



# MANUAL DE PROCESOS Y PROCEDIMIENTOS



## DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

### CÓDIGO: DITIC-MPP-001

### NOVIEMBRE – 2017

*Este documento contiene información de propiedad exclusiva. La misma que se mantendrá de forma confidencial y reservada, no pudiendo ser divulgada a personal interno o externo que no sean empleados o funcionarios autorizados del Instituto Nacional de Estadística y Censos.*

## CONTENIDO

<b>FIRMAS DE REVISIÓN Y APROBACIÓN .....</b>	<b>9</b>
<b>1. CONTROL E HISTORIAL DE CAMBIOS .....</b>	<b>9</b>
<b>3. GLOSARIO DE TÉRMINOS Y ABREVIATURAS .....</b>	<b>10</b>
<b>4. MAPA DE INTERRELACIÓN .....</b>	<b>16</b>
<b>5. DESCRIPCIÓN DE LOS SUBPROCESOS DE LA GESTIÓN DE INFRAESTRUCTURA DE TECNOLOGÍAS DE LA INFORMACIÓN .....</b>	<b>20</b>
5.1. SUBPROCESO DE ADMINISTRACIÓN DE REDES Y COMUNICACIONES .....	20
5.1.1. FICHA TÉCNICA DEL SUBPROCESO DE ADMINISTRACIÓN DE REDES Y COMUNICACIONES.....	20
5.1.2. CONTROLES DEL SUBPROCESO DE ADMINISTRACIÓN DE REDES Y COMUNICACIONES .....	21
5.1.3. DIAGRAMA DE FLUJO DEL SUBPROCESO DE ADMINISTRACIÓN DE REDES Y COMUNICACIONES	25
5.1.4. PROCEDIMIENTO DEL SUBPROCESO DE ADMINISTRACIÓN DE REDES Y COMUNICACIONES ..	26
5.1.5. INDICADORES DEL SUBPROCESO DE ADMINISTRACIÓN DE REDES Y COMUNICACIONES .....	28
5.1.6. FORMATOS DEL SUBPROCESO DE ADMINISTRACIÓN DE REDES Y COMUNICACIONES.....	28
5.1.7. ANEXOS DEL SUBPROCESO DE ADMINISTRACIÓN DE REDES Y COMUNICACIONES .....	28
5.2. SUBPROCESO DE ADMINISTRACIÓN DE PORTALES WEB .....	29
5.2.1. FICHA TÉCNICA DEL SUBPROCESO DE ADMINISTRACIÓN DE PORTALES WEB .....	29
5.2.2. CONTROLES DEL SUBPROCESO DE ADMINISTRACIÓN DE PORTALES WEB.....	30
5.2.3. DIAGRAMA DE FLUJO DEL SUBPROCESO DE ADMINISTRACIÓN DE PORTALES WEB.....	34
5.2.4. PROCEDIMIENTO DEL SUBPROCESO DE ADMINISTRACIÓN DE PORTALES WEB .....	35
5.2.5. INDICADORES DEL SUBPROCESO DE ADMINISTRACIÓN DE PORTALES WEB.....	37
5.2.6. FORMATOS DEL SUBPROCESO DE ADMINISTRACIÓN DE PORTALES WEB .....	37
5.2.7. ANEXOS DEL SUBPROCESO DE ADMINISTRACIÓN DE PORTALES WEB .....	37
5.3. SUBPROCESO DE ADMINISTRACIÓN DE DATA CENTER .....	38
5.3.1. FICHA TÉCNICA DEL SUBPROCESO DE ADMINISTRACIÓN DE DATA CENTER .....	38
5.3.2. CONTROLES DEL SUBPROCESO DE ADMINISTRACIÓN DE DATA CENTER .....	39
5.3.3. DIAGRAMA DE FLUJO DEL SUBPROCESO DE ADMINISTRACIÓN DE DATA CENTER .....	41
5.3.4. PROCEDIMIENTO DEL SUBPROCESO DE ADMINISTRACIÓN DE DATA CENTER .....	42
5.3.5. INDICADORES DEL SUBPROCESO DE ADMINISTRACIÓN DE DATA CENTER .....	43
5.3.6. FORMATOS DEL SUBPROCESO DE ADMINISTRACIÓN DE DATA CENTER .....	43
5.3.7. ANEXOS DEL SUBPROCESO DE ADMINISTRACIÓN DE DATA CENTER .....	43
5.4. SUBPROCESO DE ADMINISTRACIÓN DE INFRAESTRUCTURA .....	44
5.4.1. FICHA TÉCNICA DEL SUBPROCESO DE ADMINISTRACIÓN DE INFRAESTRUCTURA .....	44
5.4.2. CONTROLES DEL SUBPROCESO DE ADMINISTRACIÓN DE INFRAESTRUCTURA .....	45
5.4.3. DIAGRAMA DE FLUJO DEL SUBPROCESO DE ADMINISTRACIÓN DE INFRAESTRUCTURA .....	48
5.4.4. PROCEDIMIENTO DEL SUBPROCESO DE ADMINISTRACIÓN DE INFRAESTRUCTURA .....	49
5.4.5. INDICADORES DEL SUBPROCESO DE ADMINISTRACIÓN DE INFRAESTRUCTURA .....	51

<b>Elaborado por:</b>	<b>Revisado por:</b>	<b>Aprobado /Autorizado por:</b>	<b>Registrado por:</b>
PC	DIPLA - DITIC	DIREJ	DIPLA, PC

5.4.6.	FORMATOS DEL SUBPROCESO DE ADMINISTRACIÓN DE INFRAESTRUCTURA .....	51
5.4.7.	ANEXOS DEL SUBPROCESO DE ADMINISTRACIÓN DE INFRAESTRUCTURA.....	51
5.5.	SUBPROCESO DE ADMINISTRACIÓN DE GESTIÓN DOCUMENTAL QUIPUX .....	52
5.5.1.	FICHA TÉCNICA DEL SUBPROCESO DE ADMINISTRACIÓN DE GESTIÓN DOCUMENTAL QUIPUX	52
5.5.2.	CONTROLES DEL SUBPROCESO DE ADMINISTRACIÓN DE GESTIÓN DOCUMENTAL QUIPUX ...	53
5.5.3.	DIAGRAMA DE FLUJO DEL SUBPROCESO DE ADMINISTRACIÓN DE GESTIÓN DOCUMENTAL QUIPUX.....	54
5.5.4.	PROCEDIMIENTO DEL SUBPROCESO DE ADMINISTRACIÓN DE GESTIÓN DOCUMENTAL QUIPUX	55
5.5.5.	INDICADORES DEL SUBPROCESO DE ADMINISTRACIÓN DE GESTIÓN DOCUMENTAL QUIPUX	56
5.5.6.	FORMATOS DEL SUBPROCESO DE ADMINISTRACIÓN DE GESTIÓN DOCUMENTAL QUIPUX....	56
5.5.7.	ANEXOS DEL SUBPROCESO DE ADMINISTRACIÓN DE GESTIÓN DOCUMENTAL QUIPUX .....	56
5.6.	SUBPROCESO DE ADMINISTRACIÓN DE BASE DE DATOS .....	57
5.6.1.	FICHA TÉCNICA DEL SUBPROCESO DE ADMINISTRACIÓN DE BASE DE DATOS .....	57
5.6.2.	CONTROLES DEL SUBPROCESO DE ADMINISTRACIÓN DE BASE DE DATOS .....	58
5.6.3.	DIAGRAMA DE FLUJO DEL SUBPROCESO DE ADMINISTRACIÓN DE BASE DE DATOS .....	60
5.6.4.	PROCEDIMIENTO DEL SUBPROCESO DE ADMINISTRACIÓN DE BASE DE DATOS.....	61
5.6.5.	INDICADORES DEL SUBPROCESO DE ADMINISTRACIÓN DE BASE DE DATOS .....	65
5.6.6.	FORMATOS DEL SUBPROCESO DE ADMINISTRACIÓN DE BASE DE DATOS.....	65
5.6.7.	ANEXOS DEL SUBPROCESO DE ADMINISTRACIÓN DE BASE DE DATOS .....	65
5.7.	SUBPROCESO DE ASESORAMIENTO TECNOLÓGICO DE INFRAESTRUCTURA.....	66
5.7.1.	FICHA TÉCNICA DEL SUBPROCESO DE ASESORAMIENTO TECNOLÓGICO DE INFRAESTRUCTURA	66
5.7.2.	CONTROLES DEL SUBPROCESO DE ASESORAMIENTO TECNOLÓGICO DE INFRAESTRUCTURA	67
5.7.3.	DIAGRAMA DE FLUJO DEL SUBPROCESO DE ASESORAMIENTO TECNOLÓGICO DE INFRAESTRUCTURA .....	69
5.7.4.	PROCEDIMIENTO DEL SUBPROCESO DE ASESORAMIENTO TECNOLÓGICO DE INFRAESTRUCTURA .....	70
5.7.5.	INDICADORES DEL SUBPROCESO DE ASESORAMIENTO TECNOLÓGICO DE INFRAESTRUCTURA	71
5.7.6.	FORMATOS DEL SUBPROCESO DE ASESORAMIENTO TECNOLÓGICO DE INFRAESTRUCTURA .	71
5.7.7.	ANEXOS DEL SUBPROCESO DE ASESORAMIENTO TECNOLÓGICO DE INFRAESTRUCTURA.....	71
	“No hay anexos.” .....	71
5.8.	SUBPROCESO DE SOPORTE A USUARIOS EN INFRAESTRUCTURA.....	72
5.8.1.	FICHA TÉCNICA DEL SUBPROCESO DE SOPORTE A USUARIOS EN INFRAESTRUCTURA .....	72
5.8.2.	CONTROLES DEL SUBPROCESO DE SOPORTE A USUARIOS EN INFRAESTRUCTURA .....	73
5.8.3.	DIAGRAMA DE FLUJO DEL SUBPROCESO DE SOPORTE A USUARIOS EN INFRAESTRUCTURA ..	75
5.8.4.	PROCEDIMIENTO DEL SUBPROCESO DE SOPORTE A USUARIOS EN INFRAESTRUCTURA .....	76
5.8.5.	INDICADORES DEL SUBPROCESO DE SOPORTE A USUARIOS EN INFRAESTRUCTURA .....	76
5.8.6.	FORMATOS DEL SUBPROCESO DE SOPORTE A USUARIOS EN INFRAESTRUCTURA .....	77

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

5.8.7.	ANEXOS DEL SUBPROCESO DE SOPORTE A USUARIOS EN INFRAESTRUCTURA.....	77
5.9.	SUBPROCESO ADMINISTRACIÓN DE CORREO ELECTRÓNICO.....	78
5.9.1.	FICHA TÉCNICA DEL SUBPROCESO DE ADMINISTRACIÓN DE CORREO ELECTRÓNICO .....	78
5.9.2.	CONTROLES DEL SUBPROCESO DE ADMINISTRACIÓN DE CORREO .....	79
5.9.3.	DIAGRAMA DE FLUJO DEL SUBPROCESO DE ADMINISTRACIÓN DE CORREO .....	83
5.9.4.	PROCEDIMIENTO DEL SUBPROCESO DE ADMINISTRACIÓN DE CORREO.....	84
5.9.5.	INDICADORES DEL SUBPROCESO DE ADMINISTRACIÓN DE CORREO .....	86
5.9.6.	FORMATOS DEL SUBPROCESO DE ADMINISTRACIÓN DE CORREO .....	86
5.9.7.	ANEXOS DEL SUBPROCESO DE ADMINISTRACIÓN DE CORREO .....	86
5.10.	SUBPROCESO DE ADMINISTRACIÓN DE SERVICIOS DE SEGURIDAD .....	87
5.10.1.	FICHA TÉCNICA DEL SUBPROCESO DE ADMINISTRACIÓN DE SERVICIOS DE SEGURIDAD .....	87
5.10.2.	CONTROLES DEL SUBPROCESO DE ADMINISTRACIÓN DE SERVICIOS DE SEGURIDAD.....	88
5.10.3.	DIAGRAMA DE FLUJO DEL SUBPROCESO DE ADMINISTRACIÓN DE SERVICIOS DE SEGURIDAD	89
5.10.4.	PROCEDIMIENTO DEL SUBPROCESO DE ADMINISTRACIÓN DE SERVICIOS DE SEGURIDAD .....	90
5.10.5.	INDICADORES DEL SUBPROCESO DE ADMINISTRACIÓN DE SERVICIOS DE SEGURIDAD.....	91
5.10.6.	FORMATOS DEL SUBPROCESO DE ADMINISTRACIÓN DE SERVICIOS DE SEGURIDAD .....	91
5.10.7.	ANEXOS DEL SUBPROCESO DE ADMINISTRACIÓN DE SERVICIOS DE SEGURIDAD.....	91
5.11.	SUBPROCESO DE ADMINISTRACIÓN DE CONFIGURACIÓN DE USUARIOS .....	92
5.11.1.	FICHA TÉCNICA DEL SUBPROCESO DE ADMINISTRACIÓN DE CONFIGURACIÓN DE USUARIOS	92
5.11.2.	CONTROLES DEL SUBPROCESO DE ADMINISTRACIÓN DE CONFIGURACIÓN DE USUARIOS.....	93
5.11.3.	DIAGRAMA DE FLUJO DEL SUBPROCESO DE ADMINISTRACIÓN DE CONFIGURACIÓN DE	USUARIOS.....
5.11.4.	PROCEDIMIENTO DEL SUBPROCESO DE ADMINISTRACIÓN DE CONFIGURACIÓN DE USUARIOS	95
5.11.5.	INDICADORES DEL SUBPROCESO DE ADMINISTRACIÓN DE CONFIGURACIÓN DE USUARIOS..	96
5.11.6.	FORMATOS DEL SUBPROCESO DE ADMINISTRACIÓN DE CONFIGURACIÓN DE USUARIOS .....	97
5.11.7.	ANEXOS DEL SUBPROCESO DE ADMINISTRACIÓN DE CONFIGURACIÓN DE USUARIOS.....	97
5.12.	SUBPROCESO DE ADMINISTRACIÓN DE CONEXIÓN REMOTA .....	98
5.12.1.	FICHA TÉCNICA DEL SUBPROCESO DE ADMINISTRACIÓN DE CONEXIÓN REMOTA.....	98
5.12.2.	CONTROLES DEL SUBPROCESO DE ADMINISTRACIÓN DE CONEXIÓN REMOTA.....	99
5.12.3.	DIAGRAMA DE FLUJO DEL SUBPROCESO DE ADMINISTRACIÓN DE CONEXIÓN REMOTA.....	103
5.12.4.	PROCEDIMIENTO DEL SUBPROCESO DE ADMINISTRACIÓN DE CONEXIÓN REMOTA.....	104
5.12.5.	INDICADORES DEL SUBPROCESO DE ADMINISTRACIÓN DE CONEXIÓN REMOTA.....	105
5.12.6.	FORMATOS DEL SUBPROCESO DE ADMINISTRACIÓN DE CONEXIÓN REMOTA.....	105
5.12.7.	ANEXOS DEL SUBPROCESO DE ADMINISTRACIÓN DE CONEXIÓN REMOTA .....	105
5.13.	SUBPROCESO DE ADMINISTRACIÓN DE HERRAMIENTAS DE MONITOREO.....	106
5.13.1.	FICHA TÉCNICA DEL SUBPROCESO DE ADMINISTRACIÓN DE HERRAMIENTAS DE MONITOREO	106
5.13.2.	CONTROLES DEL SUBPROCESO DE ADMINISTRACIÓN DE HERRAMIENTAS DE MONITOREO.	107

