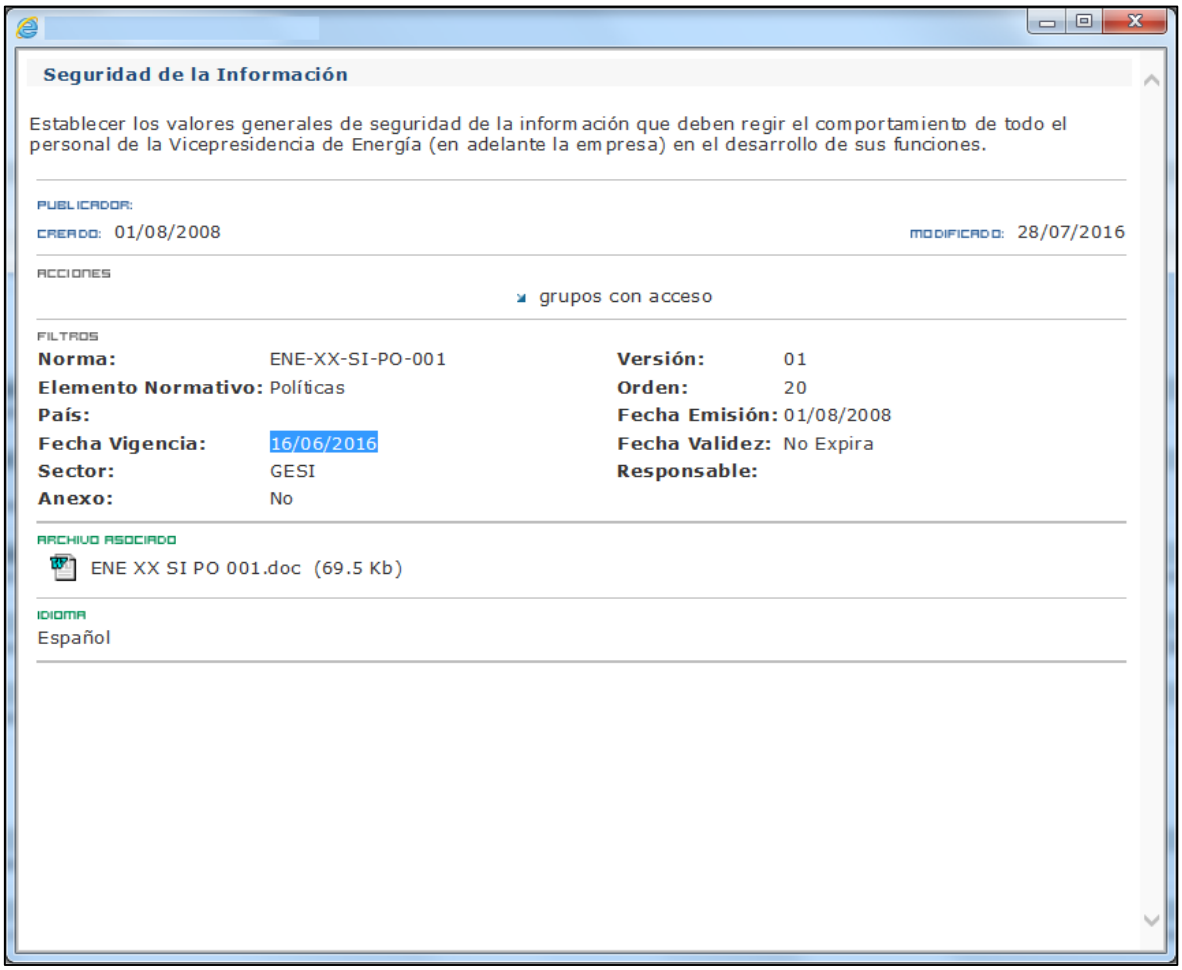
ARCHIVO ASOCIADO

ENE XX SI PO 002 Politica de Sistemas.doc (469.5 Kb)

IDIOMA

Español

ANEXO 3: Extracto Política Seguridad de Información (MAR 17 SI PO 001) actualizada.



Seguridad de la Información

Establecer los valores generales de seguridad de la información que deben regir el comportamiento de todo el personal de la Vicepresidencia de Energía (en adelante la empresa) en el desarrollo de sus funciones.

PUBLICADOR:

CREADO: 01/08/2008 MODIFICADO: 28/07/2016

ACCIONES

grupos con acceso

FILTROS

Norma:	ENE-XX-SI-PO-001	**Versión:**	01
Elemento Normativo:	Políticas	**Orden:**	20
País:		**Fecha Emisión:**	01/08/2008
Fecha Vigencia:	16/06/2016	**Fecha Validez:**	No Expira
Sector:	GESI	**Responsable:**	
Anexo:	No		

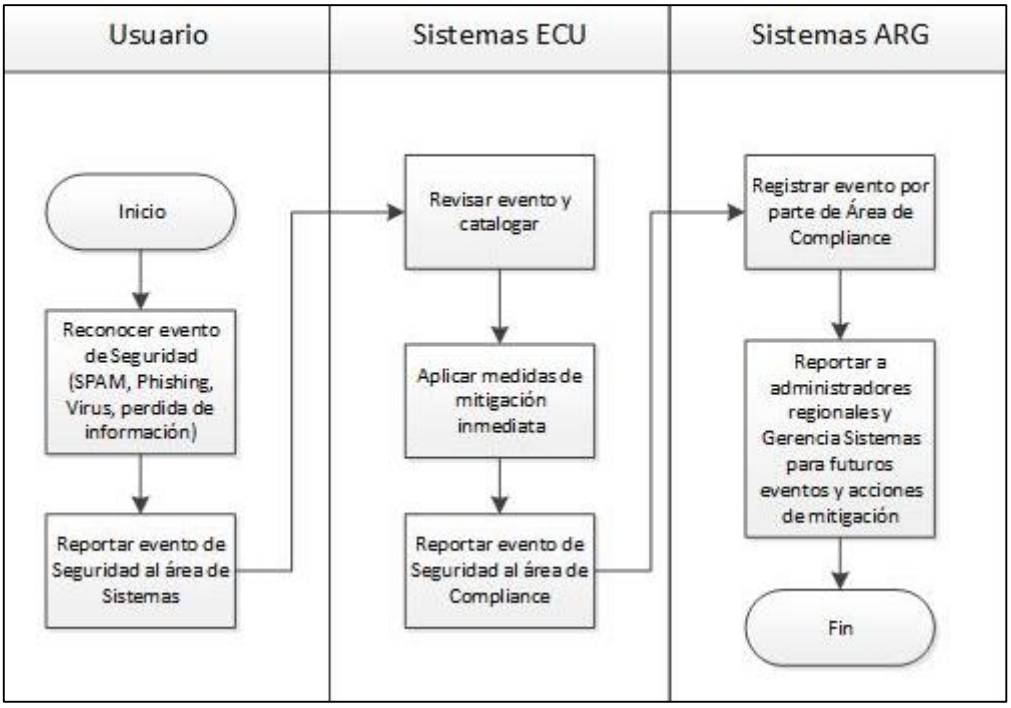
ARCHIVO ASOCIADO

ENE XX SI PO 001.doc (69.5 Kb)

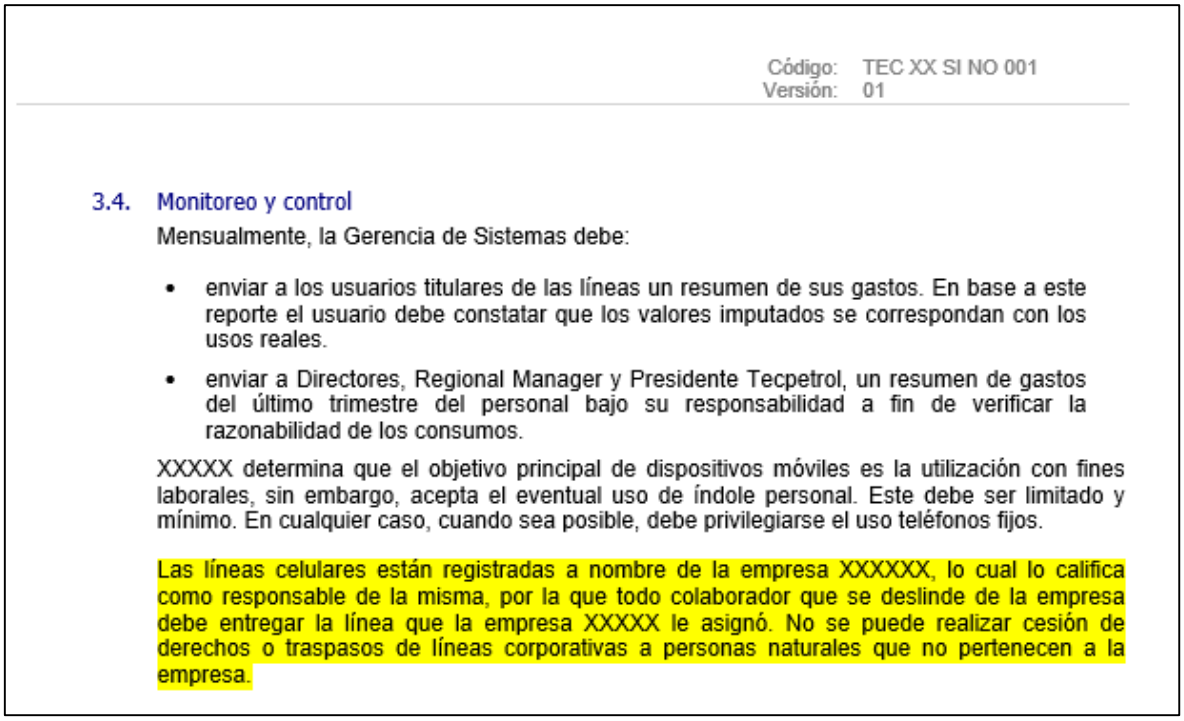
IDIOMA

Español

ANEXO 4: Flujograma de escalamiento y reporte de eventos que afecten a la Seguridad de la Información.



Anexo 5: Aclaratoria a la Norma Utilización de dispositivos móviles - 3.4 Monitoreo y Control, concepto de “Propiedad de la línea”.



Código: TEC XX SI NO 001
Versión: 01

3.4. Monitoreo y control

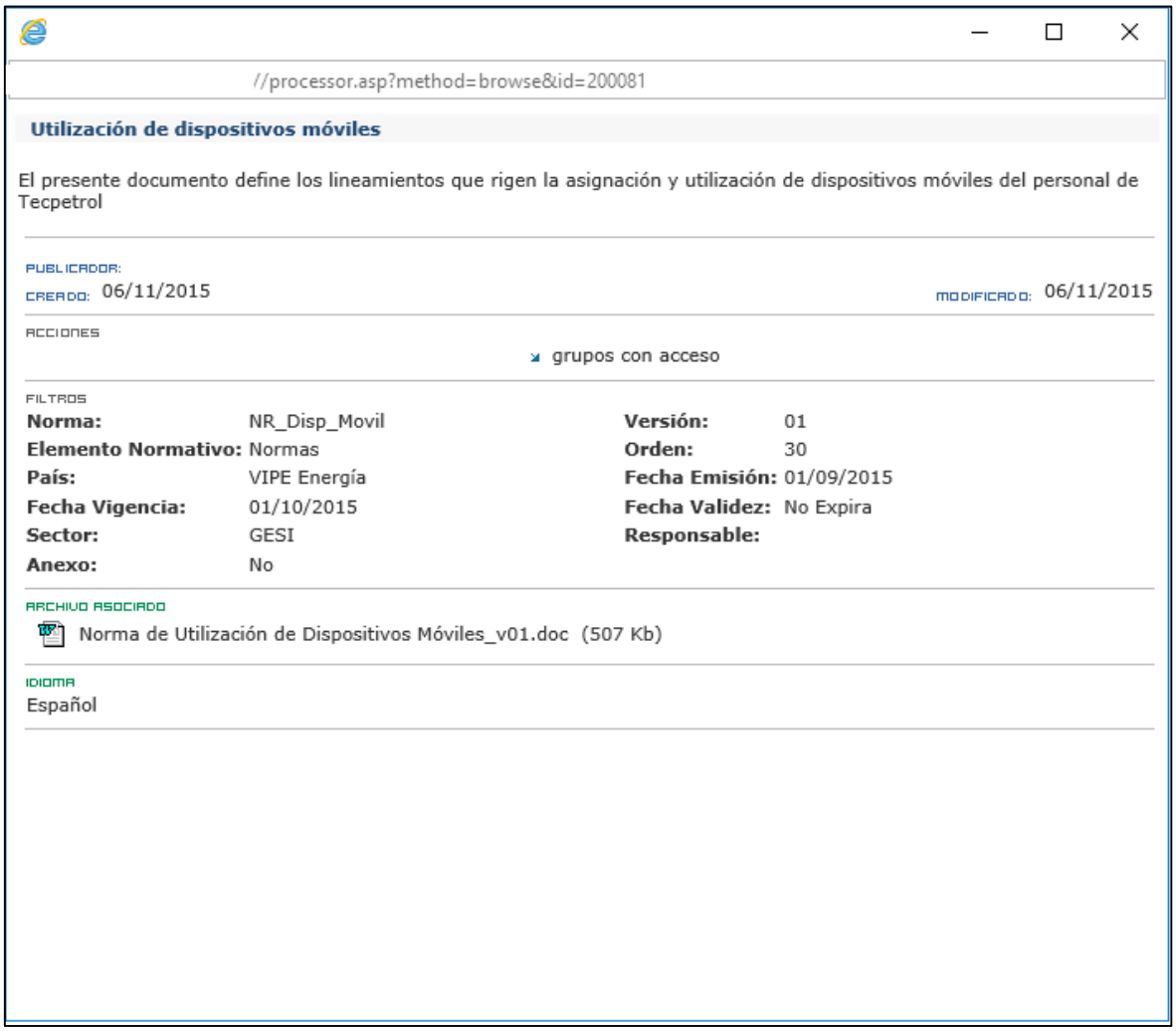
Mensualmente, la Gerencia de Sistemas debe:

- enviar a los usuarios titulares de las líneas un resumen de sus gastos. En base a este reporte el usuario debe constatar que los valores imputados se correspondan con los usos reales.
- enviar a Directores, Regional Manager y Presidente Tecpetrol, un resumen de gastos del último trimestre del personal bajo su responsabilidad a fin de verificar la razonabilidad de los consumos.

XXXXX determina que el objetivo principal de dispositivos móviles es la utilización con fines laborales, sin embargo, acepta el eventual uso de índole personal. Este debe ser limitado y mínimo. En cualquier caso, cuando sea posible, debe privilegiarse el uso teléfonos fijos.

Las líneas celulares están registradas a nombre de la empresa XXXXXX, lo cual lo califica como responsable de la misma, por la que todo colaborador que se deslinde de la empresa debe entregar la línea que la empresa XXXXX le asignó. No se puede realizar cesión de derechos o traspasos de líneas corporativas a personas naturales que no pertenecen a la empresa.

Anexo 6: Extracto Norma Utilización de dispositivos móviles actualizada a Marzo del 2017.



//processor.asp?method=browse&id=200081

Utilización de dispositivos móviles

El presente documento define los lineamientos que rigen la asignación y utilización de dispositivos móviles del personal de Tecpetrol

PUBLICADOR:

CREADO: 06/11/2015 MODIFICADO: 06/11/2015

ACCIONES

grupos con acceso

FILTROS

Norma:	NR_Disp_Movil	**Versión:**	01
Elemento Normativo:	Normas	**Orden:**	30
País:	VIPE Energía	**Fecha Emisión:**	01/09/2015
Fecha Vigencia:	01/10/2015	**Fecha Validez:**	No Expira
Sector:	GESI	**Responsable:**	
Anexo:	No		

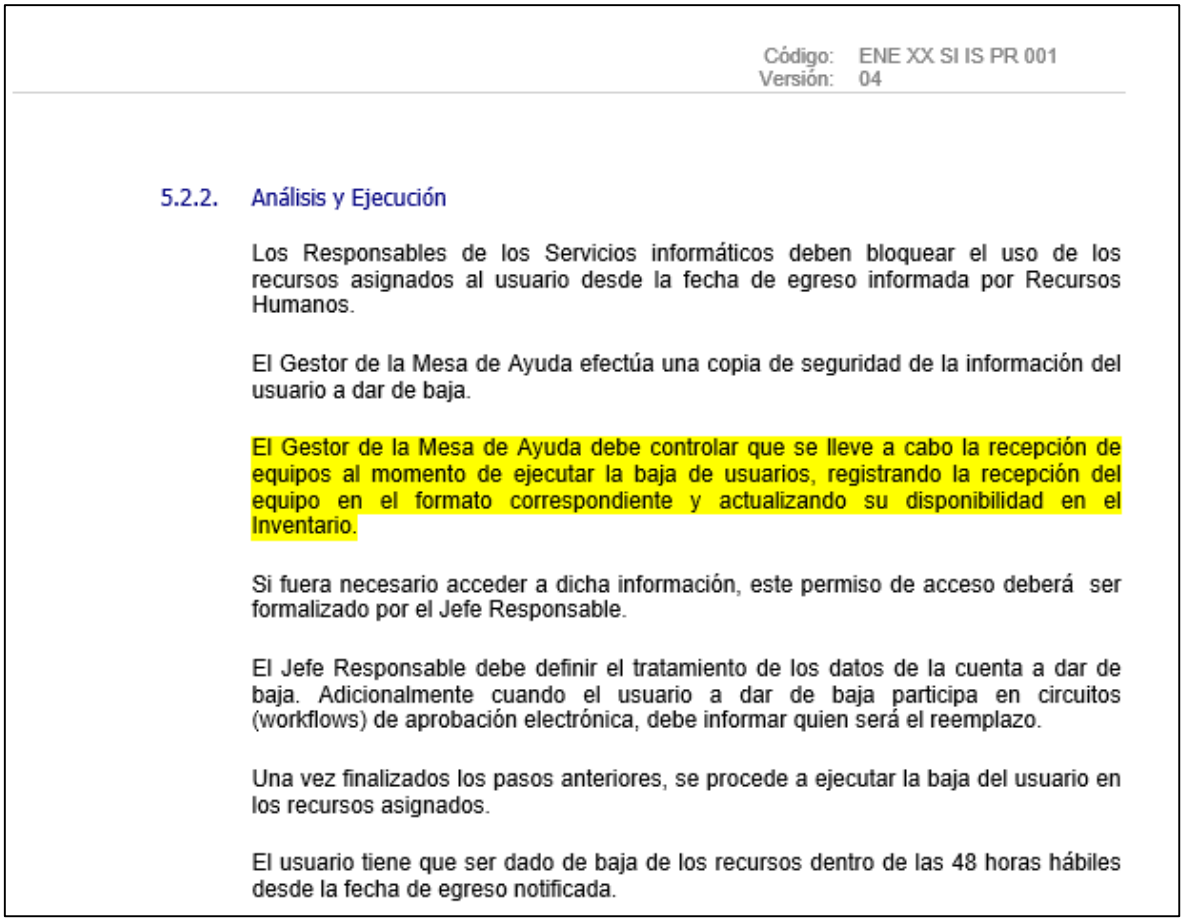
ARCHIVO ASOCIADO

Norma de Utilización de Dispositivos Móviles_v01.doc (507 Kb)

IDIOMA

Español

Anexo 7: Extracto Política de Alta, Baja y Modificación de Usuarios, punto 5.2.2, inclusión actividad “Entrega y Retiro equipos”.