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

5.13.3. DIAGRAMA DE FLUJO DEL SUBPROCESO DE ADMINISTRACIÓN DE HERRAMIENTAS DE MONITOREO.....	108
5.13.4. PROCEDIMIENTO DEL SUBPROCESO DE ADMINISTRACIÓN DE HERRAMIENTAS DE MONITOREO.....	109
5.13.5. INDICADORES DEL SUBPROCESO DE ADMINISTRACIÓN DE HERRAMIENTAS DE MONITOREO	110
5.13.6. FORMATOS DEL SUBPROCESO DE ADMINISTRACIÓN DE HERRAMIENTAS DE MONITOREO .	110
5.13.7. ANEXOS DEL SUBPROCESO DE ADMINISTRACIÓN DE HERRAMIENTAS DE MONITOREO.....	110
5.14. SUBPROCESO DE ADMINISTRACIÓN DE SERVICIOS DE VIDEO CONFERENCIA.....	111
5.14.1. FICHA TÉCNICA DEL SUBPROCESO DE ADMINISTRACIÓN DE SERVICIOS DE VIDEO CONFERENCIA .....	111
5.14.2. CONTROLES DEL SUBPROCESO DE ADMINISTRACIÓN DE SERVICIOS DE VIDEO CONFERENCIA	112
5.14.3. DIAGRAMA DE FLUJO DEL SUBPROCESO DE ADMINISTRACIÓN DE SERVICIOS DE VIDEO CONFERENCIA .....	113
5.14.4. PROCEDIMIENTO DEL SUBPROCESO DE ADMINISTRACIÓN DE SERVICIOS DE VIDEO CONFERENCIA .....	114
5.14.5. INDICADORES DEL SUBPROCESO DE ADMINISTRACIÓN DE SERVICIOS DE VIDEO CONFERENCIA	115
5.14.6. FORMATOS DEL SUBPROCESO DE ADMINISTRACIÓN DE SERVICIOS DE VIDEO CONFERENCIA	115
5.14.7. ANEXOS DEL SUBPROCESO DE ADMINISTRACIÓN DE SERVICIOS DE VIDEO CONFERENCIA...	115
5.15. SUBPROCESO DE GENERACIÓN DE RESPALDOS DE INFORMACIÓN.....	116
5.15.1. FICHA TÉCNICA DEL SUBPROCESO DE GENERACIÓN DE RESPALDOS DE INFORMACIÓN.....	116
5.15.2. CONTROLES DEL SUBPROCESO DE GENERACIÓN DE RESPALDOS DE INFORMACIÓN .....	117
5.15.3. DIAGRAMA DE FLUJO DEL SUBPROCESO DE GENERACIÓN DE RESPALDOS DE INFORMACIÓN	119
5.15.4. PROCEDIMIENTO DEL SUBPROCESO DE GENERACIÓN DE RESPALDOS DE INFORMACIÓN....	120
5.15.5. INDICADORES DEL SUBPROCESO DE GENERACIÓN DE RESPALDOS DE INFORMACIÓN .....	121
5.15.6. FORMATOS DEL SUBPROCESO DE GENERACIÓN DE RESPALDOS DE INFORMACIÓN.....	121
5.15.7. ANEXOS DEL SUBPROCESO DE GENERACIÓN DE RESPALDOS DE INFORMACIÓN .....	121
<b>6. DESCRIPCIÓN DE PROCESOS DE GESTIÓN DE SOPORTE A USUARIOS.....</b>	<b>122</b>
6.1. SUBPROCESO DE ASESORAMIENTO TECNOLÓGICO .....	122
6.1.1. FICHA TÉCNICA DEL SUBPROCESO DE ASESORAMIENTO TECNOLÓGICO .....	122
6.1.2. CONTROLES DEL SUBPROCESO DE ASESORAMIENTO TECNOLÓGICO .....	123
6.1.3. DIAGRAMA DE FLUJO DEL SUBPROCESO DE ASESORAMIENTO TECNOLÓGICO .....	124
6.1.4. PROCEDIMIENTO DEL SUBPROCESO DE ASESORAMIENTO TECNOLÓGICO.....	125
6.1.5. INDICADORES DEL SUBPROCESO DE ASESORAMIENTO TECNOLÓGICO .....	126
6.1.6. FORMATOS DEL SUBPROCESO DE ASESORAMIENTO TECNOLÓGICO .....	126
6.1.7. ANEXOS DEL SUBPROCESO DE ASESORAMIENTO TECNOLÓGICO .....	126

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------



6.2.	SUBPROCESO DE MANTENIMIENTO PREVENTIVO DE EQUIPOS TECNOLÓGICOS .....	127
6.2.1.	FICHA TÉCNICA DEL SUBPROCESO DE MANTENIMIENTO PREVENTIVO DE EQUIPOS TECNOLÓGICOS .....	127
6.2.2.	CONTROLES DEL SUBPROCESO DE MANTENIMIENTO PREVENTIVO DE EQUIPOS TECNOLÓGICO	128
6.2.3.	DIAGRAMA DE FLUJO DEL SUBPROCESO DE MANTENIMIENTO PREVENTIVO DE EQUIPOS TECNOLÓGICOS .....	129
6.2.4.	PROCEDIMIENTO DEL SUBPROCESO DE MANTENIMIENTO PREVENTIVO DE EQUIPOS TECNOLÓGICOS .....	130
6.2.5.	INDICADORES DEL SUBPROCESO DE MANTENIMIENTO PREVENTIVO DE EQUIPOS TECNOLÓGICOS .....	131
6.2.6.	FORMATOS DEL SUBPROCESO DE MANTENIMIENTO PREVENTIVO DE EQUIPOS TECNOLÓGICOS .....	131
6.2.7.	ANEXOS DEL SUBPROCESO DE MANTENIMIENTO PREVENTIVO DE EQUIPOS TECNOLÓGICOS	131
6.3.	SUBPROCESO DE SOPORTE TÉCNICO .....	132
6.3.1.	FICHA TÉCNICA DEL SUBPROCESO DE SOPORTE TÉCNICO .....	132
6.3.2.	CONTROLES DEL SUBPROCESO DE SOPORTE TÉCNICO .....	133
6.3.3.	DIAGRAMA DE FLUJO DEL SUBPROCESO DE SOPORTE TÉCNICO .....	134
6.3.4.	PROCEDIMIENTO DEL SUBPROCESO DE SOPORTE TÉCNICO .....	135
6.3.5.	INDICADORES DEL SUBPROCESO DE SOPORTE TÉCNICO .....	136
6.3.6.	FORMATOS DEL SUBPROCESO DE SOPORTE TÉCNICO .....	136
6.3.7.	ANEXOS DEL SUBPROCESO DE SOPORTE TÉCNICO .....	136
6.4.	SUBPROCESO DE INVENTARIO TECNOLÓGICO .....	137
6.4.1.	FICHA TÉCNICA DEL SUBPROCESO DE INVENTARIO TECNOLÓGICO .....	137
6.4.2.	CONTROLES DEL SUBPROCESO DE INVENTARIO TECNOLÓGICO .....	138
6.4.3.	DIAGRAMA DE FLUJO DEL SUBPROCESO DE INVENTARIO TECNOLÓGICO .....	140
6.4.4.	PROCEDIMIENTO DEL SUBPROCESO DE INVENTARIO TECNOLÓGICO .....	141
6.4.5.	INDICADORES DEL SUBPROCESO DE INVENTARIO TECNOLÓGICO .....	142
6.4.6.	FORMATOS DEL SUBPROCESO DE INVENTARIO TECNOLÓGICO .....	142
6.4.7.	ANEXOS DEL SUBPROCESO DE INVENTARIO TECNOLÓGICO .....	142
6.5.	SUBPROCESO DE GESTIÓN DEL PARQUE INFORMÁTICO .....	143
6.5.1.	FICHA TÉCNICA DEL SUBPROCESO DE GESTIÓN DEL PARQUE INFORMÁTICO .....	143
6.5.2.	CONTROLES DEL SUBPROCESO DE GESTIÓN DEL PARQUE INFORMÁTICO .....	144
6.5.3.	DIAGRAMA DE FLUJO DEL SUBPROCESO DE GESTIÓN DEL PARQUE INFORMÁTICO .....	145
6.5.4.	PROCEDIMIENTO DEL SUBPROCESO DE GESTIÓN DEL PARQUE INFORMÁTICO .....	146
6.5.5.	INDICADORES DEL SUBPROCESO DE GESTIÓN DEL PARQUE INFORMÁTICO .....	147
6.5.6.	FORMATOS DEL SUBPROCESO DE GESTIÓN DEL PARQUE INFORMÁTICO .....	147
6.5.7.	ANEXOS DEL SUBPROCESO DE GESTIÓN DEL PARQUE INFORMÁTICO .....	147

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

## **7. DESCRIPCIÓN DE PROCESOS DE GESTIÓN DE SEGURIDAD INFORMÁTICA, INTEROPERABILIDAD Y RIESGOS ..... 148**

7.1. SUBPROCESO DE DESARROLLO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA.....	148
7.1.1. FICHA TÉCNICA DEL SUBPROCESO DE DESARROLLO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA .....	148
7.1.2. CONTROLES DEL SUBPROCESO DE DESARROLLO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA	149
7.1.3. DIAGRAMA DE FLUJO DEL SUBPROCESO DE DESARROLLO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA .....	153
7.1.4. PROCEDIMIENTO DEL SUBPROCESO DE DESARROLLO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA .....	154
7.1.5. INDICADORES DEL SUBPROCESO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA .....	155
7.1.6. FORMATOS DEL SUBPROCESO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA.....	155
7.1.7. ANEXOS DEL SUBPROCESO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA .....	155
7.2. FICHA TÉCNICA DEL SUBPROCESO DE PLAN DE CONCIENCIACIÓN DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA A USUARIOS .....	156
7.2.1. FICHA TÉCNICA DEL SUBPROCESO DE PLAN DE CONCIENCIACIÓN DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA A USUARIOS .....	156
7.2.2. CONTROLES DEL SUBPROCESO DE PLAN DE CONCIENCIACIÓN DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA A USUARIOS .....	157
7.2.3. DIAGRAMA DE FLUJO DEL SUBPROCESO DE PLAN DE CONCIENCIACIÓN DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA A USUARIOS .....	158
7.2.4. PROCEDIMIENTO DEL SUBPROCESO DE PLAN DE CONCIENCIACIÓN DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA A USUARIOS .....	159
7.2.5. INDICADORES DEL SUBPROCESO DE PLAN DE CONCIENCIACIÓN DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA A USUARIOS .....	160
7.2.6. FORMATOS DEL SUBPROCESO DE PLAN DE CONCIENCIACIÓN DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA A USUARIOS .....	160
7.2.7. ANEXOS DEL SUBPROCESO DE PLAN DE CONCIENCIACIÓN DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA A USUARIOS .....	160
7.3. SUBPROCESO DE MONITOREO Y CUMPLIMIENTO DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN RELACIONADO A LA SEGURIDAD INFORMÁTICA.....	161
7.3.1. FICHA TÉCNICA DEL SUBPROCESO DE MONITOREO Y CUMPLIMIENTO DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN RELACIONADO A LA SEGURIDAD INFORMÁTICA .....	161
7.3.2. CONTROLES DEL SUBPROCESO DE MONITOREO Y CUMPLIMIENTO DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN RELACIONADO A LA SEGURIDAD INFORMÁTICA .....	162


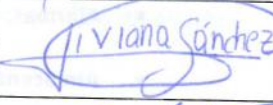
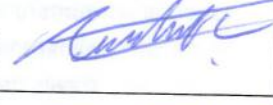




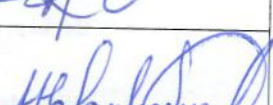
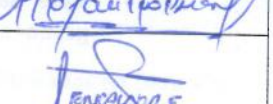
<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

7.3.3. DIAGRAMA DE FLUJO DEL SUBPROCESO DE MONITOREO Y CUMPLIMIENTO DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN RELACIONADO A LA SEGURIDAD INFORMÁTICA .....	163
7.3.4. PROCEDIMIENTO DEL SUBPROCESO DE MONITOREO Y CUMPLIMIENTO DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN RELACIONADO A LA SEGURIDAD INFORMÁTICA .....	164
7.3.5. INDICADORES DEL SUBPROCESO DE MONITOREO Y CUMPLIMIENTO DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN RELACIONADO A LA SEGURIDAD INFORMÁTICA .....	165
7.3.6. FORMATOS DEL SUBPROCESO DE MONITOREO Y CUMPLIMIENTO DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN RELACIONADO A LA SEGURIDAD INFORMÁTICA .....	165
7.3.7. ANEXOS DEL SUBPROCESO DE MONITOREO Y CUMPLIMIENTO DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN RELACIONADO A LA SEGURIDAD INFORMÁTICA .....	165
7.4. SUBPROCESO DE ADMINISTRACIÓN DE SISTEMA GPR.....	166
7.4.1. FICHA TÉCNICA DEL SUBPROCESO DE ADMINISTRACIÓN DE SISTEMA GPR.....	166
7.4.2. CONTROLES DEL SUBPROCESO DE ADMINISTRACIÓN DE SISTEMA GPR.....	167
7.4.3. DIAGRAMA DE FLUJO DEL SUBPROCESO DE ADMINISTRACIÓN DE SISTEMA GPR.....	169
7.4.4. PROCEDIMIENTO DEL SUBPROCESO DE ADMINISTRACIÓN DE SISTEMA GPR.....	170
7.4.5. INDICADORES DEL SUBPROCESO DE ADMINISTRACIÓN DE SISTEMA GPR.....	171
7.4.6. FORMATOS DEL SUBPROCESO DE ADMINISTRACIÓN DE SISTEMA GPR.....	171
7.4.7. ANEXOS DEL SUBPROCESO DE ADMINISTRACIÓN DE SISTEMA GPR .....	171

Elaborado por: PC	Revisado por: DIPLA - DITIC	Aprobado /Autorizado por: DIREJ	Registrado por: DIPLA, PC
----------------------	--------------------------------	------------------------------------	------------------------------



**FIRMAS DE REVISIÓN Y APROBACIÓN**

	Nombre y Apellido	Cargo	Firma
Elaborado por:	David Carrión	Asistente de Servicios, Procesos y Calidad	
Elaborado por:	Viviana Sánchez	Analista de Servicios, Procesos y Calidad	
Elaborado por:	Christian Estrella	Analista de Servicios, Procesos y Calidad	
Revisado por:	Franklin Gualoto	Jefe de Gestión de Servicios, Procesos y Calidad	
Revisado por:	Jeaneth Zarsosa	Jefe de Gestión de Infraestructura de Tecnologías de la Información	
Revisado por:	Jenny Delgado	Jefe de Gestión de Seguridad Informática, Interoperabilidad y Riesgos	
Revisado por:	Washington Muñoz	Jefe de Gestión Soporte a Usuarios	
Aprobado por:	Paulina Suárez	Directora de Tecnologías de la Información y Comunicación	
Aprobado por:	Estefanía Encalada	Directora de Planificación y Gestión Estratégica	

**1. CONTROL E HISTORIAL DE CAMBIOS**

Versión	Descripción del cambio	Fecha de Actualización
1.0	Versión Original	30/12/2015
2.0	Actualización de procesos y formato *La actualización de este manual no incluye la transición de desarrollos informáticos de la Dirección de Registros Administrativos a la Dirección de Tecnología de la Información y Comunicación	27/10/2017

Elaborado por: PC	Revisado por: DIPLA - DITIC	Aprobado /Autorizado por: DIREJ	Registrado por: DIPLA, PC
----------------------	--------------------------------	------------------------------------	------------------------------

### 3. GLOSARIO DE TÉRMINOS Y ABREVIATURAS

- **Active Directory:** Término que usa Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores.
- **Activo:** Son aquellos recursos (hardware/software), que explota una empresa.
- **Alarmas:** Aviso de un incidente que se registra en un aplicativo.
- **Almacenamiento NAS:** El almacenamiento conectado en red, Network Attached Storage (NAS), es el nombre dado a una tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento de un computador (servidor) con computadoras personales o servidores clientes a través de una red (normalmente TCP/IP), haciendo uso de un sistema operativo optimizado para dar acceso con los protocolos CIFS, NFS, FTP o TFTP.
- **Almacenamiento SAN:** Una SAN es una red dedicada al almacenamiento que está conectada a las redes de comunicación de una compañía. Además de contar con interfaces de red tradicionales, los equipos con acceso a la SAN tienen una interfaz de red específica que se conecta a la SAN.
- **Ambientes de Prueba:** Los ambientes de prueba son una parte de la fase de ensayos en el ciclo de producción. Antes de la fase de ensayos viene la fase de desarrollo opcional.
- **Antivirus:** programa que busca y eventualmente elimina los virus informáticos que pueden haber infectado un disco rígido disquete.
- **Backup:** copia de seguridad. Se hace para prevenir una posible pérdida de información.
- **Base de datos:** conjunto de datos organizados de modo tal que resulte fácil acceder a ellos, gestionarlos y actualizarlos.
- **Bitácora:** Una bitácora representa un cuaderno donde se reportan los avances y resultados de un determinado estudio o trabajo; el mismo incluye hipótesis, observaciones, ideas, datos, obstáculos que puedan surgir en el transcurso de la investigación.
- **Capacidades Tecnológicas:** Conceptuada como factor de producción, la capacidad tecnológica está constituida por el conjunto de conocimientos y habilidades que dan sustento al proceso de producción.
- **Casos de uso:** Un caso de uso es una descripción de los pasos o las actividades que deberán realizarse para llevar a cabo algún proceso.
- **Cifrado:** un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido
- **Cintas:** Tira de material plástico (mylar), recubierta de material magnético, empleada para el almacenamiento de información. Por su estructura, la cinta magnética almacena la información de forma secuencial y se presta al almacenaje de grandes volúmenes de datos de escasa utilización.

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

- **Código Fuente:** El código fuente de un programa informático (o software) es un conjunto de líneas de texto que son las instrucciones que debe seguir la computadora para ejecutar dicho programa. Por tanto, en el código fuente de un programa está escrito por completo su funcionamiento.
- **Consola:** Un método que permite a las personas dar instrucciones a algún programa informático.
- **Contraseña:** Una contraseña o clave es una forma de autenticación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña debe mantenerse en secreto ante aquellos a quien no se les permite el acceso.
- **Control Interno.-** Conjunto de normas, principios, fundamentos, procesos, procedimientos, acciones, mecanismos, técnicas e instrumentos de Control que, ordenados, relacionados entre sí y unidos a las personas que conforman una institución pública, se constituye en un medio para lograr una función administrativa de Estado integra, eficaz y transparente, apoyando el cumplimiento de sus objetivos institucionales y contribuyendo al logro de la finalidad social del Estado.
- **Data center:** Sistema de monitoreo de los equipos que se encuentran en el cuarto frio como son servidores, switch, racks, ups, sistema de video vigilancia.
- **Datos:** Toda aquella información que maneja un programa y está en contraposición a código o instrucciones.
- **DIPLA:** Dirección de Planificación y Gestión Estratégica.
- **DITIC:** Dirección de Tecnologías de la Información y Comunicación.
- **Documentar:** Proporcionar documentos para acreditar algo que se dice o se escribe.
- **Efectividad:** es la capacidad de lograr un efecto deseado, esperado o anhelado.
- **Esquema Gubernamental de Seguridad de la Información – EGSI.-** Directrices elaboradas en base a la norma NTE INEN-ISO/IEC 27002 “Código de Práctica para la Gestión de Seguridad de la Información” con la finalidad de reducir amenazas, riesgos y vulnerabilidades relacionadas a la gestión de la información, tanto física y electrónica; y, orientado a personas, procesos y sistemas de las entidades de la función ejecutiva.
- **Estatuto Orgánico por Procesos.-** Instrumento normativo que regulará los lineamientos bajos los cuales se organizará la institución a fin de desarrollar adecuadamente sus funciones sustantivas, adjetivas y la proyección de su sistema.
- **Evento:** es una acción que es detectada por un programa; éste, a su vez, puede hacer uso del mismo o ignorarlo.
- **Firewall:** comprueba la información procedente de Internet o de una red y, a continuación, bloquea o permite el paso de ésta al equipo, en función de la configuración del firewall.

Elaborado por:	Revisado por:	Aprobado /Autorizado por:	Registrado por:
PC	DIPLA - DITIC	DIREJ	DIPLA, PC

- **Gateway:** es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación.
- **Gestión de red:** Consiste en monitorizar y controlar los recursos de una red con el fin de evitar que esta llegue a funcionar incorrectamente degradando sus prestaciones
- **Gestión del Riesgo.-** Consiste en detectar oportunamente los riesgos que pueden afectar a la empresa, para generar estrategias que se anticipen a ellos y los conviertan en oportunidades de rentabilidad para la empresa.
- **Hardware:** Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.
- **Incidente de Seguridad.-** Es un hecho o amenaza que atenta contra la confidencialidad, integridad o disponibilidad de un sistema de seguridad de información.
- **Incidente:** Reporte de un proceso fallido. Es la violación o amenaza inminente a la Política de Seguridad de la Información implícita o explícita.
- **Información:** Conjunto de conocimientos representados de forma discreta mediante un conjunto de símbolos. Es una entidad de orden superior a los datos, ya que estos se suponen información elaborada.
- **Inventario:** El inventario es aquel registro documental de los bienes y demás objetos pertenecientes a una persona física u organización y que se encuentra realizado a partir de mucha precisión y prolijidad en la plasmación de los datos
- **IT:** Gestión de Infraestructura de Tecnologías de la Información.
- **Librería de software:** Conjunto de funciones pres compilados que se unen a un programa en tiempo de compilación. Se agrupan según funcionalidades determinadas y permiten simplificar tareas complejas en fase de programación
- **Metadatos:** literalmente «sobre datos», son datos que describen otros datos. En general, un grupo de metadatos se refiere a un grupo de datos, llamado recurso.
- **Modelo entidad-relación:** Un diagrama o modelo entidad-relación (a veces denominado por sus siglas en inglés, E-R "Entity relationship", o del español DER "Diagrama de Entidad Relación") es una herramienta para el modelado de datos que permite representar las entidades relevantes de un sistema de información así como sus interrelaciones y propiedades.
- **Monitoreo:** describe el uso de un sistema que constantemente monitoriza una red de computadoras en busca de componentes defectuosos o lentos, para luego informar a los administradores de redes mediante correo electrónico, pager u otras alarmas.

Elaborado por:	Revisado por:	Aprobado /Autorizado por:	Registrado por:
PC	DIPLA - DITIC	DIREJ	DIPLA, PC



- **NAS:** Network Attached Storage, los sistemas NAS son dispositivos de almacenamiento a los que se accede desde los equipos a través de protocolos de red (normalmente TCP/IP). También se podría considerar un sistema NAS a un servidor (Microsoft Windows, Linux, etcétera) que comparte sus unidades por red, pero la definición suele aplicarse a sistemas específicos.
- **Niveles de Servicio:** es, simplemente, un acuerdo contractual entre una empresa de servicios y su cliente, donde se define, fundamentalmente, el servicio y los compromisos de calidad.
- **Paquetes:** Conjunto de caracteres, valores alfanuméricos o binarios.
- **PC:** Gestión de Servicios, Procesos y Calidad.
- **Perfil de usuario:** El perfil de usuario es una colección de opciones de configuración que hacen que el equipo tenga el aspecto y funcione de la manera que el usuario lo requiera.
- **Permisos de acceso:** Permite restringir o permitir el acceso de un determinado usuario a un archivo para su visualización de contenidos, modificación y/o ejecución.
- **Ping:** comprueba el estado de la comunicación del host local con uno o varios equipos remotos de una red IP por medio del envío de paquetes ICMP de solicitud y de respuesta.
- **Plan de Contingencia.-** Es un tipo de plan preventivo, predictivo y reactivo. Presenta una estructura estratégica y operativa que ayudará a controlar una situación de emergencia y a minimizar sus consecuencias negativas, intenta garantizar la continuidad del funcionamiento de la organización frente a cualquier eventualidad, ya sean materiales o personales. Un plan de contingencia incluye cuatro etapas básicas: la evaluación, la planificación, las pruebas de viabilidad y la ejecución.
- **Plan de emergencia:** Plan documentado que aborda la reacción inmediata y la respuesta a una situación de emergencia.
- **Políticas Públicas.-** Proceso integrador de decisiones, acciones, inacciones, acuerdos e instrumentos, adelantado por autoridades públicas con la participación eventual de los particulares, y encaminado a solucionar o prevenir una situación definida como problemática. La política pública hace parte de un ambiente determinado del cual se nutre y al cual pretende modificar o mantener.
- **Portal Web:** sitio web que sirve de punto de partida para navegar por Internet. Los portales ofrecen una gran diversidad de servicios: listado de sitios web, buscador, noticias, e-mail, información meteorológica, chat, news groups (grupos de discusión) y comercio electrónico.
- **Procedimiento de Acceso:** Conjunto de pasos para realizar determinada operación.
- **Procedimientos.-** Conjunto de operaciones o acciones que se realizan de la misma manera y bajo las mismas circunstancias, para lograr el mismo resultado.
- **Procesos Críticos:** Los procesos que podemos calificar como críticos son aquellos que de alguna forma hacen que nuestro negocio siga funcionando.

Elaborado por:	Revisado por:	Aprobado /Autorizado por:	Registrado por:
PC	DIPLA - DITIC	DIREJ	DIPLA, PC



- **Quipux:** Sistema de Gestión Documental, proyecto de documentación cero papeles.
- **Recuperación de Datos:** Restauración de los archivos de ordenador desde los soportes de copia de seguridad para restaurar programas y datos de producción al estado en que se encontraban en el momento de la última copia de seguridad
- **RespalDOS:** Procesos que se refiere a guardar información o datos en medios de almacenamiento sean ópticos o magnéticos
- **Respuesta Automática:** Respuesta automática es cualquier respuesta que es generada automáticamente por una aplicación.
- **Restauración de datos:** Restauración de los archivos de ordenador desde los soportes de copia de seguridad para restaurar programas y datos de producción al estado en que se encontraban en el momento de la última copia de seguridad
- **SAN:** Storage Área Network es una red de almacenamiento integral. Se trata de una arquitectura completa que agrupa los siguientes elementos: Una red de alta velocidad de canal de fibra o iSCSI. Un equipo de interconexión dedicado (conmutadores, puentes, entre otros), elementos de almacenamiento de red (discos duros).
- **Seguridad Informática.-** Disciplina que se relaciona a diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios.
- **Servicio:** Conjunto de actividades interrelacionadas que ofrece un suministrador con el fin de que el cliente obtenga el producto en el momento y lugar adecuado y se asegure un uso correcto del mismo.
- **Servidor de cuchilla:** Un servidor blade o cuchillas es un tipo de computadora para los centros de proceso de datos específicamente diseñada para aprovechar el espacio, reducir el consumo y simplificar su explotación.
- **Servidor de rack:** Los servidores tipo Rack, a diferencia de los de torre, son compactos, existen servidores de distintas medidas ya sean 1U, 2U, 4U, 8U, etc.
- **Servidor de torre:** Una torre de servidores es un grupo de servidores, normalmente mantenidos por una empresa o universidad para ejecutar tareas que van más allá de la capacidad de una sola máquina corriente, como alternativa, generalmente más económica, a un superordenador.
- **Servidor proxy:** Un proxy, o servidor proxy, en una red informática, es un servidor (un programa o sistema informático), que hace de intermediario en las peticiones de recursos que realiza un cliente (A) a otro servidor (C).
- **Servidor:** Se llama así a un ordenador central de un sistema de red que proporciona servicios y programas a otros ordenadores conectados.
- **SI:** Gestión de Seguridad Informática, Interoperabilidad y Riesgos.

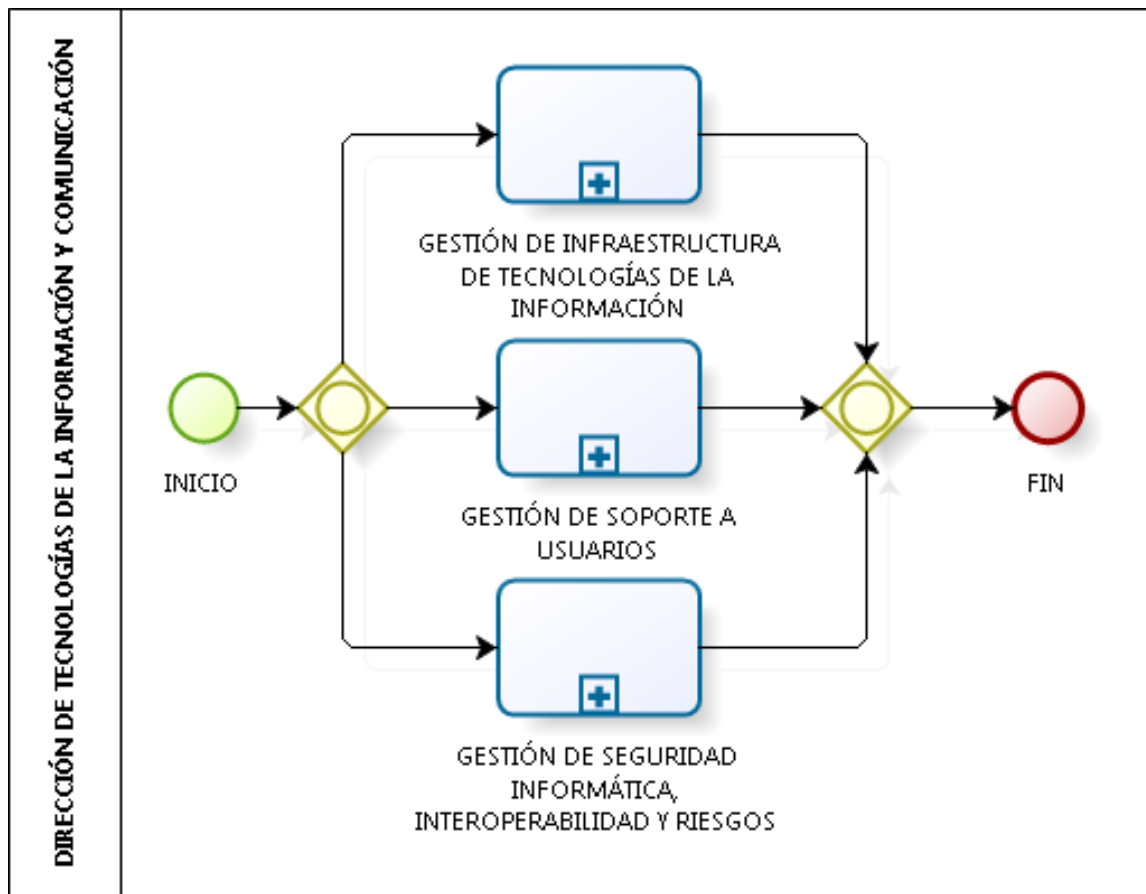
<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------



- **Sistema de UPS:** Sistema de alimentación ininterrumpida (SAI), en inglés uninterruptible power supply (UPS), es un dispositivo que gracias a sus baterías u otros elementos almacenadores de energía, puede proporcionar energía eléctrica por un tiempo limitado y durante un apagón eléctrico a todos los dispositivos que tenga conectados.
- **Sistema GPR.-** GPR es una herramienta que permite orientar las acciones del Gobierno y sus instituciones al cumplimiento de objetivos nacionales y resultados concretos que mejoran la ejecución del presupuesto gubernamental, a través de un *Balance Scored Card*.
- **SNMP:** Es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.
- **Software:** Parte lógica del ordenador. Se trata de un conjunto de órdenes lógicas cuya ejecución permite al usuario realizar un trabajo con el ordenador. Son los llamados "programas".
- **SU:** Gestión de Soporte a Usuarios.
- **Tecnologías de la Información y Comunicación (TIC).-** Son el conjunto de tecnologías desarrolladas para gestionar información y enviarla de un lugar a otro, también permiten la adquisición, producción, tratamiento, comunicación, registro y presentación de información, en forma de voz, imágenes y datos contenidos en señales de naturaleza acústica, óptica o electromagnética. Incluyen las tecnologías para almacenar información y recuperarla después, enviar y recibir información de un sitio a otro, o procesar información para poder calcular resultados y elaborar informes. Incluyen la electrónica como tecnología base que soporta el desarrollo de las telecomunicaciones, la informática y el audiovisual.
- **Tiempo de indisponibilidad:** Petición fallida de envío de paquetes.
- **UPS:** Uninterruptible Power Supply, es un dispositivo que gracias a sus baterías u otros elementos almacenadores de energía, puede proporcionar energía eléctrica por un tiempo limitado y durante un apagón eléctrico a todos los dispositivos que tenga conectados. Otras de las funciones que se pueden adicionar a estos equipos es la de mejorar la calidad de la energía eléctrica que llega a las cargas, filtrando subidas y bajadas de tensión y eliminando armónicos de la red en el caso de usar corriente.
- **Usuario final:** En informática, el término usuario final designa a la persona o personas que van a manipular de manera directa un producto de software o hardware.
- **Usuarios o clientes internos:** Son aquellas personas dentro de la Empresa u organización.