Código: ENE XX SI IS PR 001
Versión: 04

5.2.2. Análisis y Ejecución

Los Responsables de los Servicios informáticos deben bloquear el uso de los recursos asignados al usuario desde la fecha de egreso informada por Recursos Humanos.

El Gestor de la Mesa de Ayuda efectúa una copia de seguridad de la información del usuario a dar de baja.

El Gestor de la Mesa de Ayuda debe controlar que se lleve a cabo la recepción de equipos al momento de ejecutar la baja de usuarios, registrando la recepción del equipo en el formato correspondiente y actualizando su disponibilidad en el Inventario.

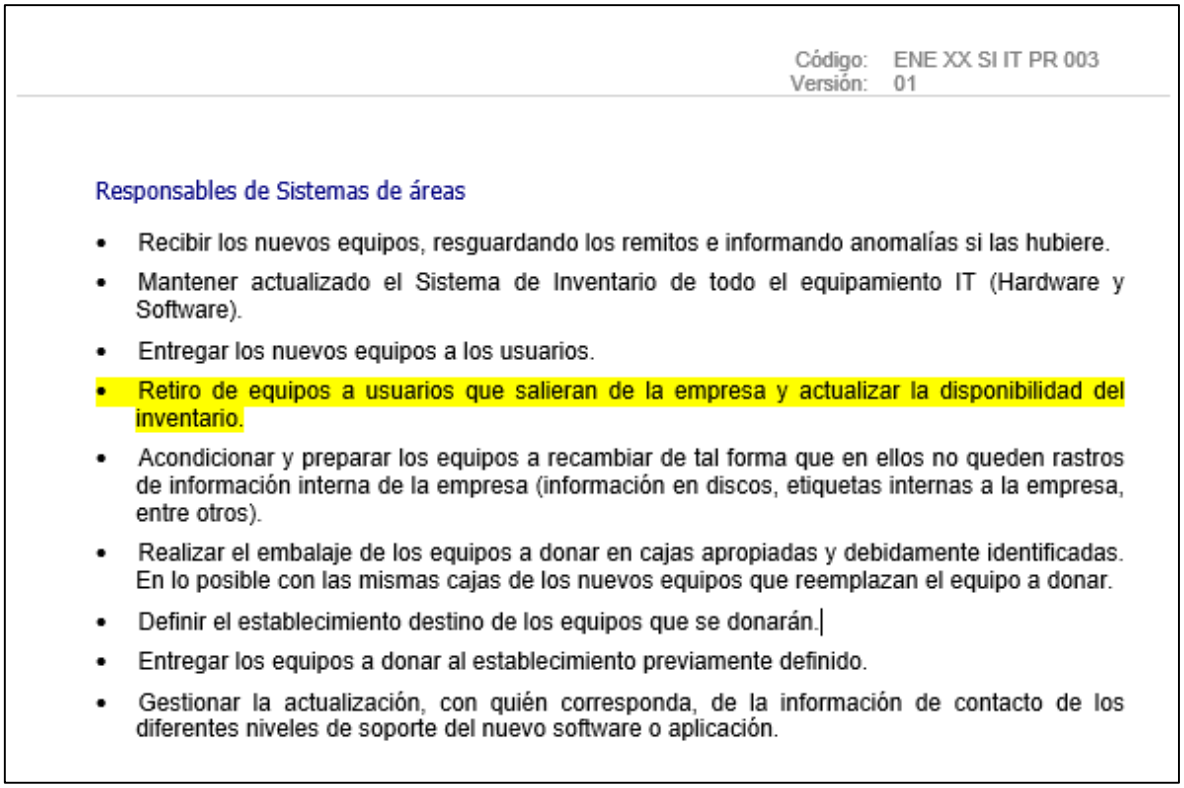
Si fuera necesario acceder a dicha información, este permiso de acceso deberá ser formalizado por el Jefe Responsable.

El Jefe Responsable debe definir el tratamiento de los datos de la cuenta a dar de baja. Adicionalmente cuando el usuario a dar de baja participa en circuitos (workflows) de aprobación electrónica, debe informar quien será el reemplazo.

Una vez finalizados los pasos anteriores, se procede a ejecutar la baja del usuario en los recursos asignados.

El usuario tiene que ser dado de baja de los recursos dentro de las 48 horas hábiles desde la fecha de egreso notificada.

Anexo 8: Extracto Procedimiento de Gestión de Activos de IT, 3. Responsabilidades - Responsable de Sistemas de área: “Actividades de retiro de equipos”.

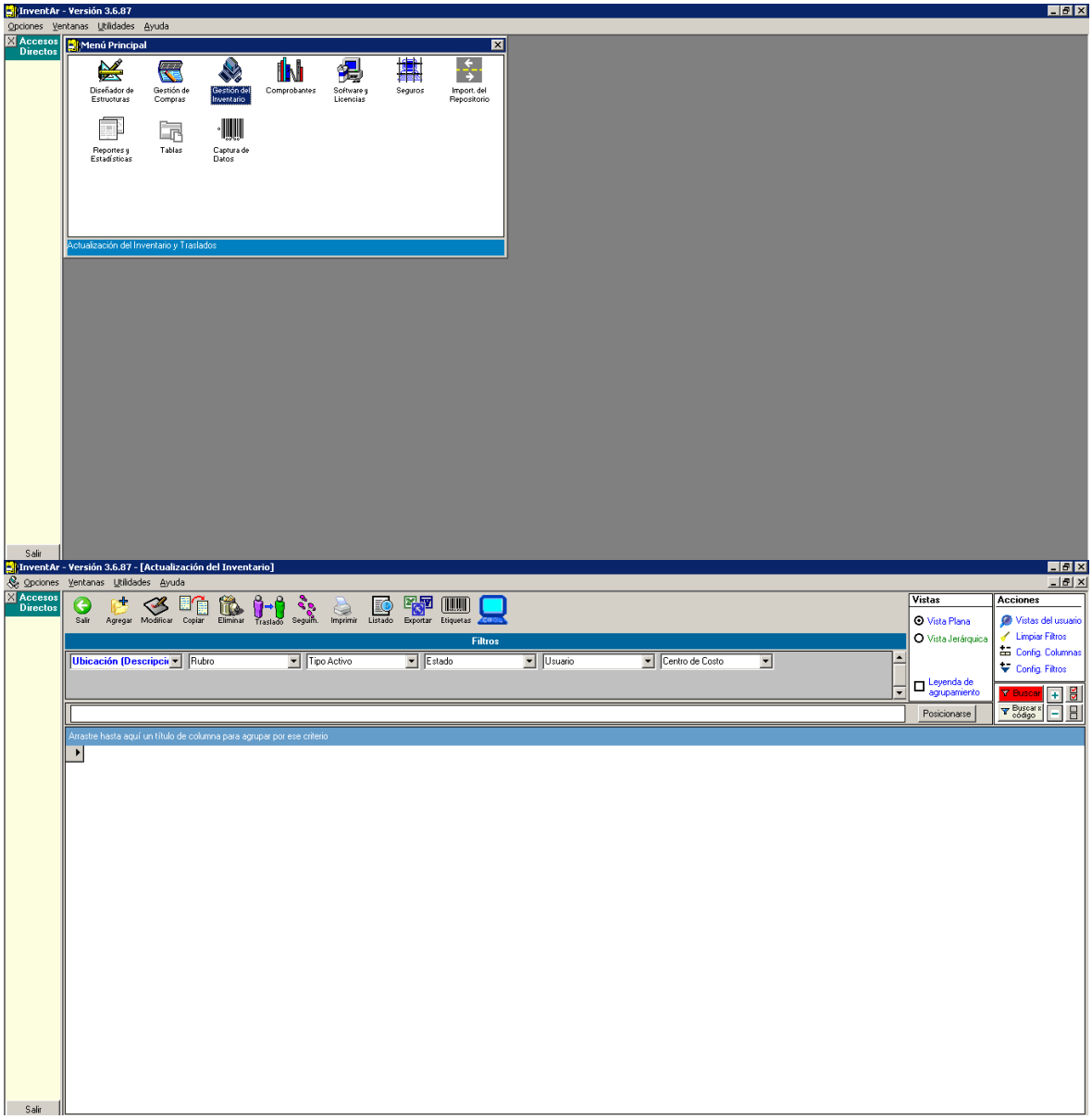


Código: ENE XX SI IT PR 003
Versión: 01

Responsables de Sistemas de áreas

- Recibir los nuevos equipos, resguardando los remitos e informando anomalías si las hubiere.
- Mantener actualizado el Sistema de Inventario de todo el equipamiento IT (Hardware y Software).
- Entregar los nuevos equipos a los usuarios.
- Retiro de equipos a usuarios que salieran de la empresa y actualizar la disponibilidad del inventario.
- Acondicionar y preparar los equipos a recambiar de tal forma que en ellos no queden rastros de información interna de la empresa (información en discos, etiquetas internas a la empresa, entre otros).
- Realizar el embalaje de los equipos a donar en cajas apropiadas y debidamente identificadas. En lo posible con las mismas cajas de los nuevos equipos que reemplazan el equipo a donar.
- Definir el establecimiento destino de los equipos que se donarán.
- Entregar los equipos a donar al establecimiento previamente definido.
- Gestionar la actualización, con quién corresponda, de la información de contacto de los diferentes niveles de soporte del nuevo software o aplicación.

Anexo 9: Captura Pantalla Sistema de Inventarios – Reporte de Activos Ecuador.



Anexo 10: Planilla de Asignación / Retiro de Equipos actualizada a Marzo 2017.

CONSTANCIA ENTREGA - RECEPCION

FECHA DE ENTREGA:	5/7/2017
DOCUMENTO N°:	ER- -2017 - 005

EQUIPOS INVENTARIADOS

Cantidad	N° Inventario	Tipo de Equipo	Marca	Modelo	Numero de Serie	Centro Costo
1	XXXXXXXX	LAPTOP	LENOVO	X250	XXXXXX	0

ACCESORIOS ADICIONALES

Item	MARCA	Cantidad	TIPO DE EQUIPO	Observaciones
1	LENOVO	1	CARGADOR	

DATOS DEL USUARIO

Usuario de AD:	XXXXXX	Persona que utilizará o será responsable del equipo
Nombre:	XXXXXX	
(*) Responsable Funcional:		(*) Indicar si el usuario es contratado (tercero)

SOFTWARE BASE

Sistema operativo	STD	Si fuera NO STD deberá adjuntar autorización

DATOS DEL SOPORTISTA

Soportista:		
Tarea:	ENTREGA EQUIPO	Firma y aclaración del Soportista

DEVOLUCION DE EQUIPO

N° inventario Equipo liberado:			
Destino:			
Nombre/Usuario destinatario:			
Fecha Devolución:		Firma y aclaración del Usuario	Firma y aclaración del Soportista

Declaro que he recibido el equipamiento mencionado y se encuentra bajo mi resguardo.

En tal sentido asumo la responsabilidad por su guarda y cuidado, y me comprometo a cumplir con las pautas mencionadas respaldadas en su mayoría por el Código de Conducta establecido en la empresa.

Les recordamos que el uso de las herramientas de Informática y de Comunicación que la empresa le provee está sujeto a principios establecidos en la **Norma "Uso de Herramientas Electrónicas de Comunicación"** de la Organización Techint publicada en nuestro Sistema Normativo.

HARDWARE:

- Mantener informado al Help Desk respecto de la ubicación física del equipamiento y de los cambios de titularidad del mismo.
- Informar al Help Desk inmediatamente en caso de anomalías en su funcionamiento o en caso de robo o hurto.
- Asegurar que únicamente acceda al mismo para su mantenimiento de software y/o cambio de configuración personal del Help Desk.
- Tomar todas las medidas preventivas razonables destinadas a asegurar la integridad física del equipamiento.

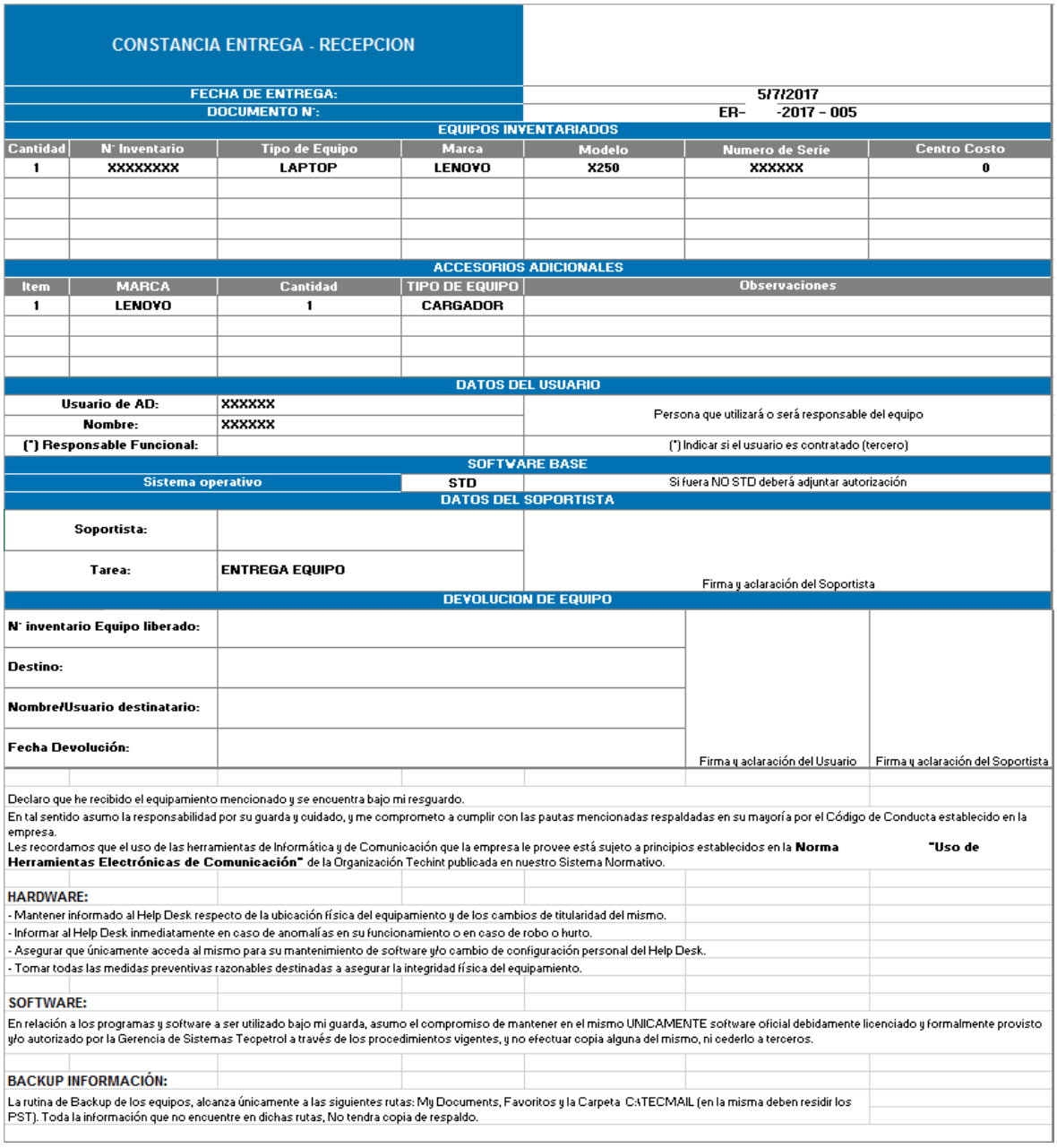
SOFTWARE:

En relación a los programas y software a ser utilizado bajo mi guarda, asumo el compromiso de mantener en el mismo UNICAMENTE software oficial debidamente licenciado y formalmente provisto y/o autorizado por la Gerencia de Sistemas Tecpetrol a través de los procedimientos vigentes, y no efectuar copia alguna del mismo, ni cederlo a terceros.

BACKUP INFORMACIÓN:

La rutina de Backup de los equipos, alcanza únicamente a las siguientes rutas: My Documents, Favoritos y la Carpeta C:\TECMAIL (en la misma deben residir los PST). Toda la información que no encuentre en dichas rutas, No tendra copia de respaldo.

Anexo 11: Captura Pantalla Formulario de registro de Equipos en Intranet Corporativa.