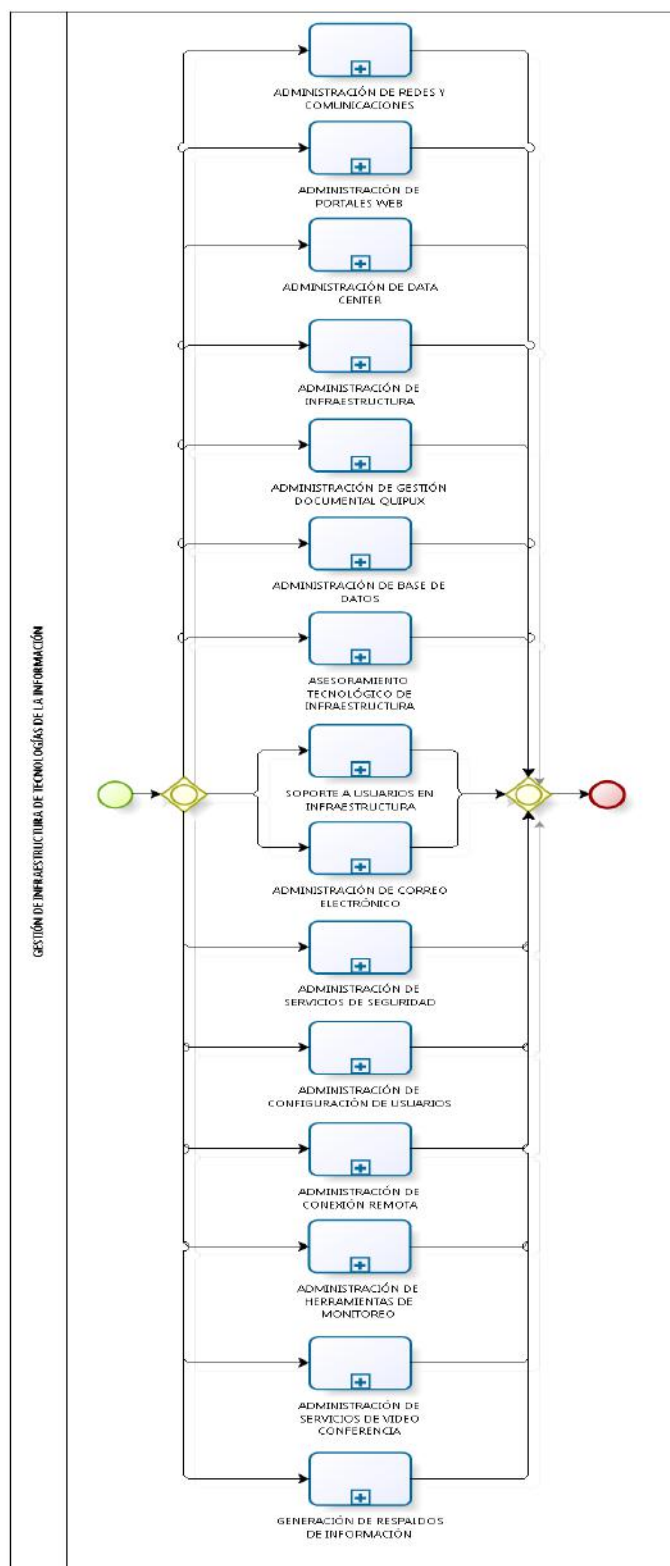
Elaborado por:	Revisado por:	Aprobado /Autorizado por:	Registrado por:
PC	DIPLA - DITIC	DIREJ	DIPLA, PC

## 4. MAPA DE INTERRELACIÓN



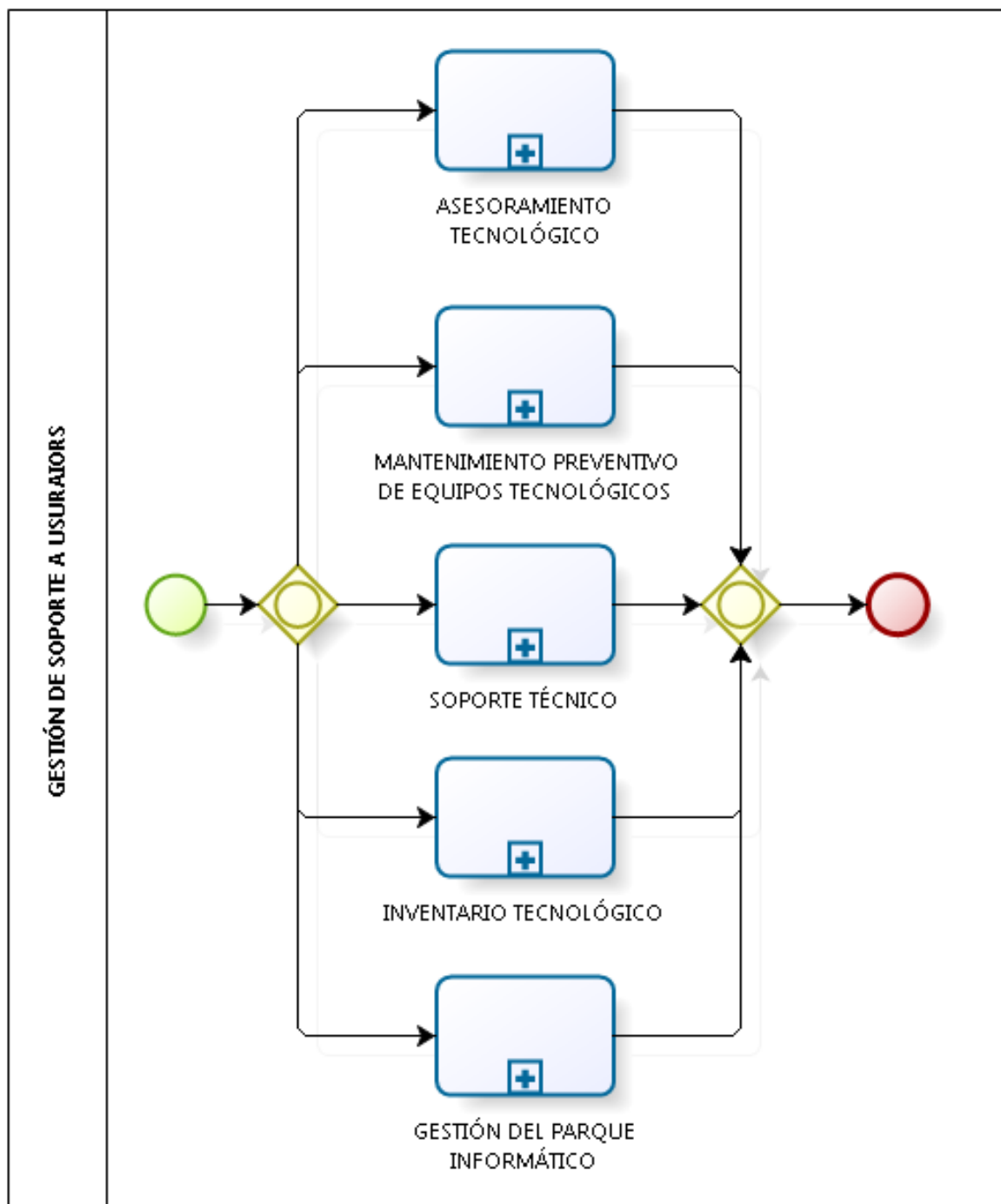
<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

## GESTIÓN DE INFRAESTRUCTURA DE TECNOLOGÍAS DE LA INFORMACIÓN



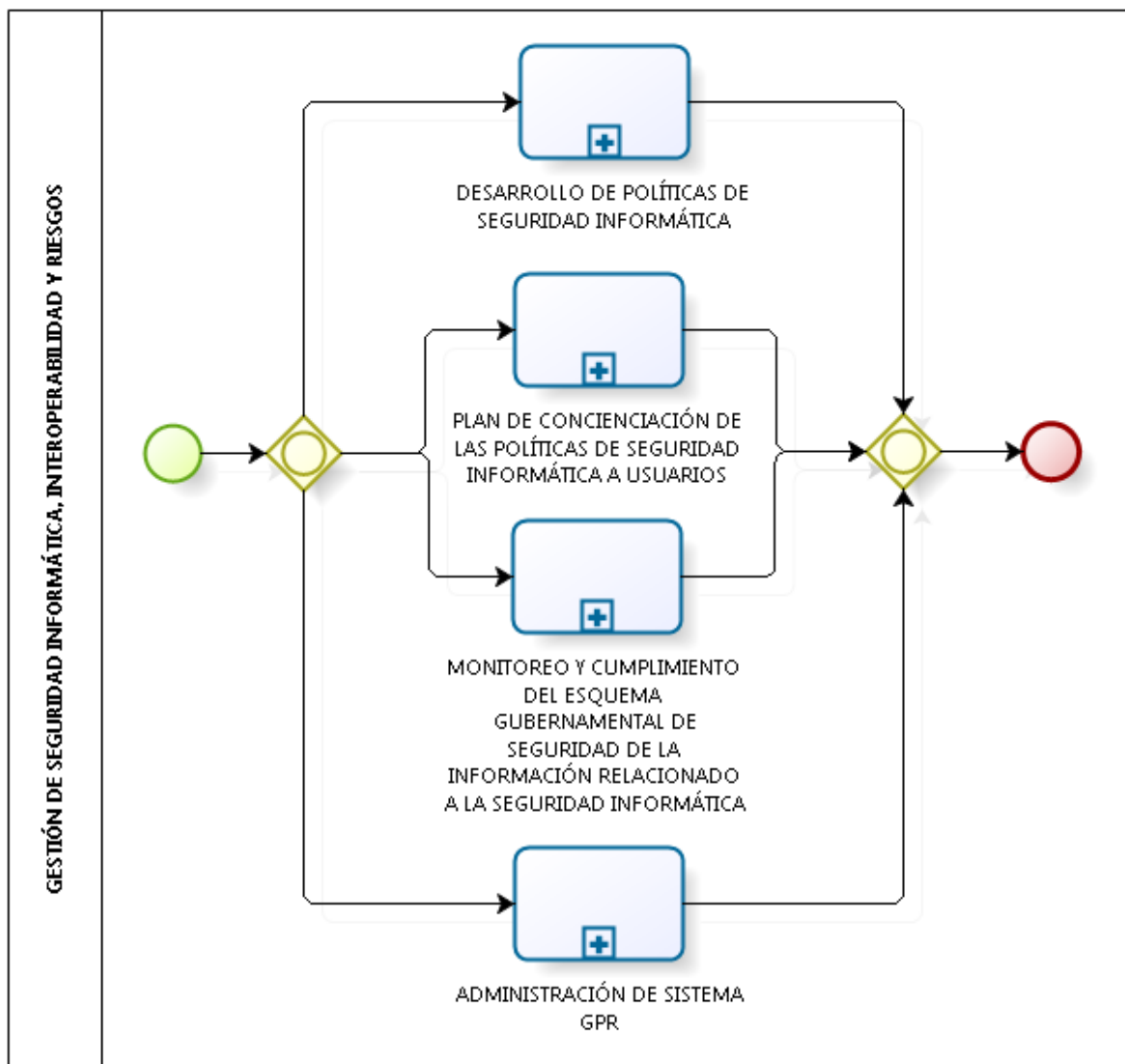
<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

## GESTIÓN DE SOPORTE A USUARIOS



<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

## GESTIÓN DE SEGURIDAD INFORMÁTICA, INTEROPERABILIDAD Y RIESGOS



<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

## 5. DESCRIPCIÓN DE LOS SUBPROCESOS DE LA GESTIÓN DE INFRAESTRUCTURA DE TECNOLOGÍAS DE LA INFORMACIÓN

### 5.1. SUBPROCESO DE ADMINISTRACIÓN DE REDES Y COMUNICACIONES

#### 5.1.1. FICHA TÉCNICA DEL SUBPROCESO DE ADMINISTRACIÓN DE REDES Y COMUNICACIONES

<b>Proceso:</b>	GESTIÓN DE INFRAESTRUCTURA DE TECNOLOGÍAS DE LA INFORMACIÓN
<b>Nombre del Subproceso:</b>	ADMINISTRACIÓN DE REDES Y COMUNICACIONES
<b>Código del Subproceso:</b>	DITIC-IT-SP1
<b>Descripción:</b>	<p><b>PROPÓSITO:</b> Asegurar y garantizar una adecuada protección de la información en los procesos de transmisión y recepción de datos en las redes internas y externas del INEC.</p> <p><b>ALCANCE:</b> Desde analizar si la administración de redes y comunicaciones es semestral o diaria, hasta enviar al director el informe técnico para su conocimiento.</p> <p><b>DISPARADOR:</b></p> <ul style="list-style-type: none"> <li>• Memorando</li> <li>• Correo electrónico</li> </ul> <p><b>PROVEEDORES:</b></p> <ul style="list-style-type: none"> <li>• Unidades del INEC.</li> <li>• Dirección de Registros Administrativos.</li> </ul> <p><b>INSUMOS:</b></p> <ul style="list-style-type: none"> <li>• Plan de Contingencia.</li> </ul>
<b>Clientes:</b>	<ul style="list-style-type: none"> <li>• Unidades del INEC.</li> </ul>
<b>Salidas:</b>	<ul style="list-style-type: none"> <li>• Informe técnico de ejecución</li> <li>• Correo electrónico.</li> </ul>
<b>Tipo de Proceso:</b>	<ul style="list-style-type: none"> <li>• Adjetivo de asesoría</li> </ul>
<b>Responsable del Proceso:</b>	Responsable de la Unidad de Gestión de Infraestructura de TI
<b>Recursos:</b>	<p><b>MATERIALES:</b></p> <ul style="list-style-type: none"> <li>• Equipo de computación</li> <li>• Equipo y materiales de oficina.</li> </ul> <p><b>HUMANOS:</b></p> <ul style="list-style-type: none"> <li>• 1 analistas de Gestión de Infraestructura de TI SP5.</li> <li>• 1 analistas de Gestión de Infraestructura de TI SP7.</li> </ul>

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------



	<b>TECNOLÓGICOS:</b> <ul style="list-style-type: none"> <li>• Correo Electrónico.</li> <li>• Software Ofimática.</li> <li>• Dispositivos de comunicación.</li> <li>• Dispositivos de seguridad perimetral.</li> </ul>
<b>Controles/Marco Legal:</b>	<p>Resolución 030- direj-diju-ni2012 uso de los servicios tecnológicos y políticas de la dirección de tecnologías de la información y comunicación del instituto nacional de estadística y censos</p> <ul style="list-style-type: none"> <li>• Normativa de seguridad de la información</li> <li>• Norma seguridad en las comunicaciones</li> </ul> <p>Normas de control interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos de la contraloría</p> <ul style="list-style-type: none"> <li>• 410 norma de tecnología de la información</li> <li>• 410-12 administración de soporte de tecnología de información</li> <li>• 410-13 monitoreo y evaluación de los procesos y servicios</li> </ul> <p>Acuerdo 166 de la secretaria de la administración pública esquema gubernamental de la seguridad de la información (EGSI)</p> <ol style="list-style-type: none"> <li>1. Política de seguridad de la información</li> <li>2. Organización de la seguridad de la información</li> <li>3. Gestión de los activos</li> <li>4. Seguridad de los recursos humanos</li> <li>5. Seguridad física y del entorno</li> <li>6. Gestión de comunicaciones y operaciones</li> <li>7. Control de acceso.</li> <li>8. Adquisición, desarrollo y mantenimiento de sistemas de información.</li> <li>9. Gestión de los incidentes de la seguridad de la información.</li> <li>10. Gestión de la continuidad del negocio.</li> <li>11. Cumplimiento.</li> </ol>

### 5.1.2. CONTROLES DEL SUBPROCESO DE ADMINISTRACIÓN DE REDES Y COMUNICACIONES

Resolución 030- DIREJ-DIJU-NI2012 Uso de Los servicios Tecnológicos y Políticas de la Dirección de Tecnologías de la Información y Comunicación del Instituto Nacional de Estadística Y Censos

- Normativa De Seguridad de La información
- Norma Comunicaciones

#### Objetivo

Definir las reglas generales para establecer una adecuada protección de la información en los procesos de transmisión y recepción de datos en las redes internas y externas del INEC.

#### Serán Responsables:

Todo el personal del área de DITIC del INEC y los terceros que interactúan de manera habitual u ocasional que estén vinculados a los procesos de transmisión de datos en el desarrollo de sus tareas habituales.

<b>Elaborado por:</b>	<b>Revisado por:</b>	<b>Aprobado /Autorizado por:</b>	<b>Registrado por:</b>
PC	DIPLA - DITIC	DIREJ	DIPLA, PC



### **Incumplimientos**

Las medidas disciplinarias serán aplicadas según resolución publicada, la normativa interna y las que determinaren las entidades de control del estado ecuatoriano.

### **Definiciones**

Conexiones internas, adicionalmente a las medidas de protección física y de acceso de usuarios ya definidas en las respectivas normas, se deben tener en cuenta las siguientes consideraciones adicionales:

- Utilizar switches, no sólo para conectar los distintos segmentos de la red interna, sino también para conectar las distintas estaciones de trabajo y servidores entre sí.
- Verificar que existan los adecuados mecanismos de encriptación para la información sensible propia de los sistemas (contraseñas, bases de datos de seguridad o similares).
- Documentar y utilizar un estándar de direccionamiento IP teniendo en cuenta las direcciones privadas definidas en normas internacionales para evitar que éstas sean accesibles desde el exterior.
- Utilizar sistemas de detección de intrusos que permitan la detección de posibles ataques y tomen acciones automáticas para prevenirlos.
- Asegurarse que todas las conexiones externas con la red interna del INEC se realicen a través de puntos controlados, que deben contemplar entre otras cosas, puertos y estaciones de trabajo que simultáneamente estén conectadas a la red interna.

### **Conexiones externas:**

En forma general, todas las conexiones externas a la red del INEC deben cumplir las siguientes consideraciones:

- El origen de todas las conexiones remotas debe ser autorizada utilizando un nivel de acceso por perfil de usuario.
- Todo acceso a la red interna del INEC debe realizarse a través de una red segmentada (DMZ - zona desmilitarizada).
- Las conexiones externas podrán acceder solamente a los servicios, sistemas y/o aplicaciones a los que están autorizados.
- Deben transmitirse en forma cifrada todos los datos considerados de acceso autorizado y/o sensible, a través de la red WAN utilizando clave pública y privada o certificados.
- Los accesos externos deben ser registrados (en una bitácora o archivo de log) a fin de determinar posibles intentos de accesos no autorizados.
- Debe incluirse en los contratos con los proveedores la utilización de otra vía alternativa ante interrupciones en el servicio.