CONSTANCIA ENTREGA - RECEPCION

FECHA DE ENTREGA:	5/7/2017
DOCUMENTO N°:	ER- -2017 - 005

EQUIPOS INVENTARIADOS

Cantidad	N° Inventario	Tipo de Equipo	Marca	Modelo	Numero de Serie	Centro Costo
1	XXXXXXXX	LAPTOP	LENOVO	X250	XXXXXX	0

ACCESORIOS ADICIONALES

Item	MARCA	Cantidad	TIPO DE EQUIPO	Observaciones
1	LENOVO	1	CARGADOR	

DATOS DEL USUARIO

Usuario de AD:	XXXXXX	Persona que utilizará o será responsable del equipo
Nombre:	XXXXXX	
(*) Responsable Funcional:		(*) Indicar si el usuario es contratado (tercero)

SOFTWARE BASE

Sistema operativo	STD	Si fuera NO STD deberá adjuntar autorización

DATOS DEL SOPORTISTA

Soportista:		
Tarea:	ENTREGA EQUIPO	Firma y aclaración del Soportista

DEVOLUCION DE EQUIPO

N° inventario Equipo liberado:			
Destino:			
Nombre/Usuario destinatario:			
Fecha Devolución:		Firma y aclaración del Usuario	Firma y aclaración del Soportista

Declaro que he recibido el equipamiento mencionado y se encuentra bajo mi resguardo.

En tal sentido asumo la responsabilidad por su guarda y cuidado, y me comprometo a cumplir con las pautas mencionadas respaldadas en su mayoría por el Código de Conducta establecido en la empresa.

Les recordamos que el uso de las herramientas de Informática y de Comunicación que la empresa le provee está sujeto a principios establecidos en la **Norma "Uso de Herramientas Electrónicas de Comunicación"** de la Organización Techint publicada en nuestro Sistema Normativo.

HARDWARE:

- Mantener informado al Help Desk respecto de la ubicación física del equipamiento y de los cambios de titularidad del mismo.
- Informar al Help Desk inmediatamente en caso de anomalías en su funcionamiento o en caso de robo o hurto.
- Asegurar que únicamente acceda al mismo para su mantenimiento de software y/o cambio de configuración personal del Help Desk.
- Tomar todas las medidas preventivas razonables destinadas a asegurar la integridad física del equipamiento.

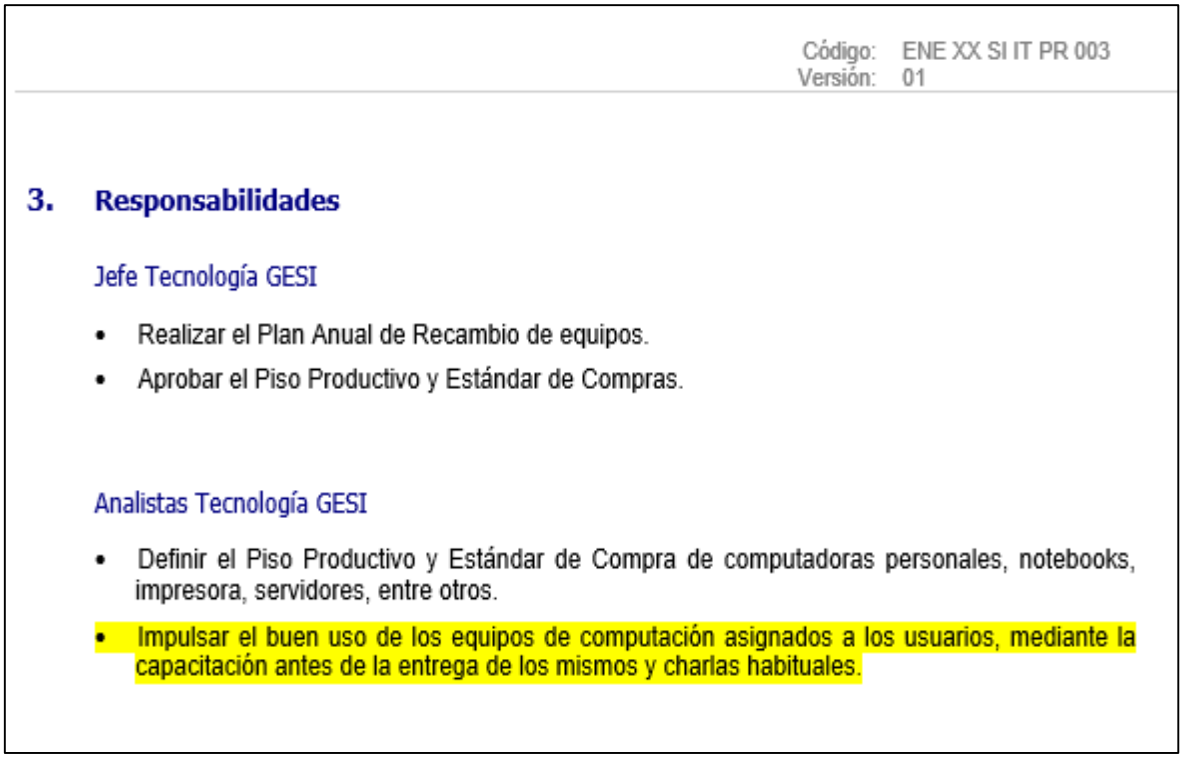
SOFTWARE:

En relación a los programas y software a ser utilizado bajo mi guarda, asumo el compromiso de mantener en el mismo UNICAMENTE software oficial debidamente licenciado y formalmente provisto y/o autorizado por la Gerencia de Sistemas Tecpetrol a través de los procedimientos vigentes, y no efectuar copia alguna del mismo, ni cederlo a terceros.

BACKUP INFORMACIÓN:

La rutina de Backup de los equipos, alcanza únicamente a las siguientes rutas: My Documents, Favoritos y la Carpeta C:\TECMAIL (en la misma deben residir los PST). Toda la información que no encuentre en dichas rutas, No tendra copia de respaldo.

Anexo 12: Extracto Procedimiento de Gestión de Activos dentro del punto que cita las actividades de comunicación sobre el buen uso de los activos.



Código: ENE XX SI IT PR 003
Versión: 01

3. Responsabilidades

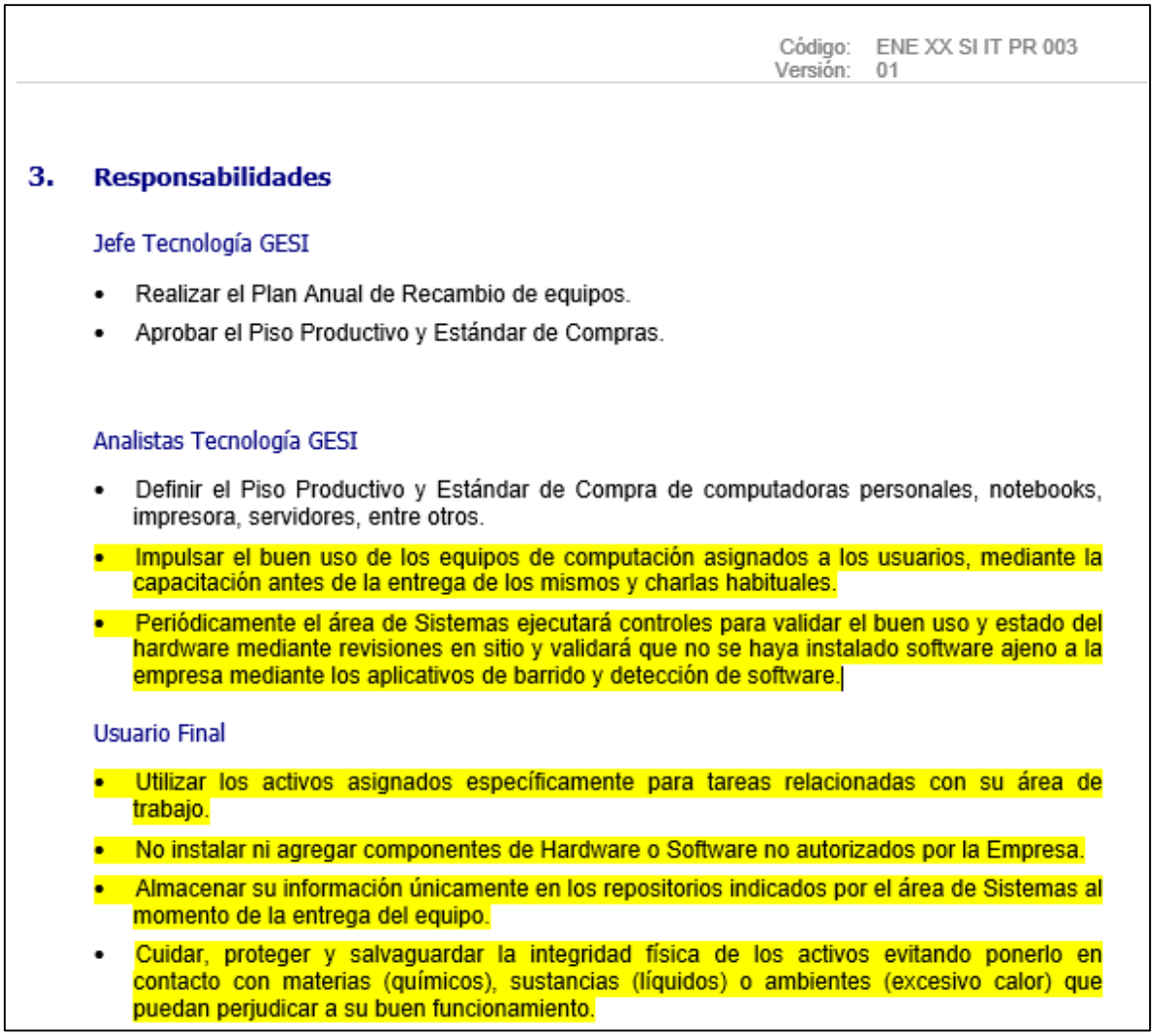
Jefe Tecnología GESI

- Realizar el Plan Anual de Recambio de equipos.
- Aprobar el Piso Productivo y Estándar de Compras.

Analistas Tecnología GESI

- Definir el Piso Productivo y Estándar de Compra de computadoras personales, notebooks, impresora, servidores, entre otros.
- Impulsar el buen uso de los equipos de computación asignados a los usuarios, mediante la capacitación antes de la entrega de los mismos y charlas habituales.

Anexo 13: Extracto Procedimiento de Gestión de Activos – Actividades de control sobre el buen uso de los activos.



Código: ENE XX SI IT PR 003
Versión: 01

3. Responsabilidades

Jefe Tecnología GESI

- Realizar el Plan Anual de Recambio de equipos.
- Aprobar el Piso Productivo y Estándar de Compras.

Analistas Tecnología GESI

- Definir el Piso Productivo y Estándar de Compra de computadoras personales, notebooks, impresora, servidores, entre otros.
- Impulsar el buen uso de los equipos de computación asignados a los usuarios, mediante la capacitación antes de la entrega de los mismos y charlas habituales.
- Periódicamente el área de Sistemas ejecutará controles para validar el buen uso y estado del hardware mediante revisiones en sitio y validará que no se haya instalado software ajeno a la empresa mediante los aplicativos de barrido y detección de software.

Usuario Final

- Utilizar los activos asignados específicamente para tareas relacionadas con su área de trabajo.
- No instalar ni agregar componentes de Hardware o Software no autorizados por la Empresa.
- Almacenar su información únicamente en los repositorios indicados por el área de Sistemas al momento de la entrega del equipo.
- Cuidar, proteger y salvaguardar la integridad física de los activos evitando ponerlo en contacto con materias (químicos), sustancias (líquidos) o ambientes (excesivo calor) que puedan perjudicar a su buen funcionamiento.

Anexo 14: Matriz de Software Estándar para Ecuador.

Ítem	Software	Estándar	Especializado
1	Adobe PRO		X
2	Adobe Reader XI	X	
3	ADUC		X
4	Airwatch		X
5	APC Advanced View		X
6	AutoCad 2015		X
7	Autograph		X
8	Chrome		X
9	Cisco AnyConect	X	
10	Infoprod		X
11	Internet Explorer	X	
12	Inventar		X
13	Lync 2010	X	
14	Lync 2013	X	
15	NetApp		X
16	Office 2013	X	
17	OFM		X
18	Open Text		X
19	OpenWells		X
20	Petrel		X
21	Project 2013		X
22	RSA Mobile	X	
23	SAP	X	
24	Skype for Business 2016		X
25	Symantec DLO	X	
26	Visio 2013		X
27	WellPlan		X
28	Windows 10		X
29	Windows 7	X	
30	Windows XP		X
31	WinRAR	X	
32	Zafiro		X

Anexo 15: Listado de perfiles de usuario (privilegios) para Ecuador.

Usuario	Nombre	Cargo
SXX	XXXXXX	Gerente General
TECFXX	XXXXXX	Gerente Administración y Finanzas
TECFXX	XXXXXX	Gerente de Facilidades
TECGXX	XXXXXX	Gerente de Planificación
TECRXX	XXXXXX	Gerente Operaciones
TECAXX	XXXXXX	Contadora
TECAXX	XXXXXX	Gerente RRHH
TECWXX	XXXXXX	Coordinador de Sistemas

Anexo 16: Clasificación de información.

Niveles de Clasificación			
Clasificación	**Daño / Impacto**	**Acceso**	**Autoriza Acceso**
MUY CONFIDENCIAL	Material / Alto	Muy Restrictivo	Dueño del Proceso (Director)
CONFIDENCIAL	Moderado	Restrictivo	Dueño de la Información (Gerente)
USO INTERNO	Bajo	Interno	Jefe del Usuario Solicitante
PUBLICA	Nulo	Público	-

Anexo 17: Controles de Seguridad.

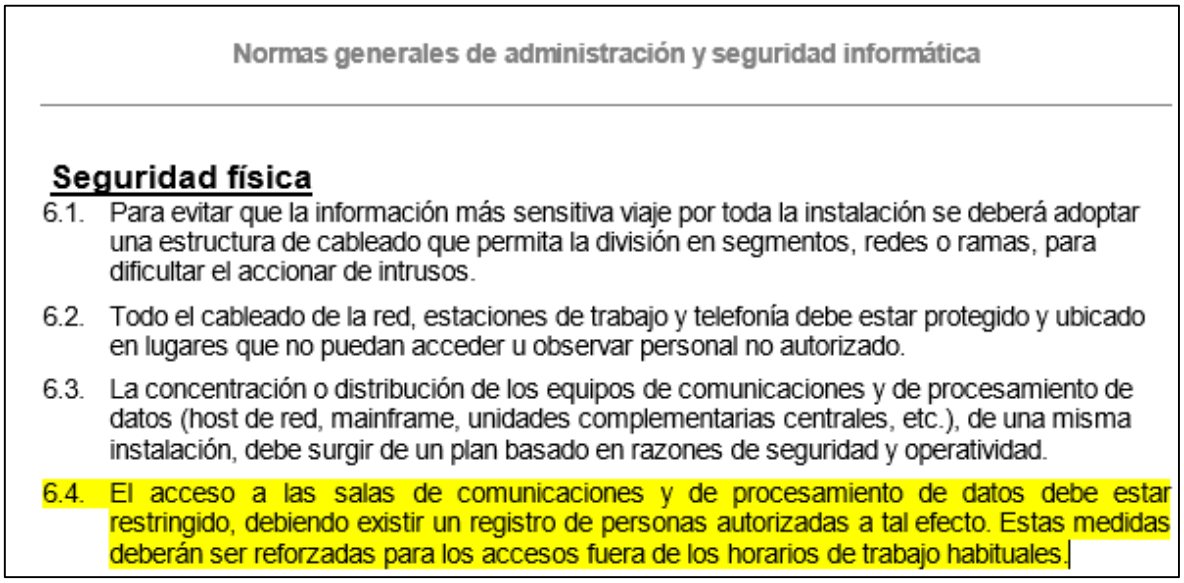
6.2.4. Alta e instalación

Una vez que se realiza la recepción de los nuevos productos, deben ser dados de alta en el Sistema de Inventario, donde deben ingresarse los datos mínimos requeridos para un adecuado control y seguimiento de los activos informáticos de la compañía. Estos datos mínimos incluyen: Rubro del activo, Fecha de compra, # de nota de pedido, Fecha de alta, Vencimiento de garantía, tipo de licenciamiento, vencimiento de licencia, versión y proveedor.

Todo equipo informático que sea preparado para la entrega debe cumplir con los siguientes requisitos:

- Sistema Operativo licenciado y registrado.
- Completar Matriz de Software instalado acorde al perfil.
- Activación de chip TPM.
- Activación de cifrado de información bitlocker.
- Activación de agente de respaldos DLO.
- Activación de agente antivirus TREND.
- Desactivar actualizaciones automáticas.
- Registrar equipo en servidor de contenido para actualizaciones aprobadas corporativamente.

Anexo 18: Acceso a Áreas restringidas.



Normas generales de administración y seguridad informática

Seguridad física

6.1. Para evitar que la información más sensitiva viaje por toda la instalación se deberá adoptar una estructura de cableado que permita la división en segmentos, redes o ramas, para dificultar el accionar de intrusos.

6.2. Todo el cableado de la red, estaciones de trabajo y telefonía debe estar protegido y ubicado en lugares que no puedan acceder u observar personal no autorizado.

6.3. La concentración o distribución de los equipos de comunicaciones y de procesamiento de datos (host de red, mainframe, unidades complementarias centrales, etc.), de una misma instalación, debe surgir de un plan basado en razones de seguridad y operatividad.

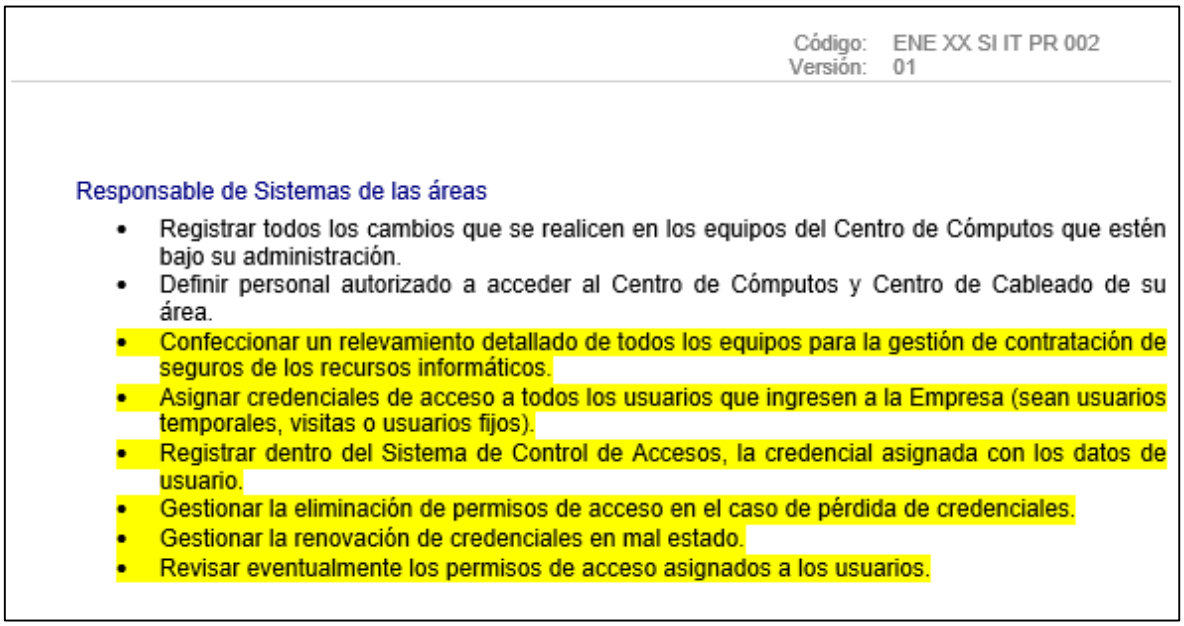
6.4. El acceso a las salas de comunicaciones y de procesamiento de datos debe estar restringido, debiendo existir un registro de personas autorizadas a tal efecto. Estas medidas deberán ser reforzadas para los accesos fuera de los horarios de trabajo habituales.

Anexo 19: Matriz de Perfiles de Usuario.

	Operaciones					Perforación					Administración y Finanzas								Planificación				Seguridad y Salud				Security		Recursos Humanos			
	Gerente	Jefatura	Analista Interno	Analista Externo	Pasante	Gerente	Jefatura	Analista Interno	Analista Externo	Pasante	Gerente	Jefatura	Analista Interno ADFI	Analista Externo ADFI	Analista Interno ABAS	Analista Interno SISTEMAS	Analista Externo SISTEMAS	Pasante	Gerente	Analista Interno	Analista Externo	Pasante	Gerente	Jefatura	Analista Interno	Analista Externo	Jefatura	Analista Externo	Gerente	Jefatura	Analista Interno	Pasante
Accesos Básicos y Equipos																																
Computador	Laptop	Laptop	Laptop	Desktop	Desktop	Laptop	Laptop	Laptop	Desktop	Desktop	Laptop	Laptop	Laptop	Desktop	Laptop	Desktop	Desktop	Desktop	Laptop	Laptop	Desktop	Desktop	Laptop	Laptop	Laptop	Desktop	Laptop	Desktop	Laptop	Laptop	Laptop	Desktop
Usuario de red	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si
Casilla de correo electrónico	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si
Tarjeta de acceso a instalaciones	Acceso General	Acceso General	Acceso General	Acceso General	Acceso General	Acceso General	Acceso General	Acceso General	Acceso General	Acceso General	Acceso General	Acceso General	Acceso General	Acceso General	Acceso General	Acceso Total	Acceso General	Acceso General	Acceso General	Acceso General	Acceso General	Acceso General	Acceso General	Acceso General	Acceso General	Acceso General	Acceso Total	Acceso General	Acceso General	Acceso General	Acceso General	Acceso General
Comunicaciones Unificadas (Lync)	Si	Si	Si	No	Si	Si	Si	Si	No	Si	Si	Si	Si	No	Si	Si	Si	Si	Si	Si	No	Si	Si	Si	Si	No	Si	Si	Si	Si	Si	Si
Extensión Telefónica	Si	Si	Si	No	Si	Si	Si	Si	No	Si	Si	Si	Si	No	Si	Si	No	Si	Si	Si	No	Si	Si	Si	Si	No	Si	Si	Si	Si	Si	Si
Aplicaciones de Seguridad																																
Token / VPN	Si	Si	Si	No	No	Si	Si	Si	No	No	Si	Si	Si	No	No	No	No	No	Si	Si	No	No	Si	Si	Si	No	Si	No	Si	Si	Si	No
Antivirus	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si
Respaldo de información	Si	Si	Si	Si	No	Si	Si	Si	Si	No	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	No	Si	Si	Si	Si	Si	Si	Si	Si	Si	No
Bitlocker	Si	Si	Si	No	No	Si	Si	Si	No	No	Si	Si	Si	No	Si	Si	No	No	Si	Si	No	No	Si	Si	Si	No	Si	No	Si	Si	Si	No
Intranet Corporativa																																
Acceso a Intranet	Si	Si	Si	No	Si	Si	Si	Si	No	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	No	Si	Si	Si	Si	No	Si	Si	Si	Si	Si	Si
Acceso a SharePoint Ecuador	Si	Si	Si	No	Si	Si	Si	Si	No	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	No	Si	Si	Si	Si	No	Si	No	Si	Si	Si	Si
Repositorio de información general	Si	Si	Si	No	Si	Si	Si	Si	No	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	No	Si	Si	Si	Si	No	Si	Si	Si	Si	Si	Si
Sistema de Notas	Si	Si	No	No	No	Si	Si	No	No	No	Si	Si	No	No	No	No	No	No	Si	No	No	No	Si	Si	No	No	Si	No	Si	Si	No	No
Biblioteca Digital Operaciones	Si	Si	Si	No	Si	Si	Si	Si	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No
Biblioteca Digital Perforación	Si	Si	No	No	No	Si	Si	Si	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No
Biblioteca Digital Planificación	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	Si	Si	No	Si	No	No	No	No	No	No	No	No	No	No
Biblioteca Digital ADFI - Contabilidad	No	No	No	No	No	No	No	No	No	No	Si	Si	Si	Si	Si	No	Si	Si	No	No	No	No	No	No	No	No	No	No	No	No	No	No
Biblioteca Digital ADFI - CUPA	No	No	No	No	No	No	No	No	No	No	Si	Si	No	No	No	No	No	Si	No	No	No	No	No	No	No	No	No	No	No	No	No	No
Biblioteca Digital ADFI - Impuestos	No	No	No	No	No	No	No	No	No	No	Si	Si	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No
Biblioteca Digital ADFI - Sistemas	No	No	No	No	No	No	No	No	No	No	Si	No	No	No	No	Si	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No
Biblioteca Digital SAS	No	No	No	No	No	No	No	No	No	No	Si	Si	Si	Si	Si	Si	Si	Si	No	No	No	No	Si	Si	Si	Si	No	No	No	No	No	No
Biblioteca Digital RRHH	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	Si	Si	Si	No
Internet																																
Navegación en Internet	Si	Si	Si	No	Si	Si	Si	Si	No	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si
Unidades de Red																																
Repositorio Común de Información	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si
Repositorio de Informac	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	Si	Si	No	No

ión de Seguridad																																
Unidad de Red Operaciones	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	No	No	No	Si	Si	Si	Si	Si	No	No	No	No	No	No	No	No	No	No	No	No	No	No
Unidad de Red Perforación	Si	Si	No	No	No	Si	Si	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No
Unidad de Red Planificación	Si	Si	No	No	No	Si	Si	No	No	No	Si	Si	No	No	Si	No	No	No	Si	Si	Si	Si	No	No	No	No	Si	No	No	No	No	No
Unidad de Red ADFI - Contabilidad	No	No	No	No	No	No	No	No	No	No	Si	Si	Si	No	Si	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No
Unidad de Red ADFI - CUPA	No	No	No	No	No	No	No	No	No	No	Si	Si	Si	No	Si	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No
Unidad de Red ADFI - Impuestos	No	No	No	No	No	No	No	No	No	No	Si	Si	Si	No	Si	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No
Unidad de Red ADFI - Sistemas	No	No	No	No	No	No	No	No	No	No	Si	No	No	No	No	Si	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No
Unidad de Red Digital SAS	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	No	Si	Si	No	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si
Unidad de Red Digital RRHH	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	Si	Si	Si	Si
Equipos adicionales																																
Equipo celular	Si	Si	No	No	No	Si	Si	No	No	No	Si	Si	No	No	No	Si	No	No	Si	No	No	No	Si	No	No	No	Si	No	Si	No	No	No
Radio VHF	Si	Si	No	No	No	Si	Si	No	No	No	Si	Si	No	No	No	Si	No	No	Si	No	No	No	Si	Si	Si	No	Si	Si	Si	No	No	No
Aplicaciones específicas																																
SAP General	Si	Si	Si	No	No	Si	Si	Si	No	No	Si	Si	Si	No	Si	Si	Si	No	Si	Si	Si	Si	Si	Si	Si	No	Si	No	Si	Si	Si	Si
SAP Compras	No	No	No	No	No	No	No	No	No	No	No	Si	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No
SAP RRHH	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	Si	Si	Si	Si
SAP Básico	Si	Si	No	No	No	Si	Si	No	No	No	Si	Si	No	No	No	Si	No	No	Si	Si	Si	Si	Si	Si	No	No	Si	No	Si	Si	Si	No
SAP Producción	Si	No	No	No	No	Si	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No
Meta 4	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	Si	Si	No
SharePoint Argentina	Si	Si	Si	No	No	Si	Si	Si	No	No	Si	Si	Si	No	No	Si	No	No	Si	Si	No	No	Si	Si	Si	No	No	No	Si	Si	Si	Si	No
Sistema SAS	Si	Si	Si	No	Si	Si	Si	Si	No	Si	Si	Si	Si	No	No	Si	No	No	Si	Si	No	Si	Si	Si	Si	No	Si	No	Si	Si	Si	Si	Si

Anexo 20: Asignación de credenciales de acceso.

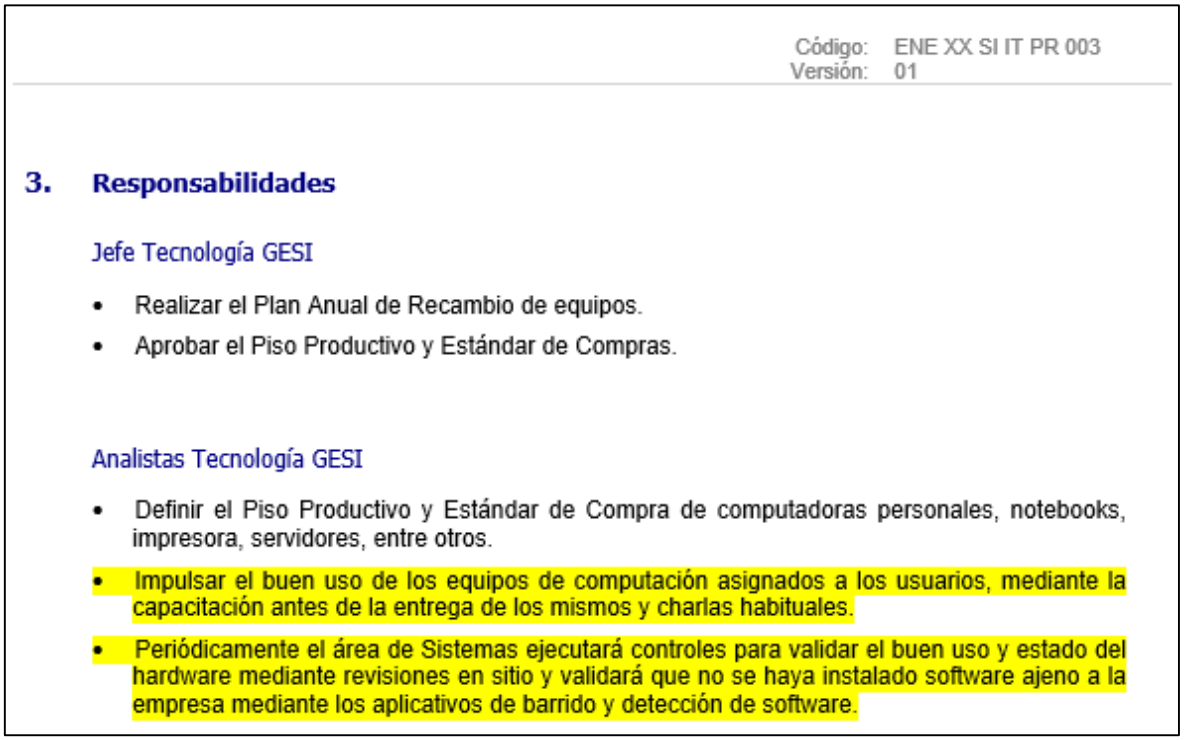


Código: ENE XX SI IT PR 002
Versión: 01

Responsable de Sistemas de las áreas

- Registrar todos los cambios que se realicen en los equipos del Centro de Cómputos que estén bajo su administración.
- Definir personal autorizado a acceder al Centro de Cómputos y Centro de Cableado de su área.
- Confeccionar un relevamiento detallado de todos los equipos para la gestión de contratación de seguros de los recursos informáticos.
- Asignar credenciales de acceso a todos los usuarios que ingresen a la Empresa (sean usuarios temporales, visitas o usuarios fijos).
- Registrar dentro del Sistema de Control de Accesos, la credencial asignada con los datos de usuario.
- Gestionar la eliminación de permisos de acceso en el caso de pérdida de credenciales.
- Gestionar la renovación de credenciales en mal estado.
- Revisar eventualmente los permisos de acceso asignados a los usuarios.

Anexo 21: Extracto Procedimiento de Gestión de Activos de IT, 3. Responsabilidades - Responsable de Sistemas de área: “Control de Activos”.



Código: ENE XX SI IT PR 003
Versión: 01

3. Responsabilidades

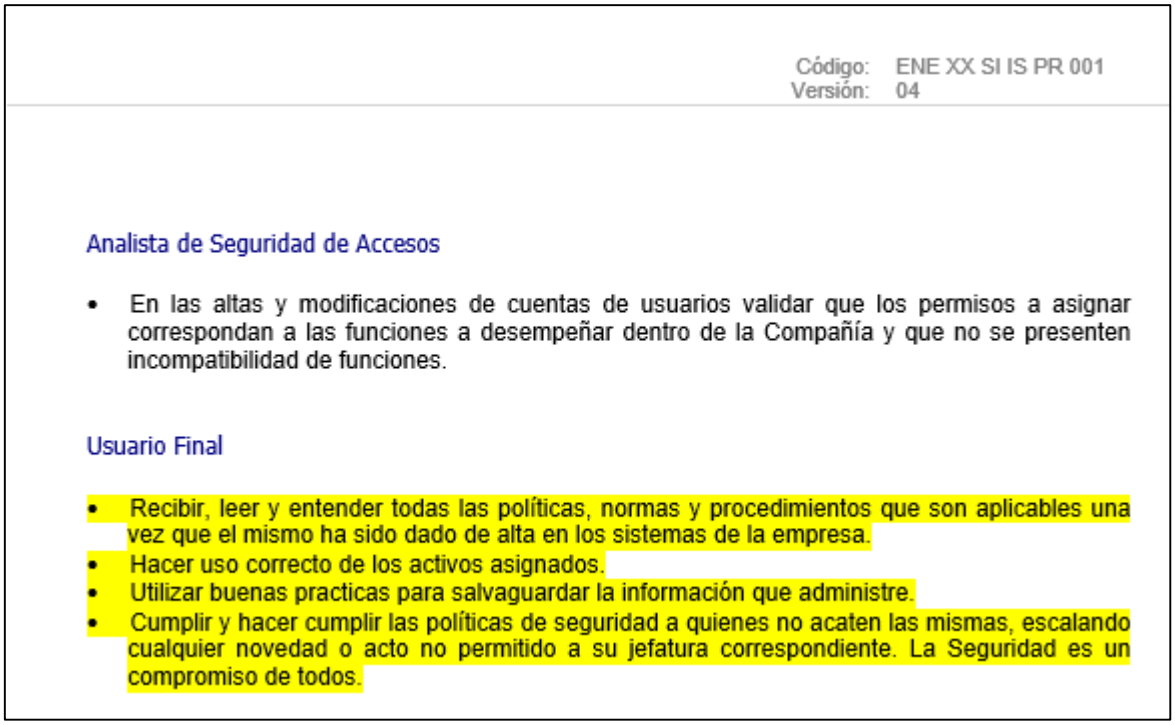
Jefe Tecnología GESI

- Realizar el Plan Anual de Recambio de equipos.
- Aprobar el Piso Productivo y Estándar de Compras.

Analistas Tecnología GESI

- Definir el Piso Productivo y Estándar de Compra de computadoras personales, notebooks, impresora, servidores, entre otros.
- Impulsar el buen uso de los equipos de computación asignados a los usuarios, mediante la capacitación antes de la entrega de los mismos y charlas habituales.
- Periódicamente el área de Sistemas ejecutará controles para validar el buen uso y estado del hardware mediante revisiones en sitio y validará que no se haya instalado software ajeno a la empresa mediante los aplicativos de barrido y detección de software.

Anexo 22: Extracto Política de Alta, Baja y Modificación de Usuarios, inclusión actividad "Compromiso de los usuarios".



Código: ENE XX SI IS PR 001
Versión: 04

Analista de Seguridad de Accesos

- En las altas y modificaciones de cuentas de usuarios validar que los permisos a asignar correspondan a las funciones a desempeñar dentro de la Compañía y que no se presenten incompatibilidad de funciones.