Aspectos particulares de los distintos tipos de accesos externos:

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------



## Internet

Todo contrato con un proveedor de servicios de Internet debe contemplar la descripción de todos los servicios provistos. Todas las conexiones deben realizarse a través de un Firewall. En el caso particular de las conexiones salientes, éstas deben ser validadas a través de un servidor del tipo “AAA” (que verifica la autenticidad - Authentication, la autorización - Authorization y el monitoreo - Accounting de la cuenta de usuario) a fin de controlar los accesos de los usuarios, para lo cual se debe llevar un registro de los servicios utilizados y como mínimo la cuenta de usuario, la dirección IP accedida, la dirección URL accedida, la fecha y la hora. En el caso de las conexiones entrantes, se debe llevar registro de los intentos fallidos que contenga la dirección IP de origen, el servicio requerido, el motivo del rechazo, la fecha y la hora.

### **NORMAS DE CONTROL INTERNO PARA LAS ENTIDADES, ORGANISMOS DEL SECTOR PÚBLICO Y PERSONAS JURÍDICAS DE DERECHO PRIVADO QUE DISPONGAN DE RECURSOS PÚBLICOS- DE LA CONTRALORIA**

- 410 Norma de tecnología de la información
- 410-12 Administración de soporte de tecnología de información

La unidad de tecnología de información definirá, aprobará y difundirá procedimientos de operación que faciliten una adecuada administración del soporte tecnológico y garanticen la seguridad, integridad, confiabilidad y disponibilidad de los recursos y datos, tanto como la oportunidad de los servicios tecnológicos que se ofrecen. Los aspectos a considerar son:

1. Revisiones periódicas para determinar si la capacidad y desempeño actual y futura de los recursos tecnológicos son suficientes para cubrir los niveles de servicio acordados con los usuarios.
2. Seguridad de los sistemas bajo el otorgamiento de una identificación única a todos los usuarios internos, externos y temporales que interactúen con los sistemas y servicios de tecnología de información de la entidad.
3. Estandarización de la identificación, autenticación y autorización de los usuarios, así como la administración de sus cuentas.
4. Revisiones regulares de todas las cuentas de usuarios y los privilegios asociados a cargo de los dueños de los procesos y administradores de los sistemas de tecnología de información.
5. Medidas de prevención, detección y corrección que protejan a los sistemas de información y a la tecnología de la organización de software malicioso y virus informáticos.
6. Definición y manejo de niveles de servicio y de operación para todos los procesos críticos de tecnología de información sobre la base de los requerimientos de los usuarios o clientes internos y externos de la entidad y a las capacidades tecnológicas.
7. Alineación de los servicios claves de tecnología de información con los requerimientos y las prioridades de la organización sustentados en la revisión, monitoreo y notificación de la efectividad y cumplimiento de dichos acuerdos.
8. Administración de los incidentes reportados, requerimientos de servicio y solicitudes de información y de cambios que demandan los usuarios, a través de mecanismos efectivos y oportunos como mesas de ayuda o de servicios, entre otros.
9. Mantenimiento de un repositorio de diagramas y configuraciones de hardware y software actualizado que garantice su integridad, disponibilidad y faciliten una rápida resolución de los problemas de producción.
10. Administración adecuada de la información, librerías de software, respaldos y recuperación de datos.

Elaborado por:	Revisado por:	Aprobado /Autorizado por:	Registrado por:
PC	DIPLA - DITIC	DIREJ	DIPLA, PC



11. Incorporación de mecanismos de seguridad aplicables a la recepción, procesamiento, almacenamiento físico y entrega de información y de mensajes sensitivos, así como la protección y conservación de información utilizada para encriptación y autenticación.

La unidad de tecnología de información presentará informes periódicos de gestión a la alta dirección, para que ésta supervise el cumplimiento de los objetivos planteados y se identifiquen e implanten acciones correctivas y de mejoramiento del desempeño.

**ACUERDO 166 DE LA SECRETARIA DE LA ADMINISTRACION PÚBLICA ESQUEMA GUBERNAMENTAL DE LA SEGURIDAD DE LA INFORMACION (EGSI)**

2. Organización de la seguridad de la información

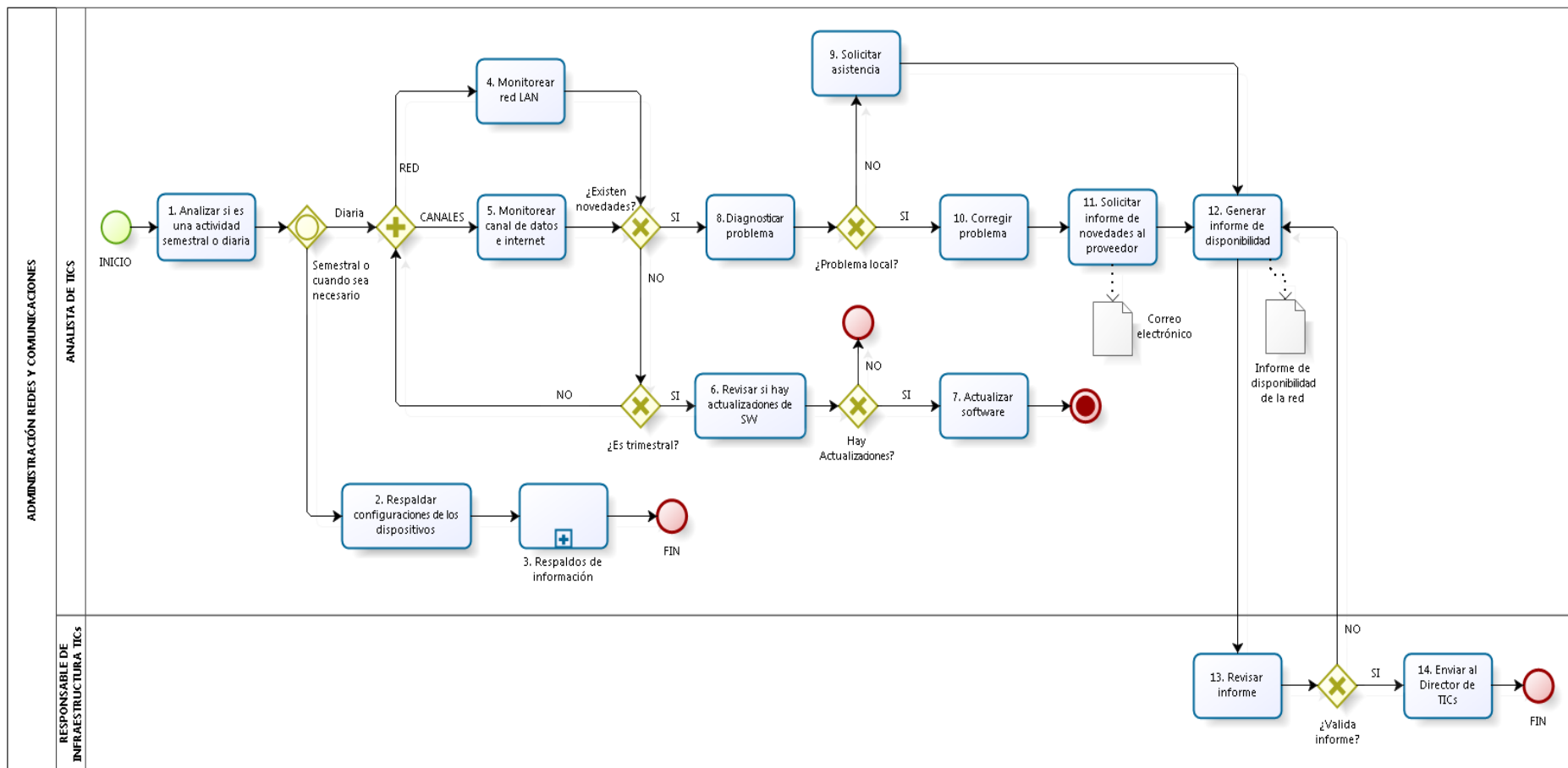
2.10 Consideraciones de la seguridad cuando se trata con ciudadanos o clientes

a) Identificar requisitos de seguridad antes de facilitar servicios a ciudadanos o clientes de entidades gubernamentales que utilicen o procesen información de los mismos o de la entidad. Se podrá utilizar los siguientes criterios:

- Protección de activos de información;
- Descripción del producto o servicio;
- Las diversas razones, requisitos y beneficios del acceso del cliente;
- Política de control del acceso;
- Convenios para gestión de inexactitudes de la información, incidentes de la seguridad de la información y violaciones de la seguridad;
- Descripción de cada servicio que va a estar disponible;
- Nivel de servicio comprometido y los niveles inaceptables de servicio;
- El derecho a monitorear y revocar cualquier actividad relacionada con los activos de la Organización;
- Las respectivas responsabilidades civiles de la organización y del cliente;
- Las responsabilidades relacionadas con asuntos legales y la forma en que se garantiza el cumplimiento de los requisitos legales
- Derechos de propiedad intelectual y asignación de derechos de copia y la protección de cualquier trabajo colaborativos
- Protección de datos en base la Constitución y leyes nacionales, particularmente datos personales o financieros de los ciudadanos

Elaborado por:	Revisado por:	Aprobado /Autorizado por:	Registrado por:
PC	DIPLA - DITIC	DIREJ	DIPLA, PC

### 5.1.3. DIAGRAMA DE FLUJO DEL SUBPROCESO DE ADMINISTRACIÓN DE REDES Y COMUNICACIONES



<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

#### 5.1.4. PROCEDIMIENTO DEL SUBPROCESO DE ADMINISTRACIÓN DE REDES Y COMUNICACIONES

N	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	DOCUMENTO GENERADO
1	Analizar si es una actividad semestral o diaria.	Analiza si la administración de redes y comunicaciones es semestral o diaria.	Analista de Infraestructura	N/A
	Decisión	<b>¿Es semestral o diaria?</b> <b>Semestral o cuando sea necesario:</b> Realiza las actividades 2 – 3. <b>Diaria:</b> Continúa con la Decisión <b>¿Es de Red o de Canales?</b>	Analista de Infraestructura	N/A
2	Respaldar configuraciones de los dispositivos	<b>Semestral o cuando sea necesario:</b> Realiza los respaldos de las configuraciones de los dispositivos de manera mensual	Analista de Infraestructura	Carpeta compartida
3	Respaldos de información	Realiza los respaldos de la información para su almacenamiento. <b>Fin del proceso.</b>	Analista de Infraestructura	N/A
	Decisión	<b>¿Es de Red o de Canales?</b> <b>Red:</b> Realiza la actividad 4. Monitorear red LAN. <b>Canales:</b> Realiza la actividad 5. Monitorear canales de datos e internet.	Analista de Infraestructura	N/A
4	Monitorear red LAN	<b>Diaria Red:</b> Realiza un monitoreo de la red LAN de manera diaria. Continúa con la decisión <b>¿Existen novedades?</b>	Analista de Infraestructura	N/A
5	Monitorear canal de datos e internet	<b>Diaria Canales:</b> Monitorea el canal de datos e internet de manera diaria.	Analista de Infraestructura	N/A
	Decisión	<b>¿Existen novedades?</b> <b>No:</b> Continúa con la decisión <b>¿Es trimestral?</b> <b>SI:</b> Realiza la actividad 8. Diagnosticar problema.	Analista de Infraestructura	N/A
	Decisión	<b>¿Es trimestral?</b> <b>NO:</b> Regresa a la decisión <b>¿Es de Red o de Canales?</b> <b>SI:</b> Revisar si hay actualizaciones de SW, pasa a la actividad 5.	Analista de Infraestructura	N/A
6	Revisar si hay actualizaciones de SW	Revisa si existe actualizaciones de software	Analista de Infraestructura	N/A
	Decisión	<b>¿Hay Actualizaciones?</b> <b>NO:</b> Fin del proceso.	Analista de Infraestructura	N/A

Elaborado por: PC	Revisado por: DIPLA - DIFI	Aprobado /Autorizado por: DIREJ	Registrado por: DIPLA, PC
----------------------	-------------------------------	------------------------------------	------------------------------



		<b>SI:</b> Realiza la actividad <b>7.</b> Actualizar software.		
7	Actualizar software, fin	Actualiza el software según la planificación realizada. <b>Fin del proceso.</b>	Analista de Infraestructura	N/A
8	Diagnosticar problema	<b>Existen novedades:</b> Diagnostica el problema en función del requerimiento realizado o el problema detectado.	Analista de Infraestructura	N/A
	Decisión	<b>¿Problema local?</b> <b>NO:</b> Realiza la actividad <b>9.</b> Solicitar asistencia. <b>SI:</b> Realiza la actividad <b>10.</b> Corregir problema, pasa a la actividad <b>10.</b>	Analista de Infraestructura	N/A
9	Solicitar asistencia	Solicita la asistencia para la reparación de los equipos informáticos, al proveedor de comunicaciones o al proveedor de garantía de los equipos del INEC. Continúa con la actividad <b>12.</b>	Analista de Infraestructura	Correo electrónico / Ticket (proveedor de equipo)
10	Corregir problema	Corrige el problema según análisis que se realizó al equipo informático	Proveedor	N/A
11	Solicitar informe de novedades al proveedor	Solicita el informe de las novedades encontradas al proveedor de comunicaciones o al proveedor de garantía de los equipos.	Analista de Infraestructura	Correo electrónico
12	Generar informe de disponibilidad	Genera el informe de disponibilidad de la red institucional	Analista de Infraestructura	Informe de disponibilidad de la red
13	Revisar informe	Revisa el informe para conocer las acciones realizadas para solucionar inconveniente	Responsable de Infraestructura TICs	N/A
	Decisión	<b>¿Valida informe?</b> <b>NO:</b> Regresa a la actividad <b>12.</b> Generar informe de disponibilidad. <b>SI:</b> Enviar al Director de TICs. <b>Fin del proceso.</b>	Responsable de Infraestructura TICs	N/A
14	Enviar al Director de TICs, fin	Envía al director el informe técnico para su conocimiento.	Responsable de Infraestructura TICs	Correo electrónico / Memorando

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------



#### 5.1.5. INDICADORES DEL SUBPROCESO DE ADMINISTRACIÓN DE REDES Y COMUNICACIONES

N°	Indicador	Fórmula de Cálculo	Unidad de Medida	Responsable de Medición	Fuente de Medición	Frecuencia de Medición
1	Porcentaje de disponibilidad de red	$((\text{Tiempo total sondeo} - \text{tiempo no disponible}) / \text{tiempo total de sondeo}) * 100\%$	%	Responsable de la Unidad de Infraestructura de TI	Reporte de Software WhatsUp	Trimestral

#### 5.1.6. FORMATOS DEL SUBPROCESO DE ADMINISTRACIÓN DE REDES Y COMUNICACIONES

Nombre del Registro de Calidad	Código de Formato
N/A	N/A

#### 5.1.7. ANEXOS DEL SUBPROCESO DE ADMINISTRACIÓN DE REDES Y COMUNICACIONES

“No hay anexos.”