Usuario Final

- Recibir, leer y entender todas las políticas, normas y procedimientos que son aplicables una vez que el mismo ha sido dado de alta en los sistemas de la empresa.
- Hacer uso correcto de los activos asignados.
- Utilizar buenas practicas para salvaguardar la información que administre.
- Cumplir y hacer cumplir las políticas de seguridad a quienes no acaten las mismas, escalando cualquier novedad o acto no permitido a su jefatura correspondiente. La Seguridad es un compromiso de todos.

Anexo 23: Formato de Matriz de registro de Tiempos para el subproceso Alta de Usuarios.

Ítem	Usuario	Tipo usuario	Cargo	Área	Usuario Modelo	Codigo Tipo Usuario	Permisos		
							Tipo 1	Tipo 2	Tipo 3
1	YTECHR	Externo	Auditor ARCH	Operaciones	Sin Ref.	1	X		
2	YTEMAN	Externo	Auditor ARCH	Operaciones	Sin Ref.	1	X		
3	YTECHJ	Externo	Auditor PWC	Impuestos	Sin Ref.	3			X
4	YTEPPA	Externo	Auditor ARCH	Administración	Sin Ref.	3			X
5	YTEDOL	Externo	Auditor ARCH	Administración	Sin Ref.	3			X
6	YTEFRH	Externo	Analista Sistemas	Sistemas	Sin Ref.	2		X	
7	YTEESC	Externo	Operador Security	Security	Sin Ref.	1	X		
8	YTEMED	Externo	Medico	Seguridad y Salud	Sin Ref.	1	X		
9	YTELGT	Externo	Medico	Seguridad y Salud	Sin Ref.	1	X		
10	YTEJHH	Externo	Operador Security	Security	Sin Ref.	1	X		
11	YTEGED	Externo	Operador Security	Security	Sin Ref.	1	X		
12	YTEEIL	Externo	Medico	Seguridad y Salud	Sin Ref.	1	X		
13	TECPED	Interno	Recorredor	Operaciones	Sin Ref.	2		X	
14	YTENEM	Externo	Auditor ARCH	Operaciones	Sin Ref.	1	X		
15	YTEYAN	Externo	Analista SAS	Seguridad y Salud	Sin Ref.	1	X		
16	YTEEDM	Externo	Company MAN	Producción	Sin Ref.	3			X
17	YTEAMO	Externo	Company MAN	Producción	Sin Ref.	3			X
18	TECBRA	Interno	Técnico de Mant.	Mantenimiento	Sin Ref.	2		X	
19	TECLOE	Pasante	Pasante	Planing	Sin Ref.	2		X	
20	YTEPAI	Externo	Medico	Seguridad y Salud	Sin Ref.	1	X		
21	TECMLZ	Pasante	Pasante	Reservorios	Sin Ref.	2		X	
22	TECCHB	Pasante	Pasante	Operaciones	Sin Ref.	2		X	
23	TECLER	Pasante	Pasante	Operaciones	Sin Ref.	2		X	
24	YTESPM	Externo	Analista RRHH	Recursos Humanos	Sin Ref.	3			X
25	YTEAUV	Externo	Medico	Seguridad y Salud	Sin Ref.	1	X		
26	YTEDIS	Externo	Medico	Seguridad y Salud	Sin Ref.	1	X		
27	TECDAN	Interno	Analista Financiera	Administración	Sin Ref.	3			X
28	YTEXAV	Externo	Analista Químico	Operaciones	Sin Ref.	1	X		
29	YTERIV	Externo	Analista Sistemas	Sistemas	Sin Ref.	2		X	
30	TECGAK	Pasante	Pasante	Comercial	Sin Ref.	2		X	
31	YTEJEN	Externo	Medico	Seguridad y Salud	Sin Ref.	1	X		
32	YTELIZ	Externo	Abogado	Planing	Sin Ref.	2		X	
33	TECCAI	Pasante	Pasante	RRHH	Sin Ref.	2		X	
34	YTEKLO	Externo	Analista Funcional	Impuestos	Sin Ref.	3			X
35	YTEPPA	Externo	Auditor ARCH	Administración	Sin Ref.	3			X
36	YTEZAR	Externo	Coordinador Security	Security	Sin Ref.	2		X	
37	TECZUM	Interno	Analista Comercial	Comercial	Sin Ref.	3			X
38	YTERUX	Externo	Auditor PWC	Impuestos	Sin Ref.	3			X
39	YTEVEC	Externo	Analista Sistemas	Impuestos	Sin Ref.	3			X
40	YTEJIM	Externo	Coordinador Security	Security	Sin Ref.	2		X	
41	YTEDAZ	Externo	Analista Sistemas	Sistemas	YTERIV	2		X	
42	YTEAMD	Externo	Auditor ARCH	Operaciones	Sin Ref.	1	X		
43	YTEBAL	Externo	Operador Security	Security	YTECAQ	1	X		
44	YTECIS	Externo	Operador Security	Security	YTECAQ	1	X		
45	YTEIVA	Externo	Operador Security	Security	YTECAQ	1	X		
46	YTEFMA	Externo	Analista Sistemas	Impuestos	YTEKLO	3			X
47	TECCIB	Interno	Ingeniero Reservorios	Reservorios	TECCIS	3			X

48	YTESOU	Externo	Auditor ARCH	Operaciones	Matriz	1	X		
49	YTERUX	Externo	Auditor PWC	Impuestos	Matriz	3			X
50	TECGAE	Interno	Técnico de Mant.	Mantenimiento	Matriz	2		X	
51	YTEEVE	Externo	Analista Impuestos	Impuestos	Matriz	3			X
52	YTEPRO	Externo	Coordinador Security	Security	Matriz	2		X	
53	TECKFR	Pasante	Pasante	Operaciones	Matriz	2		X	
54	TECDCE	Pasante	Pasante	Reservorios	Matriz	2		X	
55	TECDML	Pasante	Pasante	Operaciones	Matriz	2		X	
56	YTEOLG	Externo	Analista Sistemas	Impuestos	Matriz	3			X
57	YTEADN	Externo	Abogado	Administración	Matriz	2		X	
58	TECWAL	Pasante	Pasante	RRHH	Matriz	3			X
59	YTEYUJ	Externo	Medico	Seguridad y Salud	Matriz	1	X		
60	TECJIM	Interno	Recorredor	Operaciones	Matriz	2		X	
61	YTEMAR	Externo	Medico	Seguridad y Salud	Matriz	1	X		

Anexo 24: Formato de Matriz de registro de Tiempos para el subproceso Baja de Usuarios.

Ítem	Usuario	Tipo de Usuario	Área	Cargo	Código Tipo de Usuario	Tipo 1	Tipo 2	Tipo 3
1	TECCIB	Interno	Reservorios	Ingeniero Reservorios	3			X
2	TECAAC	Interno	Perforación	Company Man	3			X
3	TECEME	Interno	Perforación	Company Man	3			X
4	TECLUI	Interno	Operaciones	Ingeniero de Procesos	2		X	
5	TECCVV	Interno	Abastecimientos	Analista de Compras	3			X
6	TECSKA	Interno	Seguridad y Salud	Analista de Seguridad	2		X	
7	TECRRV	Interno	Operaciones	Ayudante Tareas Generales	2	X		
8	TECIRM	Interno	Sistemas	Coordinador Sistemas	3			X
9	YTECPU	Externo	Sistemas	Analista de Sistemas	1	X		
10	YTEJCC	Externo	Seguridad y Salud	Medico	1	X		
11	TECCEF	Interno	Operaciones	Recorredor	1	X		
12	TECMRP	Interno	Mantenimiento	Técnico de Mantenimiento	1	X		
13	YTEAUW	Externo	Operaciones	Ingeniero de Producción	1	X		
14	YTESIL	Externo	Impuestos	Analista de Impuestos	1	X		
15	YTEAYJ	Externo	Facilidades	Ingeniero de Facilidades	1	X		
16	YTEDMO	Externo	Operaciones	Auditor ARCH	1	X		
17	TECLOU	Pasante	Gerencia	Asistente de Gerencia	2		X	
18	TECMSC	Interno	Abastecimientos	Bodeguero	3			X
19	YTECZM	Externo	Security	Operador	1	X		
20	YTEZUP	Externo	Planing	Abogada	1	X		
21	YTEAMC	Externo	Impuestos	Analista de Impuestos	1	X		
22	TECRIT	Interno	Reservorios	Ingeniero Reservorios	2		X	
23	YTEDML	Externo	Operaciones	Auditor ARCH	1	X		
24	YTEJCV	Externo	Operaciones	Auditor ARCH	1	X		
25	YTEKLO	Externo	Impuestos	Analista Funcional	3			X
26	YTEIPA	Externo	Seguridad y Salud	Medico	1	X		
27	YTESIJ	Externo	Operaciones	Auditor ARCH	1	X		
28	TECPLU	Pasante	Perforación	Pasante	1	X		
29	TECKAT	Pasante	Operaciones	Pasante	1	X		
30	TECLBR	Pasante	Operaciones	Pasante	1	X		
31	TECLCH	Pasante	Operaciones	Pasante	1	X		
32	YTEDOL	Externo	Administración	Auditor ARCH	3			X
33	TECDLE	Interno	Operaciones	Recorredor	1	X		
34	YTELCM	Externo	Impuestos	Analista de Impuestos	1	X		
35	YTEPPA	Externo	Administración	Auditor ARCH	3			X
36	YTECHJ	Externo	Administración	Analista de Contabilidad	3			X
37	YTEHHV	Externo	Seguridad y Salud	Analista de Seguridad	1	X		
38	YTEJUN	Externo	Seguridad y Salud	Analista de Seguridad	1	X		

39	YTEMED	Externo	Seguridad y Salud	Medico	1	X		
40	YTEJHH	Externo	Security	Operador	1	X		
41	YTEXAV	Externo	Operaciones	Analista Químico	1	X		
42	YTEMAN	Externo	Operaciones	Auditor ARCH	1	X		
43	TECMMQ	Interno	Operaciones	Recorredor	1	X		
44	YTESAG	Externo	Operaciones	Auditora ARCH	1	X		
45	TECLOE	Pasante	Planing	Pasante	2		X	
46	TECDYA	Interno	Operaciones	Analista Comercial	2		X	
47	YTEJAT	Externo	Security	Coordinador Security	2		X	
48	TECLIZ	Pasante	Comercial	Abogada	2		X	
49	TECJCU	Interno	Security	Coordinador Security	2		X	
50	YTEKAT	Externo	Sistemas	Analista Sistemas	3			X
51	YTEPDA	Interno	Operaciones	Genérico	1	X		
52	TECP26	Interno	Operaciones	Genérico	1	X		
53	TECPMP	Interno	Operaciones	Pasante	2		X	
54	YTEPMC	Externo	Operaciones	Pasante	2		X	
55	TECDAV	Interno	Operaciones	Supervisor Producción	3			X
56	YTECHR	Externo	Operaciones	Auditora ARCH	1	X		
57	TECJIR	Interno	Comercial	Analista Comercial	3			X
58	YTEPGT	Externo	Sistemas	Analista Sistemas	2		X	
59	YTEJIM	Externo	Security	Coordinador Security	2		X	
60	TECCHB	Pasante	Operaciones	Pasante	2		X	
61	TECLER	Pasante	Operaciones	Pasante	2		X	
62	TECMLZ	Pasante	Reservorios	Pasante	2		X	
63	YTEVEC	Externo	Sistemas	Analista Sistemas	3			X
64	TECALB	Interno	Operaciones	Jóven Profesional	2		X	
65	TECEFN	Interno	Operaciones	Operador	1	X		
66	YTERIV	Externo	Sistemas	Analista Sistemas	2		X	
67	YTEAMO	Externo	Producción	Company Man	3			X
68	YTEEDM	Externo	Producción	Company Man	3			X
69	YTEAUV	Interno	Seguridad y Salud	Medico	1	X		
70	TECGAK	Pasante	Planing	Pasante	2		X	
71	TECCAI	Pasante	RRHH	Pasante	2		X	
72	YTEPPA	Externo	Administración	Auditor ARCH	2		X	
73	YTERUX	Externo	Impuestos	Auditor PWC	3			X
74	YTEEIL	Externo	Seguridad y Salud	Medico	1	X		
75	YTEPAI	Externo	Seguridad y Salud	Medico	1	X		
76	YTECCL	Externo	Administración	Abogado	1	X		
77	TECDAN	Interno	Administración	Analista Financiera	3			X
78	TECJIM	Interno	Operaciones	Recorredor	2		X	
79	TECGCP	Interno	Facilidades	Ingeniero de Mejora	3			X
80	TECGAC	Interno	RRHH	Coordinadora RRHH	3			X

Anexo 25: Tabla de valores estándar de la distribución de Gauss.

t	0.00	0.01	0.02	0.03	0.04	0.05	0.06	0.07	0.08	0.09
0.0	0.00	0.80	1.60	2.39	3.19	3.99	4.78	5.58	6.38	7.17
0.1	7.97	8.76	9.55	10.34	11.13	11.92	12.71	13.50	14.28	15.07
0.2	15.85	16.63	17.41	18.19	18.97	19.74	20.51	21.28	22.05	22.82
0.3	23.58	24.34	25.10	25.86	26.61	27.37	28.12	28.86	29.61	30.35
0.4	31.08	31.82	32.55	33.28	34.01	34.73	35.45	36.16	36.88	37.59
0.5	38.29	38.99	39.69	40.39	41.08	41.77	42.45	43.13	43.81	44.48
0.6	45.15	45.81	46.47	47.13	47.78	48.43	49.07	49.71	50.35	50.98
0.7	51.61	52.23	52.85	53.46	54.07	54.67	55.27	55.87	56.46	57.05
0.8	57.63	58.21	58.78	59.35	59.91	60.47	61.02	61.57	62.11	62.65
0.9	63.19	63.72	64.24	64.76	65.28	65.79	66.29	66.80	67.29	67.78
1.0	68.27	68.75	69.23	69.70	70.17	70.63	71.09	71.54	71.99	72.43
1.1	72.87	73.30	73.73	74.15	74.57	74.99	75.40	75.80	76.20	76.60
1.2	76.99	77.37	77.75	78.13	78.50	78.87	79.23	79.59	79.95	80.29
1.3	80.64	80.98	81.32	81.65	81.98	82.30	82.62	82.93	83.24	83.55
1.4	83.85	84.15	84.44	84.73	85.01	85.29	85.57	85.84	86.11	86.38
1.5	86.64	86.90	87.15	87.40	87.64	87.89	88.12	88.36	88.59	88.82
1.6	89.04	89.26	89.48	89.69	89.90	90.11	90.31	90.51	90.70	90.90
1.7	91.09	91.27	91.46	91.64	91.81	91.99	92.16	92.33	92.49	92.65
1.8	92.81	92.97	93.12	93.28	93.42	93.57	93.71	93.85	93.99	94.12
1.9	94.26	94.39	94.51	94.64	94.76	94.88	95.00	95.12	95.23	95.34

Anexo 26: Matriz con actividades identificadas en el Subproceso de "Alta de Usuarios".

Tiempo utilizado (días)	Tiempo utilizado (horas)	Recibir Notificación	Crear Siglas en ADM ABM Usuarios	Solicitar Usuario Modelo	Definir Usuario Modelo	Informar Permisos de Usuario a Aplicaciones	Crear usuario en AD (claves y correo)	Alta en Aplicaciones ARG	Alta en Aplicaciones ECU, permisos repositorios	Definir Equipos a asignar	Alta equipo en AD	Actualizar equipo en Inventario	Generar tarjeta acceso	Notificar asignación equipos	Asignar claves de marcación telefonía fija y Wi-Fi	Generar Clave de Conexión remota	Configurar equipos con Software	Configurar perfil usuario	Configurar Token y VPN	Configurar línea celular y aplicaciones	Entregar equipos y tarjeta de acceso	Notificar cierre y enviar reporte de equipos	Cerrar proceso de alta

Anexo 27: Matriz con actividades identificadas en el Subproceso de "Baja de Usuarios".

Iniciar proceso de baja en ABM	Bloquear Código de Usuario en ABM	Retirar equipos asignados	Entregar reporte de retiro de equipos	Respaldar información de usuario	Entregar respaldo a jefatura	Retirar tarjeta de acceso	Dar de baja en aplicaciones ECU	Dar de baja en aplicaciones ARG	Eliminar usuario en ABM	Eliminar manualmente de grupos y repositorios	Formatear equipo	Eliminar código equipo de la red	Bloquear claves de marcación telefónica y Wi-Fi	Bloquear clave de conexión remota	Retirar equipo celular	Dar de baja línea celular	Actualizar inventario de equipos	Cerrar el proceso de baja

Anexo 28: Unificación Registros con Matriz con actividades identificadas en el Subproceso de "Alta de Usuarios".