Elaborado por: PC	Revisado por: DIPLA - DIFI	Aprobado /Autorizado por: DIREJ	Registrado por: DIPLA, PC
----------------------	-------------------------------	------------------------------------	------------------------------

## 5.2. SUBPROCESO DE ADMINISTRACIÓN DE PORTALES WEB

### 5.2.1. FICHA TÉCNICA DEL SUBPROCESO DE ADMINISTRACIÓN DE PORTALES WEB

<b>Proceso:</b>	GESTIÓN DE INFRAESTRUCTURA DE TECNOLOGÍAS DE LA INFORMACIÓN
<b>Nombre del Subproceso:</b>	ADMINISTRACIÓN DE PORTALES WEB
<b>Código del Subproceso:</b>	DIFI-IT-SP2
<b>Descripción:</b>	<p><b>PROPÓSITO:</b></p> <p>Mantener el adecuado control, funcionamiento, gestión y estabilidad de la infraestructura (Hardware y Software) de los portales Web así como asegurar la disponibilidad de los mismos para los usuarios internos y externos de la institución.</p> <p><b>ALCANCE:</b></p> <ul style="list-style-type: none"> <li>Desde analizar y remitir requerimiento, hasta elaborar informe de disponibilidad de aplicaciones.</li> </ul> <p><b>DISPARADOR:</b></p> <ul style="list-style-type: none"> <li>Memorando de solicitud.</li> <li>Correo electrónico.</li> </ul> <p><b>PROVEEDORES:</b></p> <ul style="list-style-type: none"> <li>Dirección de Registros Administrativos.</li> </ul> <p><b>INSUMOS:</b></p> <ul style="list-style-type: none"> <li>Solicitud de la Dirección de Registros Administrativos.</li> </ul>
<b>Clientes:</b>	<ul style="list-style-type: none"> <li>Dirección de Registros Administrativos.</li> </ul>
<b>Salidas:</b>	<ul style="list-style-type: none"> <li>Informe de disponibilidad.</li> </ul>
<b>Tipo de Proceso:</b>	<ul style="list-style-type: none"> <li>Adjetivo de asesoría.</li> </ul>
<b>Responsable del Proceso:</b>	Responsable de la Unidad de Gestión de Infraestructura de TI
<b>Recursos:</b>	<p><b>MATERIALES:</b></p> <ul style="list-style-type: none"> <li>Equipo de computación</li> <li>Equipo y materiales de oficina.</li> </ul> <p><b>HUMANOS:</b></p> <ul style="list-style-type: none"> <li>2 analistas de Gestión de Infraestructura de TI SP5.</li> </ul> <p><b>TECNOLÓGICOS:</b></p> <ul style="list-style-type: none"> <li>Correo Electrónico.</li> <li>Software Ofimática.</li> <li>Software de monitoreo de virtualización.</li> </ul>

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------

<b>Controles/Marco Legal:</b>	<p>Acuerdo N° 166 de la secretaria de la administración pública esquema gubernamental de seguridades de la información (EGSI).</p> <ol style="list-style-type: none"> <li>1. Política de seguridad de la información</li> <li>2. Organización de la seguridad de la información</li> <li>3. Gestión de los activos</li> <li>4. Seguridad de los recursos humanos</li> <li>5. Seguridad física y del entorno</li> <li>6. Gestión de comunicaciones y operaciones</li> <li>7. Control de acceso</li> <li>8. Adquisición, desarrollo y mantenimiento de sistemas de información</li> <li>9. Gestión de los incidentes de la seguridad de la</li> <li>10. Gestión de la continuidad del negocio</li> <li>11. Cumplimiento</li> </ol> <p>Normas de control interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos</p> <ul style="list-style-type: none"> <li>• 410 norma de tecnología de la información</li> <li>• 410-10 seguridad de tecnología de información</li> <li>• 410-12 administración de soporte de tecnología de información</li> <li>• 410-14 sitio web, servicios de internet e intranet</li> </ul>
-------------------------------	--

## 5.2.2. CONTROLES DEL SUBPROCESO DE ADMINISTRACIÓN DE PORTALES WEB

**ACUERDO 166 DE LA SECRETARIA DE LA ADMINISTRACION PÚBLICA ESQUEMA GUBERNAMENTAL DE LA SEGURIDAD DE LA INFORMACION (EGSI)**

### 3 GESTIÓN DE LOS ACTIVOS

#### 3.1 Inventario de Activos.

Inventariar los activos de soporte de Hardware (\*):

k) Equipos fijos: servidor de torre, servidor de cuchilla, servidor de rack, computador de escritorio, computadoras portátiles, etc.

n) Periféricos y dispositivos de almacenamiento: sistema de almacenamiento (NAS, SAN), librería de cintas, cintas magnéticas, disco duro portátil, disco flexible, grabador de discos (CD, DVD, Blu-ray), CD, DVD, Blu-ray, memoria USB, etc.

Inventariar los activos de soporte de Software (\*):

r) Sistemas operativos

u) Aplicativos informáticos del negocio.

Inventariar los activos de soporte de redes (\*):

w) Switchs (de centros de datos, de acceso, de borde, de gabinete de servidores, access-point, transceiver, equipo terminal de datos, etc.).

x) Ruteador (router), cortafuego (firewall), controlador de red inalámbrica, etc.

y) Sistema de detección/prevenición de intrusos (IDS/IPS), firewall de aplicaciones web, balanceadoras de carga, switch de contenido, etc.

#### 3.3. Uso aceptable de los activos

c) La información y documentos generados en la institución y enviados por cualquier medio o herramienta electrónica son propiedad de la misma institución.

<b>Elaborado por:</b>	<b>Revisado por:</b>	<b>Aprobado /Autorizado por:</b>	<b>Registrado por:</b>
PC	DIPLA - DIFI	DIREJ	DIPLA, PC

## 5. SEGURIDAD FÍSICA Y DEL ENTORNO

### 5.1. Perímetro de la seguridad física

- f) Aislar los ambientes de procesamiento de información de los ambientes proporcionados por terceros.

### 5.10. Mantenimiento de los equipos

- a) Brindar mantenimientos periódicos a los equipos y dispositivos, de acuerdo a las especificaciones y recomendaciones del proveedor.
- b) Realizar el mantenimiento de los equipos únicamente con personal calificado y autorizado.

### 5.12. Seguridad en la reutilización o eliminación de los equipos

- a) Destruir, borrar o sobrescribir los dispositivos que contienen información sensible utilizando técnicas que permitan la no recuperación de la información original.
- b) Evaluar los dispositivos deteriorados que contengan información sensible antes de enviar a reparación, borrar la información o determinar si se debería eliminar físicamente el dispositivo.

## 6 GESTIÓN DE COMUNICACIONES Y OPERACIONES

### 6.4. Separación de las instancias de Desarrollo, Pruebas, Capacitación y Producción.

- b) Aislar los ambientes de desarrollo, pruebas, capacitación y producción.
- d) Implantar ambientes de prueba, iguales en capacidad, a los ambientes de producción.
- e) Utilizar sistemas de autenticación y autorización independientes para las diversas instancias o ambientes.
- f) Definir perfiles de usuario para las diferentes instancias o ambientes.
- g) Aislar los datos sensibles de los ambientes de desarrollo, pruebas y capacitación
- h) Permitir al personal de desarrollo de software el acceso al entorno de producción, únicamente en caso de extrema necesidad, con la autorización explícita correspondiente

### 6.6. Monitoreo y revisión de los servicios, por terceros.

- a) Identificar los sistemas sensibles o críticos que convenga tener dentro o fuera de la institución.
- b) Monitorear los niveles de desempeño de los servicios para verificar el cumplimiento de los acuerdos (\*).
- c) Analizar los reportes de servicios, reportes de incidentes elaborados por terceros y acordar reuniones periódicas según los acuerdos (\*).

### 6.8. Gestión de la capacidad

- a) Realizar proyecciones de los requerimientos de capacidad futura de recursos para asegurar el desempeño de los servicios y sistemas informáticos (\*).
- b) Monitorear los recursos asignados para garantizar la capacidad y rendimiento de los servicios y sistemas informáticos.
- c) Utilizar la información del monitoreo para la adquisición, asignación de recursos y evitar cuellos de botella.

### 6.9. Aceptación del Sistema

- a) Verificar el desempeño y los requerimientos de cómputo necesarios para los nuevos sistemas.
- d) Garantizar la implementación de un conjunto de controles de seguridad acordados.
- e) Asegurar que la instalación del nuevo sistema no afecte negativamente los sistemas existentes, especialmente en períodos pico de procesamiento.

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------

f) Considerar el efecto que tiene el nuevo sistema en la seguridad global de la institución.

#### 6.12. Respaldo de la información.

c) Definir la extensión (completo/diferencial) y la frecuencia de los respaldos, de acuerdo a los requisitos del negocio de la institución (\*).

e) Guardar los respaldos en un sitio lejano, a una distancia suficiente para evitar cualquier daño debido a desastres en la sede principal de la institución.

i) Considerar los respaldos a discos y en el mismo sitio si se tiene suficientes recursos, ya que en caso de mantenimientos de los sistemas de información, es más rápida su recuperación.

#### 6.27. Monitoreo de uso del sistema

c) Monitorear intentos de acceso no autorizados, como (\*):

- Acciones de usuario fallidas o rechazadas;
- Violación de la política de acceso y notificaciones de firewalls y gateways;
- Alertas de los sistemas de detección de intrusos;

d) Revisar alertas o fallas del sistema, como (\*):

- Alertas y/o mensajes de consola;
- Excepciones de registro del sistema;
- Alarmas de gestión de red;
- Alarmas del sistema de control de acceso;

e) Revisar cambios o intentos de cambio en la configuración y los controles de la seguridad del sistema.

### 8 ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACION

#### 8.16. Control de las vulnerabilidades técnicas

a) Disponer de un inventario completo y actual de los activos de software. El inventario servirá para dar soporte a la gestión de la vulnerabilidad técnica e incluye los siguientes datos: vendedor del software, números de versión, estado actual de despliegue y las personas de la institución responsables del software.

b) Definir e instaurar las funciones y responsabilidades asociadas con la gestión de la vulnerabilidad técnica, incluyendo el monitoreo de la vulnerabilidad, la evaluación de riesgos de la vulnerabilidad, el uso de parches, el rastreo de activos y todas las responsabilidades de coordinación requeridas.

c) Identificar los recursos de información que se van a utilizar para identificar las vulnerabilidades técnicas pertinentes y para mantener la concienciación sobre ellas para el software y otras tecnologías, con base en la lista de inventario de activos.

h) Evaluar los riesgos asociados con la instalación de un parche para cubrir vulnerabilidades. Los riesgos impuestos por la vulnerabilidad se deberán comparar con los riesgos de instalar el parche.

i) Probar y evaluar los parches antes de su instalación para garantizar que son eficaces y no producen efectos secundarios intolerables. Estas pruebas se realizarán en un ambiente similar al de producción.

j) Apagar los servicios o capacidades relacionadas con la vulnerabilidad.

k) Adaptar o agregar controles de acceso; por ejemplo, cortafuegos (firewalls), en las fronteras de la red.

l) Aumentar el monitoreo para detectar o prevenir los ataques reales.

m) Crear conciencia en los desarrolladores sobre la vulnerabilidad.

### 10 GESTION DE LA CONTINUIDAD DEL NEGOCIO

#### 10.4. Estructura para la planificación de la continuidad del negocio

d) Definir los acuerdos de niveles de servicios internos y con proveedores.

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------



g) Describir los procedimientos de respaldo para desplazar las actividades esenciales de los servicios informáticos o los servicios de soporte a lugares temporales alternos, y para devolver la operatividad de los procesos en los plazos establecidos.

i) Definir los activos y recursos necesarios para ejecutar los procedimientos de emergencia, respaldo y reanudación de los servicios.

## NORMAS DE CONTROL INTERNO PARA LAS ENTIDADES, ORGANISMOS DEL SECTOR PÚBLICO Y PERSONAS JURÍDICAS DE DERECHO PRIVADO QUE DISPONGAN DE RECURSOS PÚBLICOS- DE LA CONTRALORIA

### 410 TECNOLOGÍA DE LA INFORMACIÓN

#### 410-10 Seguridad de tecnología de información

La unidad de tecnología de información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos, para ello se aplicarán al menos las siguientes medidas:

- Definición de procedimientos de obtención periódica de respaldos en función a un cronograma definido y aprobado;
- En los casos de actualización de tecnologías de soporte se migrará la información a los medios físicos adecuados y con estándares abiertos para garantizar la perpetuidad de los datos y su recuperación;
- Almacenamiento de respaldos con información crítica y/o sensible en lugares externos a la organización;
- Implementación y administración de seguridades a nivel de software y hardware, que se realizará con monitoreo de seguridad, pruebas periódicas y acciones correctivas sobre las vulnerabilidades o incidentes de seguridad identificados.
- Consideración y disposición de sitios de procesamiento alternativos.

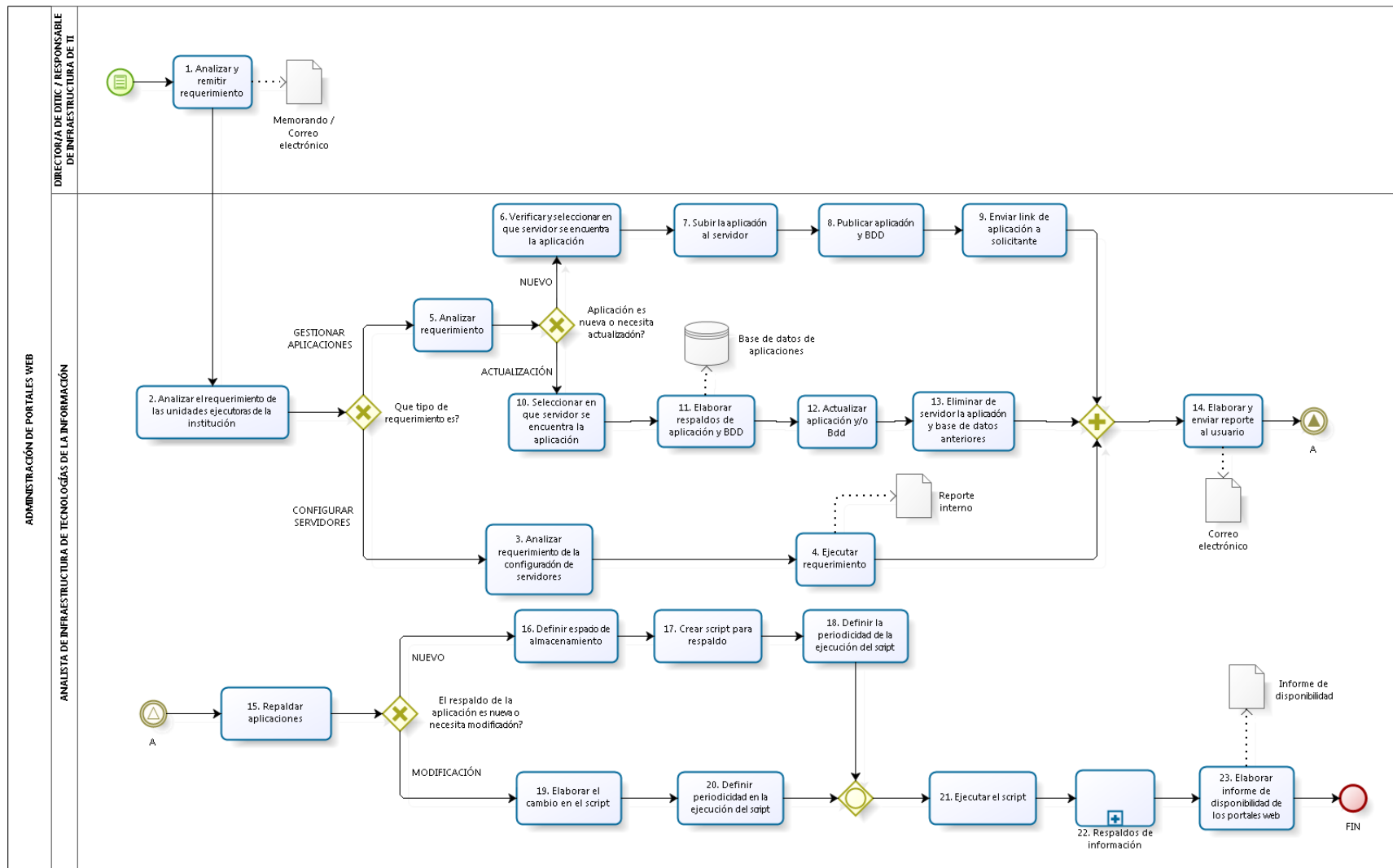
#### 410-12 Administración de soporte de tecnología de información

La unidad de tecnología de información definirá, aprobará y difundirá procedimientos de operación que faciliten una adecuada administración del soporte tecnológico y garanticen la seguridad, integridad, confiabilidad y disponibilidad de los recursos y datos, tanto como la oportunidad de los servicios tecnológicos que se ofrecen. Los aspectos a considerar son:

- Revisiones periódicas para determinar si la capacidad y desempeño actual y futura de los recursos tecnológicos son suficientes para cubrir los niveles de servicio acordados con los usuarios.
- Seguridad de los sistemas bajo el otorgamiento de una identificación única a todos los usuarios internos, externos y temporales que interactúen con los sistemas y servicios de tecnología de información de la entidad.
- Alineación de los servicios claves de tecnología de información con los requerimientos y las prioridades de la organización sustentados en la revisión, monitoreo y notificación de la efectividad y cumplimiento de dichos acuerdos.
- Administración de los incidentes reportados, requerimientos de servicio y solicitudes de información y de cambios que demandan los usuarios, a través de mecanismos efectivos y oportunos como mesas de ayuda o de servicios, entre otros.
- Mantenimiento de un repositorio de diagramas y configuraciones de hardware y software actualizado que garantice su integridad, disponibilidad y faciliten una rápida resolución de los problemas de producción.
- Administración adecuada de la información, librerías de software, respaldos y recuperación de datos.