Ítem	Usuario	Tipo usuario	Cargo	Área	Básico Red, Correo, Lync, telefonía fija	Intermedio Internet, Intranet, Repositorio Información	Avanzado VPN, SAP, telefonía celular, aplicaciones ECU	Tiempo utilizado (horas)	Recibir Notificación	Crear Siglas en ADM ABM Usuarios	Solicitar Usuario Modelo	Definir Usuario Modelo	Informar Permisos de Usuario a Aplicaciones	Crear usuario en AD (claves y correo)	Alta en Aplicaciones ARG	Alta en Aplicaciones ECU, permisos repositorios	Definir Equipos a asignar	Alta equipo en AD	Actualizar equipo en Inventario	Generar tarjeta acceso	Notificar asignación equipos	Asignar claves de marcación telefonía fija y Wi-Fi	Generar Clave de Conexión remota	Configurar equipos con Software	Configurar perfil usuario	Configurar Token y VPN	Configurar línea celular y aplicaciones	Entregar equipos y tarjeta de acceso	Notificar cierre y enviar reporte de equipos	Cerrar proceso de alta
1	YTECHR	Externo	Auditor ARCH	Operaciones	X																									
2	YTEMAN	Externo	Auditor ARCH	Operaciones	X																									
7	YTEESC	Externo	Operador Security	Security	X																									
8	YTEMED	Externo	Medico	Seguridad y Salud	X																									
9	YTELGT	Externo	Medico	Seguridad y Salud	X																									
10	YTEJHH	Externo	Operador Security	Security	X																									
11	YTEGED	Externo	Operador Security	Security	X																									
12	YTEEIL	Externo	Medico	Seguridad y Salud	X																									
14	YTENEM	Externo	Auditor ARCH	Operaciones	X																									
15	YTEYAN	Externo	Analista SAS	Seguridad y Salud	X																									
20	YTEPAI	Externo	Medico	Seguridad y Salud	X																									
25	YTEAUV	Externo	Medico	Seguridad y Salud	X																									
26	YTEDIS	Externo	Medico	Seguridad y Salud	X																									
28	YTEXAV	Externo	Analista Químico	Operaciones	X																									
31	YTEJEN	Externo	Medico	Seguridad y Salud	X																									
42	YTEAMD	Externo	Auditor ARCH	Operaciones	X																									
43	YTEBAL	Externo	Operador Security	Security	X																									
44	YTECIS	Externo	Operador Security	Security	X																									
45	YTEIVA	Externo	Operador Security	Security	X																									

6	YTEFRH	Externo	Analista Sistemas	Sistemas		X																								
13	TECPED	Interno	Recorredor	Operaciones		X																								
18	TECBRA	Interno	Técnico de Mantenimiento	Mantenimiento		X																								
19	TECLOE	Pasante	Pasante	Planing		X																								
21	TECMLZ	Pasante	Pasante	Reservorios		X																								
22	TECCHB	Pasante	Pasante	Operaciones		X																								
23	TECLER	Pasante	Pasante	Operaciones		X																								
29	YTERIV	Externo	Analista Sistemas	Sistemas		X																								
30	TECGAK	Pasante	Pasante	Comercial		X																								
32	YTELIZ	Externo	Abogado	Planing		X																								
33	TECCAI	Pasante	Pasante	RRHH		X																								
36	YTEZAR	Externo	Coordinador Security	Security		X																								
40	YTEJIM	Externo	Coordinador Security	Security		X																								
41	YTEDAZ	Externo	Analista Sistemas	Sistemas		X																								
3	YTECHJ	Externo	Auditor PWC	Impuestos			X																							
4	YTEPPA	Externo	Auditor ARCH	Administración			X																							
5	YTEDOL	Externo	Auditor ARCH	Administración			X																							
16	YTEEDM	Externo	Company MAN	Producción			X																							
17	YTEAMO	Externo	Company MAN	Producción			X																							
24	YTESPM	Externo	Analista RRHH	Recursos Humanos			X																							
27	TECDAN	Interno	Analista Financiera	Administración			X																							
34	YTEKLO	Externo	Analista Funcional	Impuestos			X																							
35	YTEPPA	Externo	Auditor ARCH	Administración			X																							
37	TECZUM	Interno	Analista Comercial	Comercial			X																							
38	YTERUX	Externo	Auditor PWC	Impuestos			X																							

39	YTEVEC	Externo	Analista Sistemas	Impuestos			X																						
46	YTEFMA	Externo	Analista Sistemas	Impuestos			X																						
47	TECCIB	Interno	Ingeniero Reservorios	Reservorios			X																						

Ítem	Usuario	Tipo usuario	Cargo	Área	Básico Red, Correo, Lync, telefonía fija	Intermedio Internet, Intranet, Repositorio Información	Avanzado VPN, SAP, telefonía celular, aplicaciones ECU	Tiempo utilizado (horas)	Recibir Notificación	Crear Siglas en ADM ABM Usuarios	Validar Matriz de Perfiles de Usuario	Definir Usuario Modelo	Informar Permisos de Usuario a Aplicaciones	Crear usuario en AD (claves y correo)	Asignar Permisos Aplicaciones ARG	Alta en Aplicaciones ECU, permisos repositorios	Definir Equipos a asignar	Alta equipo en AD	Actualizar equipo en Inventario	Generar tarjeta acceso	Notificar asignación equipos	Asignar claves de marcación telefonía fija y Wi-Fi	Generar Clave de Conexión remota	Configurar equipos con Software	Configurar perfil usuario	Configurar Token y VPN	Configurar línea celular y aplicaciones	Entregar equipos y tarjeta de acceso	Notificar cierre y enviar reporte de equipos	Cerrar proceso de alta
48	YTESOU	Externo	Auditor ARCH	Operaciones	X																								
59	YTEYUJ	Externo	Medico	Seguridad y Salud	X																								
61	YTEMAR	Externo	Medico	Seguridad y Salud	X																								
50	TECGAE	Interno	Técnico de Mantenimiento	Mantenimiento		X																							
52	YTEPRO	Externo	Coordinador Security	Security		X																							
53	TECKFR	Pasante	Pasante	Operaciones		X																							
54	TECDCE	Pasante	Pasante	Reservorios		X																							
55	TECDML	Pasante	Pasante	Operaciones		X																							
57	YTEADN	Externo	Abogado	Administración		X																							
60	TECJIM	Interno	Recorredor	Operaciones		X																							
49	YTERUX	Externo	Auditor PWC	Impuestos			X																						
51	YTEEVE	Externo	Analista Impuestos	Impuestos			X																						
56	YTEOLG	Externo	Analista Sistemas	Impuestos			X																						
58	TECWAL	Pasante	Pasante	RRHH			X																						

Anexo 29: Unificación Registros con Matriz con actividades identificadas en el Subproceso de "Baja de Usuarios".

Ítem	Usuario	Tipo de Usuario	Básico (Red, Correo, Lync, telefonía fija)	Intermedio (Internet, Intranet, Repositorios Información)	Avanzado (VPN, SAP, telefonía celular, aplicaciones ECU, Repositorios ECU VIP)	Área	Cargo	Tiempo utilizado (horas)	Iniciar proceso de baja en ABM	Bloquear Codigo de Usuario en ABM	Retirar equipos asignados	Entregar reporte de retiro de equipos	Respaldar información de usuario	Entregar respaldo a jefatura	Retirar tarjeta de acceso	Dar de baja en aplicaciones ECU	Dar de baja en aplicaciones ARG	Eliminar usuario en ABM	Eliminar manualmente de grupos y repositorios	Formatear equipo	Eliminar codigo equipo de la red	Bloquear claves de marcación telefónica y Wi-Fi	Bloquear clave de conexión remota	Retirar equipo celular	Dar de baja línea celular	Actualizar inventario de equipos	Cerrar el proceso de baja
7	TECRRV	Interno	X			Operaciones	Ayudante Tareas Generales																				
9	YTECPU	Externo	X			Sistemas	Analista de Sistemas																				
10	YTEJCC	Externo	X			Seguridad y Salud	Medico																				
11	TECCEF	Interno	X			Operaciones	Recorredor																				
12	TECMRP	Interno	X			Mantenimiento	Técnico de Mantenimiento																				
13	YTEAUW	Externo	X			Operaciones	Ingeniero de Producción																				
14	YTESIL	Externo	X			Impuestos	Analista de Impuestos																				
15	YTEAYJ	Externo	X			Facilidades	Ingeniero de Facilidades																				
16	YTEDMO	Externo	X			Operaciones	Auditor ARCH																				
19	YTECZM	Externo	X			Security	Operador																				
20	YTEZUP	Externo	X			Planing	Abogada																				
21	YTEAMC	Externo	X			Impuestos	Analista de Impuestos																				
23	YTEDML	Externo	X			Operaciones	Auditor ARCH																				
24	YTEJCV	Externo	X			Operaciones	Auditor ARCH																				
26	YTEIPA	Externo	X			Seguridad y Salud	Medico																				
27	YTESIJ	Externo	X			Operaciones	Auditor ARCH																				
28	TECPLU	Pasante	X			Perforación	Pasante																				
29	TECKAT	Pasante	X			Operaciones	Pasante																				
30	TECLBR	Pasante	X			Operaciones	Pasante																				
31	TECLCH	Pasante	X			Operaciones	Pasante																				
33	TECDLE	Interno	X			Operaciones	Recorredor																				

34	YTELCM	Externo	X			Impuestos	Analista de Impuestos																			
37	YTEHHV	Externo	X			Seguridad y Salud	Analista de Seguridad																			
38	YTEJUN	Externo	X			Seguridad y Salud	Analista de Seguridad																			
39	YTEMED	Externo	X			Seguridad y Salud	Medico																			
40	YTEJHH	Externo	X			Security	Operador																			
41	YTEXAV	Externo	X			Operaciones	Analista Químico																			
42	YTEMAN	Externo	X			Operaciones	Auditor ARCH																			
43	TECMMQ	Interno	X			Operaciones	Recorredor																			
44	YTESAG	Externo	X			Operaciones	Auditora ARCH																			
51	YTEPDA	Interno	X			Operaciones	Genérico																			
52	TECP26	Interno	X			Operaciones	Genérico																			
56	YTECHR	Externo	X			Operaciones	Auditora ARCH																			
4	TECLUI	Interno		X		Operaciones	Ingeniero de Procesos																			
6	TECSKA	Interno		X		Seguridad y Salud	Analista de Seguridad																			
17	TECLOU	Pasante		X		Gerencia	Asistente de Gerencia																			
22	TECRIT	Interno		X		Reservorios	Ingeniero Reservorios																			
45	TECLOE	Pasante		X		Planing	Pasante																			
46	TECDYA	Interno		X		Operaciones	Analista Comercial																			
47	YTEJAT	Externo		X		Security	Coordinador Security																			
48	TECLIZ	Pasante		X		Comercial	Abogada																			
49	TECJCU	Interno		X		Security	Coordinador Security																			
53	TECPMP	Interno		X		Operaciones	Pasante																			
54	YTEPMC	Externo		X		Operaciones	Pasante																			
58	YTEPGT	Externo		X		Sistemas	Analista Sistemas																			
1	TECCIB	Interno			X	Reservorios	Ingeniero Reservorios																			
2	TECAAC	Interno			X	Perforación	Company Man																			
3	TECEME	Interno			X	Perforación	Company Man																			
5	TECCVV	Interno			X	Abastecimientos	Analista de Compras																			
8	TECIRM	Interno			X	Sistemas	Coordinador Sistemas																			
18	TECMSC	Interno			X	Abastecimientos	Bodeguero																			

25	YTEKLO	Externo			X	Impuestos	Analista Funcional																			
32	YTEDOL	Externo			X	Administración	Auditor ARCH																			
35	YTEPPA	Externo			X	Administración	Auditor ARCH																			
36	YTECHJ	Externo			X	Administración	Analista de Contabilidad																			
50	YTEKAT	Externo			X	Sistemas	Analista Sistemas																			
55	TECDAV	Interno			X	Operaciones	Supervisor Producción																			
57	TECJIR	Interno			X	Comercial	Analista Comercial																			

Ítem	Usuario	Tipo de Usuario	Código Tipo de Usuario	Básico (Red, Correo, Lync, telefonía fija)	Intermedio (Internet, Intranet, Repositorios Información)	Avanzado (VPN, SAP, telefonía celular, aplicaciones ECU, Repositorios ECU VIP)	Área	Cargo	Tiempo utilizado (horas)	Iniciar proceso de baja en ABM	Validar permisos vigentes en Matriz de usuarios	Bloquear Código de Usuario en ABM	Retirar equipos asignados	Firmar planilla retiro equipos	Respaldar información de usuario	Entregar respaldo a jefatura	Retirar tarjeta de acceso	Dar de baja en aplicaciones y repositorio acorde a matriz	Dar de baja en aplicaciones ARG	Eliminar usuario en ABM	Formatear equipo	Eliminar codigo equipo de la red	Bloquear claves de marcación telefónica y Wi-Fi	Bloquear clave de conexión remota	Retirar equipo celular	Dar de baja línea celular	Actualizar inventario de equipos	Cerrar el proceso de baja
65	TECEFN	Interno	1	X			Operaciones	Operador																			
79	YTEAUV	Interno	1	X			Seguridad y Salud	Medico																			
75	YTEEIL	Externo	1	X			Seguridad y Salud	Medico																			
76	YTEPAI	Externo	1	X			Seguridad y Salud	Medico																			
77	YTECCL	Externo	1	X			Administración	Abogado																			
59	YTEJIM	Externo	2		X		Security	Coordinador Security																			
60	TECCHB	Pasante	2		X		Operaciones	Pasante																			
61	TECLER	Pasante	2		X		Operaciones	Pasante																			
62	TECMLZ	Pasante	2		X		Reservorios	Pasante																			
64	TECALB	Interno	2		X		Operaciones	Jóven Profesional																			
66	YTERIV	Externo	2		X		Sistemas	Analista Sistemas																			
80	TECGAK	Pasante	2		X		Planing	Pasante																			
78	TECCAI	Pasante	2		X		RRHH	Pasante																			
73	YTEPPA	Externo	2		X		Administración	Auditor ARCH																			
72	TECJIM	Interno	2		X		Operaciones	Recorredor																			
63	YTEVEC	Externo	3			X	Sistemas	Analista Sistemas																			
67	YTEAMO	Externo	3			X	Producción	Company Man																			

68	YTEEDM	Externo	3			X	Producción	Company Man																			
74	YTERUX	Externo	3			X	Impuestos	Auditor PWC																			
71	TECDAN	Interno	3			X	Administración	Analista Financiera																			
70	TECGCP	Interno	3			X	Facilidades	Ingeniero de Mejora																			
69	TECGAC	Interno	3			X	RRHH	Coordinadora RRHH																			

Anexo 30: Matriz de registro de Tiempos para el subproceso Alta de Usuarios.

Ítem	Usuario	Tipo usuario	Cargo	Área	Básico Red, Correo, Lync, telefonía fija	Intermedio Internet, Intranet, Repositorio Información	Avanzado VPN, SAP, telefonía celular, aplicaciones ECU	Tiempo utilizado (horas)	Recibir Notificación	Crear Siglas en ADM ABM Usuarios	Solicitar Usuario Modelo	Definir Usuario Modelo	Informar Permisos de Usuario a Aplicaciones	Crear usuario en AD (claves y correo)	Alta en Aplicaciones ARG	Alta en Aplicaciones ECU, permisos repositorios	Definir Equipos a asignar	Alta equipo en AD	Actualizar equipo en Inventario	Generar tarjeta acceso	Notificar asignación equipos	Asignar claves de marcación telefonía fija y Wi-Fi	Generar Clave de Conexión remota	Configurar equipos con Software	Configurar perfil usuario	Configurar Token y VPN	Configurar línea celular y aplicaciones	Entregar equipos y tarjeta de acceso	Notificar cierre y enviar reporte de equipos	Cerrar proceso de alta
1	YTECHR	Externo	Auditor ARCH	Operaciones	X			29	10	67	149	507	230	49		326	126	8	8	28	12	14	0	135	27	0	0	0	15	11
2	YTEMAN	Externo	Auditor ARCH	Operaciones	X			29	9	70	132	507	230	45		326	117	9	10	13	10	19	0	131	27	0	0	0	13	14
7	YTEESC	Externo	Operador Security	Security	X			20	8	69	121	310	126	34		130	115	13	8	0	8	10	0	133	23	0	0	12	12	17
8	YTEMED	Externo	Medico	Seguridad y Salud	X			19	9	61	127	296	73	49		143	120	12	10	0	13	11	0	112	21	0	0	12	11	18
9	YTELGT	Externo	Medico	Seguridad y Salud	X			20	8	64	159	365	63	52		120	118	9	9	0	11	13	0	117	18	0	0	11	12	11
10	YTEJHH	Externo	Operador Security	Security	X			21	9	70	197	290	105	49		181	118	12	9	0	5	20	0	104	25	0	0	13	13	10
11	YTEGED	Externo	Operador Security	Security	X			21	10	61	185	337	107	48		147	119	13	9	0	14	13	0	136	22	0	0	12	15	11
12	YTEEIL	Externo	Medico	Seguridad y Salud	X			21	8	67	167	352	87	46		131	129	11	10	0	5	16	0	138	23	0	0	13	12	9
14	YTENEM	Externo	Auditor ARCH	Operaciones	X			21	9	62	164	299	106	41		179	125	10	8	0	8	10	0	133	25	0	0	12	15	10
15	YTEYAN	Externo	Analista SAS	Seguridad y Salud	X			20	9	69	120	338	102	44		127	112	11	8	22	12	23	0	121	23	0	0	14	10	16
20	YTEPAI	Externo	Medico	Seguridad y Salud	X			21	9	64	163	359	78	48		158	120	13	10	0	10	17	0	139	16	0	0	12	16	9
25	YTEAUV	Externo	Medico	Seguridad y Salud	X			22	10	65	201	347	108	35		182	112	12	10	0	12	18	0	117	22	0	0	15	16	8
26	YTEDIS	Externo	Medico	Seguridad y Salud	X			21	9	70	122	365	131	49		152	113	11	9	0	7	10	0	102	24	0	0	15	11	12
28	YTEXAV	Externo	Analista Químico	Operaciones	X			20	8	67	132	285	78	48		175	132	12	9	0	5	15	0	122	15	0	0	14	10	17
31	YTEJEN	Externo	Medico	Seguridad y Salud	X			20	8	68	156	377	51	42		146	117	9	10	0	15	13	0	104	22	0	0	14	13	11
42	YTEAMD	Externo	Auditor ARCH	Operaciones	X			18	10	69	198	206	45	34		176	108	8	9	0	6	11	0	111	17	0	0	13	10	9
43	YTEBAL	Externo	Operador Security	Security	X			19	10	68	185	225	91	45		162	116	12	8	0	11	21	0	130	26	0	0	11	11	8
44	YTECIS	Externo	Operador Security	Security	X			17	8	63	148	178	59	36		123	119	13	10	0	13	23	0	136	18	0	0	13	16	17
45	YTEIVA	Externo	Operador Security	Security	X			19	9	68	175	159	79	47		192	125	8	11	0	11	20	0	115	27	0	0	16	16	14
								Media	8,95	66,42	157,95	321,16	102,58	44,26		172,42	119,00	10,84	9,21	21,00	9,89	15,63	0,00	122,95	22,16	0,00	0,00	11,68	13,00	12,21

								Desviación Estándar	0,78	3,08	27,35	92,03	50,75	5,69		58,45	6,16	1,83	0,92	8,26	3,18	4,45	0,00	12,57	3,79	0,00	0,00	4,33	2,24	3,38
								Coeficiente de Variación Tipo 1	8,72%	4,64%	17,32%	28,66%	49,47%	12,87%	0,00%	33,90%	5,17%	16,91%	9,96%	39,33%	32,12%	28,47%	0,00%	10,23%	17,10%	0,00%	0,00%	37,09%	17,20%	27,65%
								Suma	170	1262	3001	6102	1949	841	0	3276	2261	206	175	63	188	297	0	2336	421	0	0	222	247	232
								Porcentaje	0,73	5,43	12,91	26,25	8,38	3,62	0,00	14,09	9,73	0,89	0,75	0,27	0,81	1,28	0,00	10,05	1,81	0,00	0,00	0,95	1,06	1,00
6	YTEFRH	Externo	Analista Sistemas	Sistemas		X		23	10	63	132	453	98	51		152	113	10	10	15	14	19	0	129	25	0	0	14	12	17
13	TECPED	Interno	Recorredor	Operaciones		X		23	8	67	189	445	73	40		162	125	12	9	0	14	18	0	129	24	0	0	15	14	15
18	TECBRA	Interno	Técnico de Mantenimiento	Mantenimiento		X		23	10	61	136	500	82	34		170	130	8	9	0	13	23	0	123	15	0	0	19	12	16
19	TECLOE	Pasante	Pasante	Planing		X		23	8	67	180	450	113	41		137	129	10	8	15	14	20	0	112	17	0	0	14	11	9
21	TECMLZ	Pasante	Pasante	Reservorios		X		23	10	61	174	511	71	38		140	111	10	10	14	13	9	0	126	19	0	0	16	11	8
22	TECCHB	Pasante	Pasante	Operaciones		X		24	10	67	199	478	124	38		164	109	12	9	25	15	9	0	116	16	0	0	14	12	10
23	TECLER	Pasante	Pasante	Operaciones		X		23	10	66	123	503	94	34		138	124	8	10	17	7	18	0	118	26	0	0	18	12	10
29	YTERIV	Externo	Analista Sistemas	Sistemas		X		24	10	70	123	523	95	52		164	111	10	9	26	15	20	0	124	18	0	0	16	16	9
30	TECGAK	Pasante	Pasante	Comercial		X		23	9	67	170	461	75	35		158	122	8	8	13	8	13	0	105	22	0	0	17	16	15
32	YTELIZ	Externo	Abogado	Planing		X		22	8	62	186	466	94	39		123	108	9	10	26	6	11	0	115	17	0	0	12	16	9
33	TECCAI	Pasante	Pasante	RRHH		X		24	9	62	156	459	118	43		195	116	13	10	21	6	12	0	101	19	0	0	20	14	15
36	YTEZAR	Externo	Coordinador Security	Security		X		24	9	67	177	509	53	36		175	121	9	11	0	12	16	0	140	18	0	0	14	11	15
40	YTEJIM	Externo	Coordinador Security	Security		X		24	10	68	166	463	135	50		193	113	10	11	0	5	11	0	134	21	0	0	14	10	17
41	YTEDAZ	Externo	Analista Sistemas	Sistemas		X		23	8	69	197	474	45	33		126	112	9	8	28	15	16	0	118	24	0	0	16	16	16
								Media	9,21	65,50	164,86	478,21	90,71	40,29		156,93	117,43	9,86	9,43	14,29	11,21	15,36	0,00	120,71	20,07	0,00	0,00	15,64	13,07	12,93
								Desviación Estándar	0,89	3,06	26,62	25,89	26,23	6,47		22,44	7,54	1,56	1,02	10,56	3,87	4,52	0,00	10,78	3,58	0,00	0,00	2,24	2,20	3,47
								Coeficiente	9,69%	4,67%	16,15%	5,41%	28,91%	16,07%	0,00%	14,30%	6,42%	15,85%	10,78%	73,90%	34,48%	29,41%	0,00%	8,93%	17,85%	0,00%	0,00%	14,32%	16,83%	26,87%

								de Variación Tipo 2																				
								Suma	129	917	2308	6695	1270	564	0	2197	1644	138	132	200	157	215	0	1690	281	0	0	219	183	181
								Porcentaje	0,67	4,80	12,07	35,02	6,64	2,95	0,00	11,49	8,60	0,72	0,69	1,05	0,82	1,12	0,00	8,84	1,47	0,00	0,00	1,15	0,96	0,95
3	YTECHJ	Externo	Auditor PWC	Impuestos			X	36	10	63	173	497	80	51	760	158	110	10	10	21	12	23	0	118	24	0	0	0	11	18
4	YTEPPA	Externo	Auditor ARCH	Administración			X	56	8	68	168	475	74	46	1939	162	128	8	9	29	14	20	0	101	26	0	0	22	10	18
5	YTEDOL	Externo	Auditor ARCH	Administración			X	56	8	68	168	475	74	46	1939	162	0	0	0	29	0	20	0	0	0	0	0	0	10	18
16	YTEEDM	Externo	Company MAN	Producción			X	76	9	68	188	452	121	46	3121	159	132	12	9	0	10	18	0	113	17	0	0	13	12	10
17	YTEAMO	Externo	Company MAN	Producción			X	76	9	68	188	452	121	46	3121	159	132	12	9	0	10	18	0	113	17	0	0	15	12	10
24	YTESPM	Externo	Analista RRHH	Recursos Humanos			X	71	10	69	176	524	86	34	2640	185	0	0	0	0	0	0	212	173	40	50	0	0	15	16
27	TECDAN	Interno	Analista Financiera	Administración			X	39	8	61	153	486	56	34	777	168	114	13	8	18	14	23	156	115	22	31	0	16	13	8
34	YTEKLO	Externo	Analista Funcional	Impuestos			X	38	10	63	167	466	129	45	478	176	0	0	0	0	0	0	432	71	21	175	0	0	10	14
35	YTEPPA	Externo	Auditor ARCH	Administración			X	56	9	70	193	486	131	39	1832	179	132	10	10	28	14	10	0	138	15	0	0	19	10	10
37	TECZUM	Interno	Analista Comercial	Comercial			X	69	9	61	187	483	136	39	2532	152	115	9	8	28	11	12	137	102	16	45	0	17	12	10
38	YTERUX	Externo	Auditor PWC	Impuestos			X	31	9	61	146	485	118	33	411	185	112	12	10	31	9	14	0	139	18	0	0	22	14	16
39	YTEVEC	Externo	Analista Sistemas	Impuestos			X	65	10	65	127	448	62	47	1937	160	0	0	0	0	0	0	756	119	22	99	0	0	14	14
46	YTEFMA	Externo	Analista Sistemas	Impuestos			X	24	10	66	45	221	41	44	387	98	0	0	0	0	0	0	218	116	26	88	0	11	11	10
47	TECCIB	Interno	Ingeniero Reservorios	Reservorios			X	33	8	67	152	463	81	40	560	187	117	8	11	17	9	19	20	105	25	0	0	12	13	18
								Media	9,07	65,57	159,36	458,07	93,57	42,14	1602,43	163,57	78,00	6,71	6,00	14,36	7,36	12,64	137,93	108,79	20,64	34,86	0,00	10,50	11,93	13,57
								Desviación Estándar	0,83	3,20	37,83	71,15	31,50	5,64	1022,17	22,19	60,79	5,40	4,71	13,53	5,93	9,07	219,75	38,82	8,68	53,09	0,00	8,72	1,69	3,78
								Coeficiente de Variación Tipo 3	9,14%	4,89%	23,74%	15,53%	33,66%	13,39%	63,79%	13,57%	77,93%	80,40%	78,45%	94,23%	80,61%	71,73%	159,32%	35,68%	42,04%	152,32%	0,00%	83,09%	14,13%	27,83%
								Suma	127	918	2231	6413	1310	590	22434	2290	1092	94	84	201	103	177	1931	1523	289	488	0	147	167	190
								Porcentaje	0,30	2,14	5,21	14,98	3,06	1,38	52,42	5,35	2,55	0,22	0,20	0,47	0,24	0,41	4,51	3,56	0,68	1,14	0,00	0,34	0,39	0,44

Ítem	Usuario	Tipo usuario	Cargo	Área	Básico Red, Correo, Lync, telefonía fija	Intermedio Internet, Intranet, Repositorio Información	Avanzado VPN, SAP, telefonía celular, aplicaciones ECU	Tiempo utilizado (horas)	Recibir Notificación	Crear Siglas en ADM ABM Usuarios	Validar Matriz de Perfiles de Usuario	Definir Usuario Modelo	Informar Permisos de Usuario a Aplicaciones	Crear usuario en AD (claves y correo)	Asignar Permisos Aplicaciones ARG	Alta en Aplicaciones ECU, permisos repositorios	Definir Equipos a asignar	Alta equipo en AD	Actualizar equipo en Inventario	Generar tarjeta acceso	Notificar asignación equipos	Asignar claves de marcación telefonía fija y Wi-Fi	Generar Clave de Conexión remota	Configurar equipos con Software	Configurar perfil usuario	Configurar Token y VPN	Configurar línea celular y aplicaciones	Entregar equipos y tarjeta de acceso	Notificar cierre y enviar reporte de equipos	Cerrar proceso de alta
48	YTESOU	Externo	Auditor ARCH	Operaciones	X			6	12	55	9	0	9	38		20	11	9	7	0	9	9	0	119	19	0	0	11	9	11
59	YTEYUJ	Externo	Medico	Seguridad y Salud	X			6	11	75	10	0	8	27		19	10	8	8	0	10	8	0	108	18	0	0	9	9	10
61	YTEMAR	Externo	Medico	Seguridad y Salud	X			6	11	74	10	0	11	28		14	10	10	9	0	10	9	0	117	19	0	0	10	8	10
								Media	11,33	68,00	9,67	0,00	9,33	31,00	0,00	17,67	10,33	9,00	8,00	0,00	9,67	8,67	0,00	114,67	18,67	0,00	0,00	10,00	8,67	10,33
								Desviación Estándar	0,58	11,27	0,58	0,00	1,53	6,08	0,00	3,21	0,58	1,00	1,00	0,00	0,58	0,58	0,00	5,86	0,58	0,00	0,00	1,00	0,58	0,58
								Coeficiente de Variación Tipo 1	5,09%	16,57%	5,97%	0,00%	16,37%	19,62%	0,00%	18,20%	5,59%	11,11%	12,50%	0,00%	5,97%	6,66%	0,00%	5,11%	3,09%	0,00%	0,00%	10,00%	6,66%	5,59%
								Suma	34	204	29	0	28	93	0	53	31	27	24	0	29	26	0	344	56	0	0	30	26	31
								Porcentaje	3,19	19,15	2,72	0,00	2,63	8,73	0,00	4,98	2,91	2,54	2,25	0,00	2,72	2,44	0,00	32,30	5,26	0,00	0,00	2,82	2,44	2,91
50	TECGAE	Interno	Técnico de Mantenimiento	Mantenimiento		X		6	8	60	10	0	10	23		16	9	8	8	0	8	9	0	124	25	0	0	8	8	10
52	YTEPRO	Externo	Coordinador Security	Security		X		6	9	50	10	0	10	34		19	9	10	9	0	8	8	0	100	21	0	0	8	9	8
53	TECKFR	Pasante	Pasante	Operaciones		X		7	10	69	9	0	9	29		13	11	9	10	20	8	10	0	104	24	0	0	9	9	8
54	TECDCE	Pasante	Pasante	Reservorios		X		7	11	67	10	0	10	21		21	10	8	10	20	9	9	0	121	19	0	0	9	10	8
55	TECDML	Pasante	Pasante	Operaciones		X		6	10	54	9	0	10	41		16	9	9	8	20	10	8	0	110	20	0	0	8	8	8
57	YTEADN	Externo	Abogado	Administración		X		7	9	63	9	0	10	35		21	10	8	10	20	10	9	0	101	25	0	0	10	8	8
60	TECJIM	Interno	Recorredor	Operaciones		X		6	12	57	9	0	8	38		17	11	10	8	0	9	10	0	110	21	0	0	9	10	9
								Media	9,86	60,00	9,43	0,00	9,57	31,57	0,00	17,57	9,86	8,86	9,00	11,43	8,86	9,00	0,00	110,00	22,14	0,00	0,00	8,71	8,86	8,43
								Desviación Estándar	1,35	6,88	0,53	0,00	0,79	7,52	0,00	2,94	0,90	0,90	1,00	10,69	0,90	0,82	0,00	9,43	2,48	0,00	0,00	0,76	0,90	0,79
								Coeficiente de Variación Tipo 2	13,65%	11,47%	5,67%	0,00%	8,22%	23,83%	0,00%	16,71%	9,13%	10,16%	11,11%	0,00%	10,16%	9,07%	0,00%	8,58%	11,19%	0,00%	0,00%	8,67%	10,16%	9,33%
								Suma	69	420	66	0	67	221	0	123	69	62	63	80	62	63	0	770	155	0	0	61	62	59
								Porcentaje	2,79	16,99	2,67	0,00	2,71	8,94	0,00	4,98	2,79	2,51	2,55	3,24	2,51	2,55	0,00	31,15	6,27	0,00	0,00	2,47	2,51	2,39

49	YTERUX	Externo	Auditor PWC	Impuestos			X	15	9	69	10	0	10	33	521	17	9	8	10	20	9	8	0	116	20	0	0	8	10	8
51	YTEEVE	Externo	Analista Impuestos	Impuestos			X	16	8	74	11	0	8	43	512	17	9	10	10	20	10	8	0	122	17	0	0	9	10	8
56	YTEOLG	Externo	Analista Sistemas	Impuestos			X	16	8	75	10	0	8	36	659	18	0	0	0	0	0	0	20	50	24	10	0	0	8	9
58	TECWAL	Pasante	Pasante	RRHH			X	20	12	57	11	0	8	37	825	19	11	8	8	20	10	9	0	108	22	0	0	8	10	10
								Media	9,25	68,75	10,50	0,00	8,50	37,25	629,25	17,75	7,25	6,50	7,00	15,00	7,25	6,25	5,00	99,00	20,75	2,50	0,00	6,25	9,50	8,75
								Desviación Estándar	1,89	8,26	0,58	0,00	1,00	4,19	146,82	0,96	4,92	4,43	4,76	10,00	4,86	4,19	10,00	33,17	2,99	5,00	0,00	4,19	1,00	0,96
								Coeficiente de Variación Tipo 3	20,46%	12,02%	5,50%	0,00%	11,76%	11,26%	0,00%	5,39%	67,92%	68,23%	68,01%	0,00%	66,98%	67,09%	0,00%	33,50%	14,39%	0,00%	0,00%	67,09%	10,53%	10,94%
								Suma	37	275	42	0	34	149	2517	71	29	26	28	60	29	25	20	396	83	10	0	25	38	35
								Porcentaje	0,94	7,00	1,07	0,00	0,87	3,79	64,06	1,81	0,74	0,66	0,71	1,53	0,74	0,64	0,51	10,08	2,11	0,25	0,00	0,64	0,97	0,89

Anexo 31: Matriz de registro de Tiempos para el subproceso Baja de Usuarios.