Elaborado por:	Revisado por:	Aprobado /Autorizado por:	Registrado por:
PC	DIPLA - DIFI	DIREJ	DIPLA, PC

### 5.2.3. DIAGRAMA DE FLUJO DEL SUBPROCESO DE ADMINISTRACIÓN DE PORTALES WEB



**Elaborado por:**  
PC

**Revisado por:**  
DIPLA - DIFI

**Aprobado /Autorizado por:**  
DIREJ

**Registrado por:**  
DIPLA, PC

#### 5.2.4. PROCEDIMIENTO DEL SUBPROCESO DE ADMINISTRACIÓN DE PORTALES WEB

N	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	DOCUMENTO GENERADO
1	Analizar y remitir requerimiento	Realiza el análisis y remitir el requerimiento a la unidad según sus competencias	Director/a de DITIC / Responsable de Infraestructura de TI	Memorando / Correo electrónico
2	Analizar el requerimiento de las unidades ejecutoras de la institución	Realiza el análisis del requerimiento de las unidades ejecutoras de la institución	Analista de Infraestructura de Tecnologías de la Información	N/A
	Decisión	<b>¿Qué tipo de requerimiento es?</b> <b>CONFIGURAR SERVIDORES:</b> Realiza la actividad <b>3</b> . Analizar requerimiento de la configuración de servidores. <b>GESTIONAR APLICACIONES:</b> Realiza la actividad <b>5</b> . Analizar requerimiento.	Analista de Infraestructura de Tecnologías de la Información	N/A
3	Analizar requerimiento de la configuración de servidores	Analiza el requerimiento de la configuración de servidores.	Analista de Infraestructura de Tecnologías de la Información	N/A
4	Ejecutar requerimiento	Ejecuta el requerimiento solicitado y obtiene un reporte de lo efectuado. Continúa con la actividad <b>14</b> .	Analista de Infraestructura de Tecnologías de la Información	Reporte interno
5	Analizar requerimiento	Realiza el respectivo análisis del requerimiento.	Analista de Infraestructura de Tecnologías de la Información	N/A
	Decisión	<b>¿Aplicación es nueva o necesita actualización?</b> <b>NUEVO,</b> Verificar y seleccionar en que servidor se encuentra la aplicación, pasa a la actividad <b>6</b> <b>ACTUALIZACIÓN,</b> Seleccionar en que servidor se encuentra la aplicación, pasa a la actividad <b>10</b> .	Analista de Infraestructura de Tecnologías de la Información	N/A
6	Verificar y seleccionar en que servidor se encuentra la aplicación	<b>Nuevo</b> Realiza la verificación y selección en que el servidor se encuentra la aplicación	Analista de Infraestructura de Tecnologías de la Información	N/A
7	Subir la aplicación al servidor	Realiza la carga de la aplicación al servidor	Analista de Infraestructura de Tecnologías de la Información	N/A
8	Publicar aplicación y	Realiza la publicación de la aplicación de base	Analista de Infraestructura de	N/A
Elaborado por: PC		Revisado por: DIPLA - DIFI	Aprobado /Autorizado por: DIREJ	Registrado por: DIPLA, PC



	BDD	de datos	Tecnologías de la Información	
9	Enviar link de aplicación a solicitante	Realiza el envío del link de la aplicación al solicitante. Continúa con la actividad <b>14</b> .	Analista de Infraestructura de Tecnologías de la Información	Correo electrónico
10	Seleccionar en que servidor se encuentra la aplicación	<b>Actualización:</b> Realiza la selección del servidor donde se encuentra la aplicación	Analista de Infraestructura de Tecnologías de la Información	N/A
11	Elaborar respaldos de aplicación y base de datos	Realiza la elaboración de los respaldos de aplicación y base de datos.	Analista de Infraestructura de Tecnologías de la Información	N/A
12	Actualizar aplicación y/o base de datos	Realiza la actualización de la aplicación y/o base de datos.	Analista de Infraestructura de Tecnologías de la Información	N/A
13	Eliminar de servidor la aplicación y base de datos anteriores	Realiza la eliminación del servidor de la aplicación y base de datos anteriores.	Analista de Infraestructura de Tecnologías de la Información	N/A
14	Elaborar y enviar reporte al usuario, fin	Realiza la elaboración y envía la notificación de la atención al requerimiento solicitado.	Analista de Infraestructura de Tecnologías de la Información	Correo electrónico
15	Inicio 2, Respaldo aplicaciones	<b>Una vez atendido el requerimiento:</b> Realiza los respaldos de las aplicaciones gestionadas.	Analista de Infraestructura de Tecnologías de la Información	N/A
	Decisión	<b>¿El respaldo de la aplicación es nuevo o necesita modificación?</b> <b>NUEVO</b> , Definir espacio de almacenamiento, pasa a la actividad <b>16</b> . <b>MODIFICACIÓN</b> , Elaborar el cambio en el script, pasa a la actividad <b>19</b> .	Analista de Infraestructura de Tecnologías de la Información	N/A
16	Definir espacio de almacenamiento	<b>Nuevo:</b> Realiza la definición del espacio de almacenamiento informático	Analista de Infraestructura de Tecnologías de la Información	N/A
17	Crear script para respaldo	Realiza creación del script para el respaldo informático	Analista de Infraestructura de Tecnologías de la Información	N/A
18	Definir la periodicidad	Realiza la definición de la periodicidad de la	Analista de Infraestructura de	N/A

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------

	de la ejecución del script	ejecución del script. Continúa con la actividad <b>21.</b>	Tecnologías de la Información	
19	Elaborar el cambio en el script	<b>Modificación:</b> Elabora el cambio en el script informático	Analista de Infraestructura de Tecnologías de la Información	N/A
20	Definir periodicidad en la ejecución del script	Realiza la definición de la periodicidad en la ejecución del script	Analista de Infraestructura de Tecnologías de la Información	N/A
21	Ejecutar el script	Realiza la ejecución del script para verificar su desarrollo	Analista de Infraestructura de Tecnologías de la Información	N/A
22	Respallos de Información	Realiza el subproceso de “Respallos de Información”, con el fin de obtener un respaldo de la información de las aplicaciones del portal web.	Analista de Infraestructura de Tecnologías de la Información	N/A
23	Elaborar informe de disponibilidad de los portales web	Elabora el informe de disponibilidad de las aplicaciones del portal web y lo remite al responsable de la unidad y al Director de DITIC para su revisión y aprobación.	Analista de Infraestructura de Tecnologías de la Información	Informe de disponibilidad

#### 5.2.5. INDICADORES DEL SUBPROCESO DE ADMINISTRACIÓN DE PORTALES WEB

N°	Indicador	Fórmula de Cálculo	Unidad de Medida	Responsable de Medición	Fuente de Medición	Frecuencia de Medición
1	Porcentaje de disponibilidad de los portales institucionales	$(ATS-DT)/ATS * 100$ <p>Dónde:  <b>ATS</b> es el tiempo acordado de servicio total del período  <b>DT</b> es el tiempo de interrupción del servicio</p>	%	Responsable de la Unidad de Gestión de Infraestructura de TI	Informe de Disponibilidad	Trimestral

#### 5.2.6. FORMATOS DEL SUBPROCESO DE ADMINISTRACIÓN DE PORTALES WEB

Nombre del Registro de Calidad	Código de Formato
N/A	N/A

#### 5.2.7. ANEXOS DEL SUBPROCESO DE ADMINISTRACIÓN DE PORTALES WEB

“No hay anexos.”

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------

### 5.3. SUBPROCESO DE ADMINISTRACIÓN DE DATA CENTER

#### 5.3.1. FICHA TÉCNICA DEL SUBPROCESO DE ADMINISTRACIÓN DE DATA CENTER

<b>Proceso:</b>	GESTIÓN DE INFRAESTRUCTURA DE TECNOLOGÍAS DE LA INFORMACIÓN
<b>Nombre del Subproceso:</b>	ADMINISTRACIÓN DE DATA CENTER
<b>Código del Subproceso:</b>	DITIC-IT-SP3
<b>Descripción:</b>	<p><b>PROPÓSITO:</b> Asegurar y garantizar una adecuada protección de los equipos informáticos en donde se guarda la información en los procesos de transmisión y recepción de datos en las redes internas y externas del INEC.</p> <p><b>ALCANCE:</b> Desde elaborar requerimiento, hasta redactar notificaciones, dar acceso a usuarios y aprobar constatación.</p> <p><b>DISPARADOR:</b></p> <ul style="list-style-type: none"> <li>Notificación del Data Center.</li> </ul> <p><b>PROVEEDORES:</b></p> <ul style="list-style-type: none"> <li>Proveedores de mantenimiento.</li> <li>Gestión de Infraestructura de tecnologías de la información.</li> </ul> <p><b>INSUMOS:</b></p> <ul style="list-style-type: none"> <li>Notificación.</li> <li>Cronograma de mantenimientos.</li> </ul>
<b>Clientes:</b>	<ul style="list-style-type: none"> <li>Unidades del INEC.</li> </ul>
<b>Salidas:</b>	<ul style="list-style-type: none"> <li>Informe de mantenimiento.</li> </ul>
<b>Tipo de Proceso:</b>	<ul style="list-style-type: none"> <li>Adjetivo de asesoría.</li> </ul>
<b>Responsable del Proceso:</b>	Responsable de la Unidad de Gestión de Infraestructura de TI
<b>Recursos:</b>	<p><b>MATERIALES:</b></p> <ul style="list-style-type: none"> <li>Equipo de computación</li> <li>Equipo y materiales de oficina.</li> </ul> <p><b>HUMANOS:</b></p> <ul style="list-style-type: none"> <li>1 Analista de Gestión de Infraestructura de TI SP1.</li> <li>1 Analista de Gestión de Infraestructura de TI SP5.</li> </ul> <p><b>TECNOLÓGICOS:</b></p> <ul style="list-style-type: none"> <li>Correo Electrónico.</li> <li>Software Ofimática.</li> <li>Software de monitoreo de alarmas.</li> </ul>

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------

**Controles/Marco Legal:**

- Normas de control interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos
- Normativa de seguridad de la información, 410-11 plan de contingencias
- Norma seguridad en las comunicaciones
- Normas de control interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos de la contraloría
  1. Política de seguridad de la información
  2. Organización de la seguridad de la información
  3. Gestión de los activos
  4. Seguridad de los recursos humanos
  5. Seguridad física y del entorno
  6. Gestión de comunicaciones y operaciones
  7. Control de acceso
  8. Adquisición, del mantenimiento del data center.

### 5.3.2. CONTROLES DEL SUBPROCESO DE ADMINISTRACIÓN DE DATA CENTER

Resolución 030- DIREJ-DIJU-NI2012 Uso de Los servicios Tecnológicos y Políticas de la Dirección de Tecnologías de la Información y Comunicación del Instituto Nacional de Estadística Y Censos

- Normativa de Seguridad de La información, 410-11 Plan de contingencias

Plan de continuidad de las operaciones que contemplará la puesta en marcha de un centro de cómputo alternativo propio o de uso compartido en un Data Center Estatal, mientras dure la contingencia con el restablecimiento de las comunicaciones y recuperación de la información de los respaldos.

1. Objetivo.- definir las reglas generales para establecer una adecuada protección de los equipos informáticos en el Data Center del INEC.
2. Serán Responsables.- todo el personal del área de DITIC del INEC y los terceros que interactúan de manera habitual u ocasional que estén vinculados a los mantenimientos.
3. Incumplimientos.- las medidas disciplinarias serán aplicadas según resolución publicada, la normativa interna y las que determinaren las entidades de control del estado ecuatoriano.
4. Definiciones.-
  - Conexiones internas.- adicionalmente a las medidas de protección física y de acceso de usuarios ya definidas en las respectivas normas, se deben tener en cuenta las siguientes consideraciones adicionales:
  - Verificar que el sistema de monitoreo y acceso al data center estén en perfecta condiciones.
  - Mantener en perfecto estado los equipos de enfriamiento para no provocar un calentamiento en la granja de servidores.
  - Mantener el sistema de monitoreo, motores de enfriamiento en óptimas condiciones para no tener complicaciones de alguna avería con los servidores.

<b>Elaborado por:</b>	<b>Revisado por:</b>	<b>Aprobado /Autorizado por:</b>	<b>Registrado por:</b>
PC	DIPLA - DIFI	DIREJ	DIPLA, PC





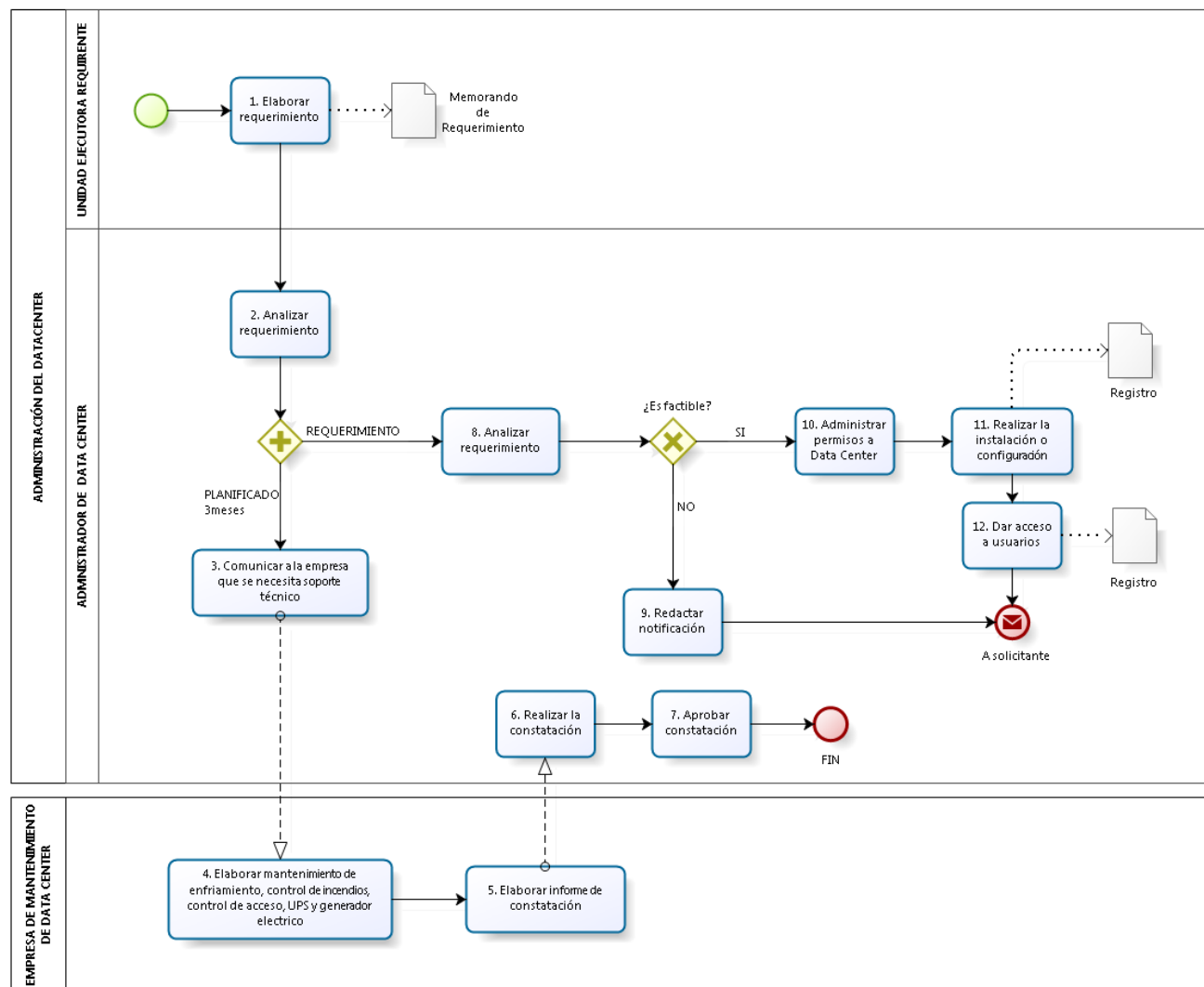
- Asegurarse que todas las conexiones externas con la red interna del INEC se realicen a través de puntos controlados, que deben contemplar entre otras cosas, que estén conectadas a la red interna y el data center.

- **410-13 Monitoreo y evaluación de los procesos y servicios**

Es necesario establecer un marco de trabajo de monitoreo y definir el alcance, la metodología y el proceso a seguir para monitorear la contribución y el impacto de tecnología de información en la entidad.