Ítem	Usuario	Tipo de Usuario	Básico (Red, Correo, Lync, telefonía fija)	Intermedio (Internet, Intranet, Repositorios Información)	Avanzado (VPN, SAP, telefonía celular, aplicaciones ECU, Repositorios ECU VIP)	Área	Cargo	Tiempo utilizado (horas)	Iniciar proceso de baja en ABM		Bloquear Codigo de Usuario en ABM	Retirar equipos asignados	Entregar reporte de retiro de equipos	Respaldar información de usuario	Entregar respaldo a jefatura	Retirar tarjeta de acceso	Dar de baja en aplicaciones ECU	Dar de baja en aplicaciones ARG	Eliminar usuario en ABM	Eliminar manualmente de grupos y repositorios	Formatear equipo	Eliminar codigo equipo de la red	Bloquear claves de marcación telefónica y Wi-Fi	Bloquear clave de conexión remota	Retirar equipo celular	Dar de baja línea celular	Actualizar inventario de equipos	Cerrar el proceso de baja
7	TECRRV	Interno	X			Operaciones	Ayudante Tareas Generales	5	5		8	12	10	66	8		27		8	28	47	8	9				13	6
9	YTECPU	Externo	X			Sistemas	Analista de Sistemas	8	4		8	16	9	73	9		26		8	195	47	8	9				13	5
10	YTEJCC	Externo	X			Seguridad y Salud	Medico	6	6		7	17	9	61	8		29		7	73	61	7	7				13	6
11	TECCEF	Interno	X			Operaciones	Recorredor	4	6		7	17	11	43	11		19		7	31	53	7	7				13	4
12	TECMRP	Interno	X			Mantenimiento	Técnico de Mantenimiento	4	4		8	15	11	38	8		19		8	37	53	8	6				17	6
13	YTEAUW	Externo	X			Operaciones	Ingeniero de Producción	7	6		9	16	12	96	11		28		9	94	55	9	7				13	6
14	YTESIL	Externo	X			Impuestos	Analista de Impuestos	5	5		9	14	10	44	8		20		9	68	48	9	6				13	6
15	YTEAYJ	Externo	X			Facilidades	Ingeniero de Facilidades	6	4		8	15	10	112	7		23		8	59	53	8	7				13	6
16	YTEDMO	Externo	X			Operaciones	Auditor ARCH	5	4		9	17	11	53	11		21		9	58	54	9	7				11	6
19	YTECZM	Externo	X			Security	Operador	4	4		9	14	10	30	7		25		9	32	58	9	7				13	5
20	YTEZUP	Externo	X			Planing	Abogada	6	6		8	12	12	66	10	4	25		8	92	57	8	8				17	6
21	YTEAMC	Externo	X			Impuestos	Analista de Impuestos	6	5		8	15	9	47	7		22		8	125	55	8	8				16	6
23	YTEDML	Externo	X			Operaciones	Auditor ARCH	6	5		7	17	8	51	8		23		7	117	55	7	9				14	6
24	YTEJCV	Externo	X			Operaciones	Auditor ARCH	6	6		7	16	12	38	7		19		7	135	48	7	6				11	5
26	YTEIPA	Externo	X			Seguridad y Salud	Medico	5	4		8	15	11	35	8		24		8	45	51	8	7				16	5
27	YTESIJ	Externo	X			Operaciones	Auditor ARCH	5	5		9	17	11	42	10		29		9	78	54	9	6				13	6
28	TECPLU	Pasante	X			Perforación	Pasante	5	4		7	16	8	70	9	5	27		7	39	58	7	8				17	5
29	TECKAT	Pasante	X			Operaciones	Pasante	5	5		9	15	12	42	8	5	20		9	44	49	9	7				17	4
30	TECLBR	Pasante	X			Operaciones	Pasante	5	6		8	13	8	45	8	4	25		8	42	58	8	7				12	6
31	TECLCH	Pasante	X			Operaciones	Pasante	5	6		9	16	12	49	9	5	26		9	48	54	9	7				16	5
33	TECDLE	Interno	X			Operaciones	Recorredor	4	5		8	15	11	21	7	5	24		8	26	53	8	9				16	4

34	YTELCM	Externo	X			Impuestos	Analista de Impuestos	5	4		8	15	12	48	8		22		8	55	55	8	9				17	6
37	YTEHHV	Externo	X			Seguridad y Salud	Analista de Seguridad	4	5		7	13	10	25	10		24		7	23	49	7	6				15	5
38	YTEJUN	Externo	X			Seguridad y Salud	Analista de Seguridad	4	6		7	15	10	28	8		19		7	23	53	7	8				16	6
39	YTEMED	Externo	X			Seguridad y Salud	Medico	4	5		9	13	12	18	11		19		9	14	58	9	9				13	6
40	YTEJHH	Externo	X			Security	Operador	4	6		9	14	10	34	9		29		9	29	54	9	6				12	5
41	YTEXAV	Externo	X			Operaciones	Analista Químico	5	4		8	13	12	49	11		23		8	57	61	8	6				17	4
42	YTEMAN	Externo	X			Operaciones	Auditor ARCH	5	6		7	14	9	37	11		29		7	62	58	7	6				13	6
43	TECMMQ	Interno	X			Operaciones	Recorredor	4	7		8	14	12	31	11		20		8	31	61	8	8				15	6
44	YTESAG	Externo	X			Operaciones	Auditora ARCH	4	6		8	13	8	27	11		27		8	34	49	8	9				11	6
51	YTEPDA	Interno	X			Operaciones	Genérico	4	4		9	14	8		8		24		9	28	56	9	8				11	6
52	TECP26	Interno	X			Operaciones	Genérico	4	5		8	12	9		11		25		8	36	57	8	9				17	5
56	YTECHR	Externo	X			Operaciones	Auditora ARCH	5	5		9	12	12	40	10	4	29		9	42	59	9	8				13	6
								Media	5,09	0,00	8,09	14,61	10,33	47,06	9,03	4,57	23,97	0,00	8,09	57,58	54,27	8,09	7,45	0,00	0,00	0,00	14,15	5,48
								Desviación estándar	0,88	0,00	0,77	1,60	1,45	20,67	1,49	0,53	3,41	0,00	0,77	39,09	4,09	0,77	1,12	0,00	0,00	0,00	2,09	0,71
								Coeficiente de variación Tipo 1	17,27%	0,00%	9,46%	10,95%	14,04%	43,92%	16,49%	11,69%	14,24%	0,00%	9,46%	67,89%	7,53%	9,46%	15,03%	0,00%	0,00%	0,00%	14,79%	12,99%
								Suma	168,00	-	267,00	482,00	341,00	1.459,00	298,00	32,00	791,00	-	267,00	1.900,00	1.791,00	267,00	246,00	-	-	-	467,00	181,00
								Porcentaje	1,88	-	2,98	5,38	3,81	16,29	3,33	0,36	8,83	-	2,98	21,21	20,00	2,98	2,75	-	-	-	5,21	2,02
4	TECLUI	Interno		X		Operaciones	Ingeniero de Procesos	10	4		7	14	8	92	10	5	18	102	7	218	56	7	9				17	4
6	TECSKA	Interno		X		Seguridad y Salud	Analista de Seguridad	11	6		8	17	12	128	10	4	24	114	8	208	52	8	6	7			11	4
17	TECLOU	Pasante		X		Gerencia	Asistente de Gerencia	10	6		8	14	10	138	11	4	22	94	8	142	58	8	7				11	4
22	TECRIT	Interno		X		Reservorios	Ingeniero Reservorios	9	4		7	13	11	113	10		23	91	7	146	56	7	8				13	4
45	TECLOE	Pasante		X		Planing	Pasante	6	4		7	16	11	11	8	4	24	98	7	22	56	7	9				14	6
46	TECDYA	Interno		X		Operaciones	Analista Comercial	6	4		7	16	10	13	10	5	28	83	7	27	60	7	8				17	4
47	YTEJAT	Externo		X		Security	Coordinador Security	7	4		7	14	10	52	9		23	105	7	71	49	7	7				11	4
48	TECLIZ	Pasante		X		Comercial	Abogada	6	5		9	16	11	43	9	5	19	78	9	31	47	9	8				17	4
49	TECJCU	Interno		X		Security	Coordinador Security	7	4		7	14	8	32	10	4	19	99	7	46	60	7	7	6	12	8	15	6
53	TECPMP	Interno		X		Operaciones	Pasante	6	5		9	13	11	44	7	5	25	84	9	34	51	9	9				11	5
54	YTEPMC	Externo		X		Operaciones	Pasante	6	4		7	14	10	45	7		28	112	7	28	58	7	8				17	5

58	YTEPGT	Externo		X		Sistemas	Analista Sistemas	10	7		8	12	8	125	9	5	27	100	8	172	59	8	6				14	4
								Media	4,75	0,00	7,58	14,42	10,00	69,67	9,17	4,56	23,33	96,67	7,58	95,42	55,17	7,58	7,67	0,00	0,00	0,00	14,00	4,50
								Desviación estándar	1,06	0,00	0,79	1,51	1,35	46,59	1,27	0,53	3,42	11,23	0,79	76,20	4,39	0,79	1,07	0,00	0,00	0,00	2,59	0,80
								Coeficiente de variación Tipo 2	22,22 %	0,00 %	10,46 %	10,44%	13,48 %	66,87%	13,83 %	11,57 %	14,66%	11,61%	10,46 %	79,86%	7,95%	10,46 %	14,00%	0,00%	0,00 %	0,00 %	18,53%	17,73 %
								Suma	57,00	-	91,00	173,00	120,00	836,00	110,00	41,00	280,00	1.160,00	91,00	1.145,00	662,00	91,00	92,00	13,00	12,00	8,00	168,00	54,00
								Porcentaje	1,10	-	1,75	3,32	2,31	16,06	2,11	0,79	5,38	22,29	1,75	22,00	12,72	1,75	1,77	0,25	0,23	0,15	3,23	1,04
1	TECCIB	Interno			X	Reservorios	Ingeniero Reservorios	11	4		9	15	12	114	11	5	26	74	9	247	56	9	7				17	4
2	TECAAC	Interno			X	Perforación	Company Man	12	7		8	16	11	134	8		25	81	8	271	57	8	7				17	5
3	TECEME	Interno			X	Perforación	Company Man	11	4		8	16	11	134	8		24	81	8	271	57	8	7				17	5
5	TECCVV	Interno			X	Abastecimientos	Analista de Compras	13	5		9	13	11	162	11	5	29	109	9	291	48	9	8	6			12	6
8	TECIRM	Interno			X	Sistemas	Coordinador Sistemas	12	6		8	12	12	102	7	5	28	77	8	312	58	8	6	12	8	12	14	5
18	TECMSC	Interno			X	Abastecimientos	Bodeguero	10	6		8	14	11	125	9	4	27	98	8	144	49	8	6	8			12	4
25	YTEKLO	Externo			X	Impuestos	Analista Funcional	3	4		7						24	102	7					7				4
32	YTEDOL	Externo			X	Administración	Auditor ARCH	6	4		8	16	11	30	7		20	122	8	14	53	8	9				13	5
35	YTEPPA	Externo			X	Administración	Auditor ARCH	6	4		7	17	11	36	8	4	22	107	7	39	54	7	9				16	4
36	YTECHJ	Externo			X	Administración	Analista de Contabilidad	6	6		7	15	11	28	7	4	19	100	7	48	61	7	7				14	5
50	YTEKAT	Externo			X	Sistemas	Analista Sistemas	3	4		7						23	80	7					7				6
55	TECDAV	Interno			X	Operaciones	Supervisor Producción	7	4		9	12	11	51	10	4	26	107	9	53	54	9	9				15	4
57	TECJIR	Interno			X	Comercial	Analista Comercial	10	4		7	16	9	142	10	5	18	90	7	183	58	7	7	8			17	5
								Media	4,77	0,00	7,85	14,73	11,00	96,18	8,73	4,50	23,92	94,46	7,85	170,27	55,00	8,00	7,45	8,00	8,00	12,00	14,91	4,77
								Desviación estándar	1,09	0,00	0,80	1,74	0,77	50,17	1,56	0,53	3,43	15,00	0,80	114,91	3,92	0,77	1,13	2,10	0,00	0,00	2,02	0,73
								Coeficiente de variación Tipo 3	22,90 %	0,00 %	10,20 %	11,80%	7,04%	52,16%	17,82 %	11,88 %	14,32%	15,88%	10,20 %	67,49%	7,14%	9,68%	15,13%	26,22 %	0,00 %	0,00 %	13,57%	15,20 %
								Suma	62,00	-	102,00	162,00	121,00	1.058,00	96,00	36,00	311,00	1.228,00	102,00	1.873,00	605,00	88,00	82,00	48,00	8,00	12,00	164,00	62,00
								Porcentaje	1,00	-	1,64	2,60	1,95	17,01	1,54	0,58	5,00	19,74	1,64	30,11	9,73	1,41	1,32	0,77	0,13	0,19	2,64	1,00

Ítem	Usuario	Tipo de Usuario	Código Tipo de Usuario	Básico (Red, Correo, Lync, telefonía fija)	Intermedio (Internet, Intranet, Repositorios Información)	Avanzado (VPN, SAP, telefonía celular, aplicaciones ECU, Repositorios ECU VIP)	Área	Cargo	Tiempo utilizado (horas)	Iniciar proceso de baja en ABM	Validar permisos vigentes en Matriz de usuarios	Bloquear Código de Usuario en ABM	Retirar equipos asignados	Firmar planilla retiro equipos	Respaldar información de usuario	Entregar respaldo a jefatura	Retirar tarjeta de acceso	Dar de baja en aplicaciones y repositorio acorde a matriz	Dar de baja en aplicaciones ARG	Eliminar usuario en ABM		Formatear equipo	Eliminar codigo equipo de la red	Bloquear claves de marcación telefónica y Wi-Fi	Bloquear clave de conexión remota	Retirar equipo celular	Dar de baja línea celular	Actualizar inventario de equipos	Cerrar el proceso de baja
65	TECEFN	Interno	1	X			Operaciones	Operador	4	5	8	9	13	5	34	8		12		5		50	8	7				15	5
79	YTEAUV	Interno	1	X			Seguridad y Salud	Medico	4	7	8	7	16	3	40	10		11		5		53	7	7				17	5
75	YTEEIL	Externo	1	X			Seguridad y Salud	Medico	4	6	7	7	13	5	32	10		12		5		65	7	7				13	6
76	YTEPAI	Externo	1	X			Seguridad y Salud	Medico	4	7	5	7	13	4	47	10		13		5		53	9	7				15	4
77	YTECCL	Externo	1	X			Administración	Abogado	5	4	7	9	15	3	98	11	6	8		5		53	8	6				17	6
									Media	5,80	7,00	7,80	14,00	4,00	50,20	9,80	6,00	11,20	0,00	5,00	0,00	54,80	7,80	6,80	#DIV/0!	0,00	0,00	15,40	5,20
									Desviación estandar	1,30	1,22	1,10	1,41	1,00	27,35	1,10	0,00	1,92	0,00	0,00	0,00	5,85	0,84	0,45	0,00	0,00	0,00	1,67	0,84
									Coeficiente de variación Tipo 1	22,48 %	17,50 %	14,04 %	10,10%	25,00 %	54,49%	11,18 %	0,00 %	17,17%	0,00%	0,00%	0,00 %	10,67%	10,73 %	6,58%	#DIV/0!	0,00 %	0,00 %	10,87%	16,09 %
									Suma	29,00	35,00	39,00	70,00	20,00	251,00	49,00	6,00	56,00	-	25,00	-	274,00	39,00	34,00	-	-	-	77,00	26,00
									Porcentaje	2,82	3,40	3,79	6,80	1,94	24,37	4,76	0,58	5,44	-	2,43	-	26,60	3,79	3,30	-	-	-	7,48	2,52
59	YTEJIM	Externo	2		X		Security	Coordinador Security	4	5	7	7	15	4	44	9		17		5		61	8	6	23			17	6
60	TECCHB	Pasante	2		X		Operaciones	Pasante	4	7	5	8	16	5	25	7	4	15		5		56	7	8				16	4
61	TECLER	Pasante	2		X		Operaciones	Pasante	4	4	7	8	15	5	30	8	5	15		5		59	7	8				14	4
62	TECMLZ	Pasante	2		X		Reservorios	Pasante	4	4	7	8	13	4	28	7	4	15		5		56	9	9				15	5
64	TECALB	Interno	2		X		Operaciones	Jóven Profesional	5	5	5	8	14	4	63	8	6	23	39	5		50	8	9				12	4
66	YTERIV	Externo	2		X		Sistemas	Analista Sistemas	4	6	6	7	14	5	25	8	5	13		4		57	8	9				14	4
80	TECGAK	Pasante	2		X		Planing	Pasante	4	4	6	7	13	5	41	10	6	12	38	4		61	7	6				14	6
78	TECCAI	Pasante	2		X		RRHH	Pasante	4	7	6	7	14	4	38	7	5	18	36	4		52	8	9				12	5
73	YTEPPA	Externo	2		X		Administración	Auditor ARCH	4	7	7	7	12	5	29	7	6	13	31	5		52	8	8				12	5
72	TECJIM	Interno	2		X		Operaciones	Recorredor	3	4	5	8	12	3				17		5		56	8	7				14	5
									Media	5,30	6,10	7,50	13,80	4,40	35,89	7,89	5,13	15,80	36,00	4,70	0,00	56,00	7,80	7,90	23,00	0,00	0,00	14,00	4,80
									Desviación estandar	1,34	0,88	0,53	1,32	0,70	12,31	1,05	0,83	3,19	3,56	0,48	0,00	3,77	0,63	1,20	0,00	0,00	0,00	1,70	0,79

									Coeficiente de variación Tipo 2	25,24 %	14,35 %	7,03%	9,54%	15,89 %	34,31%	13,36 %	16,28 %	20,19%	9,89%	10,28 %	0,00 %	6,73%	8,11%	15,15%	0,00%	0,00 %	0,00 %	12,14%	16,43 %
									Suma	53,00	61,00	75,00	138,00	44,00	323,00	71,00	41,00	158,00	144,00	47,00	-	560,00	78,00	79,00	23,00	-	-	140,00	48,00
									Porcentaje	2,54	2,93	3,60	6,63	2,11	15,51	3,41	1,97	7,59	6,91	2,26	-	26,88	3,74	3,79	1,10	-	-	6,72	2,30
63	YTEVEC	Externo	3			X	Sistemas	Analista Sistemas	3	6	8	8							33	5		65	7	9				16	4
67	YTEAMO	Externo	3			X	Producción	Company Man	5	7	5	7	13	5	84	7		26	42	4		50	8	8				14	5
68	YTEEDM	Externo	3			X	Producción	Company Man	6	7	8	8	16	4	92	8		26	42	5		50	7	7				17	5
74	YTERUX	Externo	3			X	Impuestos	Auditor PWC	5	4	8	8	13	4	35	11	6	12	37	4		53	7	8	21			14	5
71	TECDAN	Interno	3			X	Administración	Analista Financiera	6	7	6	8	13	3	133	11	7	22	41	5		59	8	7				12	5
70	TECGCP	Interno	3			X	Facilidades	Ingeniero de Mejora	6	6	8	9	13	4	126	7	6	24	39	5		53	9	9	21			14	5
69	TECGAC	Interno	3			X	RRHH	Coordinadora RRHH	7	7	8	8	14	4	148	7	7	29	58	4		61	8	8	22			12	6
									Media	6,29	7,29	8,00	13,67	4,00	103,00	8,50	6,50	23,17	41,71	4,57	0,00	55,86	7,71	8,00	21,33	0,00	0,00	14,14	5,00
									Desviación estandar	1,11	1,25	0,58	1,21	0,63	41,38	1,97	0,58	5,95	7,87	0,53	0,00	5,84	0,76	0,82	0,58	0,00	0,00	1,86	0,58
									Coeficiente de variación Tipo 3	17,70 %	17,21 %	7,22%	8,86%	15,81 %	40,17%	23,23 %	8,88 %	25,67%	18,86%	11,69 %	0,00 %	10,46%	9,80%	10,21%	2,71%	0,00 %	0,00 %	13,18%	11,55 %
									Suma	44,00	51,00	56,00	82,00	24,00	618,00	51,00	26,00	139,00	292,00	32,00	-	391,00	54,00	56,00	64,00	-	-	99,00	35,00
									Porcentaje	2,08	2,41	2,65	3,88	1,14	29,23	2,41	1,23	6,58	13,81	1,51	-	18,50	2,55	2,65	3,03	-	-	4,68	1,66