Elaborado por:	Revisado por:	Aprobado /Autorizado por:	Registrado por:
PC	DIPLA - DIFI	DIREJ	DIPLA, PC

### 5.3.3. DIAGRAMA DE FLUJO DEL SUBPROCESO DE ADMINISTRACIÓN DE DATA CENTER



Elaborado por: PC	Revisado por: DIPLA - DIFI	Aprobado /Autorizado por: DIREJ	Registrado por: DIPLA, PC
----------------------	-------------------------------	------------------------------------	------------------------------

#### 5.3.4. PROCEDIMIENTO DEL SUBPROCESO DE ADMINISTRACIÓN DE DATA CENTER

N	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	DOCUMENTO GENERADO
1	Elaborar requerimiento	Elabora el requerimiento cuando se tiene inconvenientes informáticos	Unidad ejecutora requirente	Memorando de Requerimiento
2	Analizar requerimiento	Realiza el respectivo análisis del requerimiento recibido	Administrador de data center	N/A
3	Comunicar a la empresa que se necesita soporte técnico	<b>PLANIFICADO 3meses:</b> Realiza la comunicación a la empresa que se necesita soporte técnico	Administrador de data center	N/A
4	Elaborar mantenimiento de enfriamiento, control de incendios, control de acceso, UPS y generador eléctrico	Elabora del mantenimiento de enfriamiento, control de incendios, control de acceso, UPS y generador eléctrico	Empresa de mantenimiento de data center	N/A
5	Elaborar informe de constatación	Elabora el informe de constatación de la gestión realizada	Empresa de mantenimiento de data center	Informe de constatación de la gestión realizada
6	Realizar la constatación	Realiza la constatación de la gestión ejecutada	Administrador de data center	Informe de evaluación de la constatación
7	Aprobar constatación, fin	Realiza la aprobación de la constatación de la gestión ejecutada. <b>Fin de proceso.</b>	Administrador de data center	N/A
8	Analizar requerimiento	<b>REQUERIMIENTO:</b> Realiza el requerimiento de repuestos necesarios para el Data Center.	Administrador de data center	Requerimiento
	Decisión	<b>¿Es factible?</b> <b>NO</b> , Redactar notificación, pasa a la actividad <b>9</b> <b>SI</b> , Administrar permisos a Data Center, pasa a la actividad <b>10</b>	Administrador de data center	N/A
9	Elaborar notificación	Elabora la notificación de la gestión realizada	Administrador de data center	N/A
10	Administrar permisos a Data Center	Realiza la administración de permisos del data center.	Administrador de data center	N/A
11	Realizar la instalación o configuración	Realiza la instalación o configuración informática	Administrador de data center	Registro
12	Brindar asistencia para acceso al Data Center	Brinda la asistencia necesaria a los usuarios de la institución para que realicen las modificaciones requeridas en el Data Center.	Administrador de data center	Registro de acceso al Data Center

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------



### 5.3.5. INDICADORES DEL SUBPROCESO DE ADMINISTRACIÓN DE DATA CENTER

N°	Indicador	Fórmula de Cálculo	Unidad de Medida	Responsable de Medición	Fuente de Medición	Frecuencia de Medición
1	Porcentaje de disponibilidad efectiva de Data Center	$((\text{N}^\circ \text{ de horas comprometidas de disponibilidad} - \text{N}^\circ \text{ de horas de indisponibilidad (mantenimientos, cortes de luz)}) / \text{N}^\circ \text{ de horas comprometidas de disponibilidad})$	%	Responsable de infraestructura	Informe técnico de ejecución	Trimestral

### 5.3.6. FORMATOS DEL SUBPROCESO DE ADMINISTRACIÓN DE DATA CENTER

Nombre del Registro de Calidad	Código de Formato
N/A	N/A

### 5.3.7. ANEXOS DEL SUBPROCESO DE ADMINISTRACIÓN DE DATA CENTER

“No hay anexos.”

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------

## 5.4. SUBPROCESO DE ADMINISTRACIÓN DE INFRAESTRUCTURA

### 5.4.1. FICHA TÉCNICA DEL SUBPROCESO DE ADMINISTRACIÓN DE INFRAESTRUCTURA

<b>Proceso:</b>	GESTIÓN DE INFRAESTRUCTURA DE TECNOLOGÍAS DE LA INFORMACIÓN		
<b>Nombre del Subproceso:</b>	ADMINISTRACIÓN DE INFRAESTRUCTURA		
<b>Código del Subproceso:</b>	DITIC-IT-SP4		
<b>Descripción:</b>	<p><b>PROPÓSITO:</b>  Brindar una administración optima de la infraestructura tecnológica que posee la Institución, lo que permita dar seguimiento, control, y monitoreo de cada uno de los servidores y servicios que se brinda a los usuarios del INEC internos</p> <p><b>ALCANCE:</b>  Desde analizar la alerta, hasta analizar y aprobar la gestión.</p> <p><b>DISPARADOR:</b></p> <ul style="list-style-type: none"> <li>• Memorando o correo electrónico.</li> </ul> <p><b>PROVEEDORES:</b></p> <ul style="list-style-type: none"> <li>• Direcciones del INEC</li> </ul> <p><b>INSUMOS:</b></p> <ul style="list-style-type: none"> <li>• Requerimiento detallado</li> <li>• Autorización del Director/a o jefe de unidad de DITIC para atender el requerimiento</li> </ul>		
<b>Clientes:</b>	<ul style="list-style-type: none"> <li>• Direcciones del INEC</li> </ul>		
<b>Salidas:</b>	<ul style="list-style-type: none"> <li>• Informe de disponibilidad de infraestructura.</li> <li>• Requerimiento atendido.</li> </ul>		
<b>Tipo de Proceso:</b>	<ul style="list-style-type: none"> <li>• Adjetivo de asesoría.</li> </ul>		
<b>Responsable del Proceso:</b>	Responsable de la Unidad de Gestión de Infraestructura de TI		
<b>Recursos:</b>	<p><b>MATERIALES:</b></p> <ul style="list-style-type: none"> <li>• Equipo de computación</li> <li>• Equipo y materiales de oficina.</li> </ul> <p><b>HUMANOS:</b></p> <ul style="list-style-type: none"> <li>• 1 Analista de Gestión de Infraestructura de Tecnologías de la Información (SP7)</li> <li>• 4 Analista de Gestión de Infraestructura de Tecnologías de la Información (SP5)</li> </ul> <p><b>TECNOLÓGICOS:</b></p> <ul style="list-style-type: none"> <li>• Correo Electrónico.</li> <li>• Software Ofimática.</li> </ul>		
<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC

	<ul style="list-style-type: none"> <li>Whatsup.</li> </ul>
<b>Controles/Marco Legal:</b>	<ul style="list-style-type: none"> <li>Esquema Gubernamental de Seguridad de la Información (EGSI). Organización de la seguridad de la información 2.4</li> <li>Esquema Gubernamental de Seguridad de la Información (EGSI). Gestión de Activos 3.2</li> <li>Esquema Gubernamental de Seguridad de la Información (EGSI). Gestión de comunicaciones y Operaciones 6.1 literal e.</li> <li>Esquema Gubernamental de Seguridad de la Información (EGSI). Gestión de Comunicaciones y Operaciones 6.3. literal a.</li> <li>Esquema Gubernamental de Seguridad de la Información (EGSI). Gestión de comunicaciones y Operaciones. 6.6 literal c.</li> <li>Esquema Gubernamental de Seguridad de la Información (EGSI). Gestión de Comunicaciones y Operaciones 6.27.</li> <li>Esquema Gubernamental de Seguridad de la Información (EGSI). Gestión de Comunicaciones y Operaciones 6.29.</li> <li>Esquema Gubernamental de Seguridad de la Información (EGSI). Gestión de Comunicaciones y Operaciones 6.30.</li> <li>Esquema Gubernamental de Seguridad de la Información (EGSI). Gestión de la continuidad del negocio 10.2 literal b.</li> <li>Esquema Gubernamental de Seguridad de la Información (EGSI). Gestión de la Continuidad del Negocio 10.4 literal d.</li> <li>Esquema Gubernamental de Seguridad de la Información (EGSI). Cumplimiento 11.8 literal a.</li> <li>Normas de control interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos. 410-09 Mantenimiento y control de la infraestructura tecnológica. Tema 6.</li> </ul>

#### 5.4.2. CONTROLES DEL SUBPROCESO DE ADMINISTRACIÓN DE INFRAESTRUCTURA

#### ACUERDO 166 DE LA SECRETARIA DE LA ADMINISTRACION PÚBLICA ESQUEMA GUBERNAMENTAL DE LA SEGURIDAD DE LA INFORMACION (EGSI)

##### 2. Organización de la seguridad de la información

2.4 Proceso de autorización para nuevos servicios de procesamiento de la información

a) Asignar un custodio o responsable para cualquier nuevo servicio a implementar, generalmente del área peticionaria, incluyendo la definición de las características de la información y la definición de los diferentes niveles de acceso por usuario.

##### 3. Gestión de los activos

3.2. Responsable de los activos

a) Asignar los activos asociados (o grupos de activos) a un individuo que actuará como Responsable del Activo.

Por ejemplo, debe haber un responsable de los computadores de escritorio, otro de los celulares, otro de los servidores del centro de datos, etc. El término "responsable" no implica que la persona tenga realmente los derechos de propiedad de los activos. El Responsable del Activo tendrá las siguientes funciones:

- Elaborar el inventario de los activos a su cargo y mantenerlo actualizado.
- Delegar tareas rutinarias, tomando en cuenta que la responsabilidad sigue siendo del responsable.
- Administrar la información dentro de los procesos de la institución a los cuales ha sido asignado.
- Elaborar las reglas para el uso aceptable del mismo e implantarlas previa autorización de la autoridad correspondiente.

<b>Elaborado por:</b>	<b>Revisado por:</b>	<b>Aprobado /Autorizado por:</b>	<b>Registrado por:</b>
PC	DIPLA - DIFI	DIREJ	DIPLA, PC

- Clasificar, documentar y mantener actualizada la información y los activos, y definir los permisos de acceso a la información.

## 6. Gestión de comunicaciones y operaciones

### 6.1. Documentación de los procedimientos de Operación

e) Documentar los contactos de soporte, necesarios en caso de incidentes (\*).

### 6.3. Distribución de funciones

a) Distribuir las funciones y las áreas de responsabilidad, para reducir oportunidades de modificaciones no autorizadas, no intencionales, o el uso inadecuado de los activos de la institución.

### 6.6. Monitoreo y revisión de los servicios, por terceros

c) Analizar los reportes de servicios, reportes de incidentes elaborados por terceros y acordar reuniones periódicas según los acuerdos (\*).

### 6.27. Monitoreo de uso del sistema

a) Registrar los accesos autorizados, incluyendo (\*):

- Identificación del ID de usuario;
- Fecha y hora de eventos clave;
- Tipos de evento;
- Archivos a los que se han tenido acceso;
- Programas y utilitarios utilizados;

b) Monitorear las operaciones privilegiadas, como (\*):

- Uso de cuentas privilegiadas;
- Encendido y detección del sistema;
- Acople y desacople de dispositivos de entrada;

c) Monitorear intentos de acceso no autorizados, como (\*):

- Acciones de usuario fallidas o rechazadas;
- Violación de la política de acceso y notificaciones de firewalls y gateways;
- Alertas de los sistemas de detección de intrusos;

d) Revisar alertas o fallas del sistema, como (\*):

- Alertas y/o mensajes de consola;
- Excepciones de registro del sistema;
- Alarmas de gestión de red;
- Alarmas del sistema de control de acceso;

e) Revisar cambios o intentos de cambio en la configuración y los controles de la seguridad del sistema.

### 6.29. Registros del administrador y del operador.

a) Incluir al registro, la hora en la que ocurrió el evento (\*).

b) Incluir al registro, información sobre el evento (\*).

c) Incluir al registro, la cuenta de administrador y operador que estuvo involucrado (\*).

d) Añadir al registro, los procesos que estuvieron implicados (\*).

### 6.30. Registro de fallas

a) Revisar los registros de fallas o errores del sistema (\*).

b) Revisar las medidas correctivas para garantizar que no se hayan vulnerado los controles (\*).

c) Asegurar que el registro de fallas esté habilitado (\*).

## 10. Gestión de la continuidad del negocio

<b>Elaborado por:</b>	<b>Revisado por:</b>	<b>Aprobado /Autorizado por:</b>	<b>Registrado por:</b>
PC	DIPLA - DIFI	DIREJ	DIPLA, PC





10.2. Continuidad del negocio y evaluación de riesgos

b) Entender las complejidades e interrelaciones existentes entre equipamiento, personas, tareas, departamentos, mecanismos de comunicación y relaciones con proveedores externos, los cuales pueden prestar servicios críticos que deben ser considerados.

10.4. Estructura para la planificación de la continuidad del negocio

d) Definir los acuerdos de niveles de servicios internos y con proveedores.

**11. Cumplimiento**

11.8. Verificación del cumplimiento técnico

a) Verificar el cumplimiento técnico bien sea manualmente (con soporte de las herramientas de Software apropiadas, si es necesario) por un ingeniero de sistemas con experiencia, y/o con la ayuda de herramientas automáticas que generen un informe técnico para la interpretación posterior por parte del especialista técnico.

**Normas de control interno para las entidades, organismos del sector público y personas jurídica de derecho privado que dispongan de recursos públicos- de la contraloría**

**410 Tecnología de la información**

410 - 09 Mantenimiento y control de la infraestructura tecnológica

6. Se elaborará un plan de mantenimiento preventivo y/o correctivo de la infraestructura tecnológica sustentado en revisiones periódicas y monitoreo en función de las necesidades organizacionales (principalmente en las aplicaciones críticas de la organización), estrategias de actualización de hardware y software, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad.

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------

```

graph TD
    subgraph Proveedor_Externo [Proveedor Externo]
        E1[5. Recibir y analizar incidente] --> E2[6. Solucionar incidente]
        E2 --> E3[7. Elaborar informe de gestión]
    end

    subgraph Administracion_De_Infraestructura [ADMINISTRACIÓN DE INFRAESTRUCTURA]
        subgraph Analista_IN [Analista IN]
            A1{¿Se puede solucionar?}
            A2{¿Es factible?}
            A3{¿Existe conectividad?}
            A4{Tipo de servidor}
            A5{ }
        end

        subgraph Jefe_IN [Jefe IN]
            J1[3. Aprobar la gestión realizada]
            J2[10. Analizar requerimiento]
            J3[16. Aprobar y reasignar plan]
            J4[19. Aprobar el informe de planificación]
        end

        subgraph Directoria_DTIC [Directoria DTIC]
            D1[9. Analizar requerimiento y asignarlo]
            D2[15. Analizar y aprobar gestión]
        end

        E3 -.-> A1
        A1 -- SI --> A2
        A1 -- NO --> A4
        A2 -- SI --> J1
        A2 -- NO --> A3
        A3 -- SI --> A5
        A3 -- NO --> A4
        A4 -- VIRTUAL --> J2
        A4 -- FISICO --> A5
        J1 --> D1
        J2 --> D1
        D1 -- PLANIFICADO --> A5
        D1 -- REQUERIMIENTO --> D2
        A5 --> A4
        A5 --> J3
        A5 --> J4
        A5 --> D2
        A5 --> FIN((FIN))
    end
  
```

**Registrado por:**  
DIPLA, PC

#### 5.4.4. PROCEDIMIENTO DEL SUBPROCESO DE ADMINISTRACIÓN DE INFRAESTRUCTURA

N	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	DOCUMENTO GENERADO
	Decisión	<b>Tipo de Administración</b> <b>Alerta:</b> Pasa a la actividad 1. Analizar alerta. <b>Planificado:</b> Pasa a la actividad 16. Aprobar y reasignar plan. <b>Requerimiento:</b> Pasa a la actividad 9. Analizar requerimiento.	Director(a) DITIC	N/A
1	Analizar alerta	<b>Alerta:</b> Analizar la alerta en daños de infraestructura, virtualización y seguridad.	Analista de Infraestructura de Tecnologías de la Información	N/A
	Decisión	<b>¿Se puede solucionar el problema?</b> <b>SI:</b> Pasa a la actividad 2. Realizar arreglo. <b>NO:</b> Pasa a la actividad 4. Escalar eventos.	Analista de Infraestructura de Tecnologías de la Información	N/A
2	Realizar arreglo	Realizar las actividades necesarias para arreglar el problema encontrado.	Analista de Infraestructura de Tecnologías de la Información	N/A
3	Aprobar gestión	Revisar y aprobar las acciones emprendidas para arreglar el problema. <b>Fin del subproceso.</b>	Jefe de Infraestructura de Tecnologías de la Información	N/A
4	Escalar eventos	Cuando el evento no se puede arreglar por los técnicos de DITIC, se escala el caso y se contacta a un proveedor externo.	Analista de Infraestructura de Tecnologías de la Información	N/A
5	Receptar incidente	Receptar y analizar el incidente ocurrido.	Proveedor externo	N/A
6	Solucionar incidente	Solucionar el incidente.	Proveedor externo	N/A
7	Elaborar informe	Elaborar y remitir al INEC un informe en el cual conste cuál fue el trabajo realizado para el arreglo del incidente.	Proveedor externo	Informe de incidente arreglado
8	Revisar informe	Revisar que el informe se encuentre bien realizado, y archivar el mismo. <b>Fin del subproceso.</b>	Analista TI	N/A
9	Analizar requerimiento	<b>Requerimiento:</b> Analizar la factibilidad de atención del requerimiento y reasignar el mismo al responsable de la Gestión de Infraestructura de Tecnologías de la Información.	Director(a) DITIC	N/A

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------

10	Analizar requerimiento	Analizar la factibilidad de atención del requerimiento.	Jefe de Infraestructura de Tecnologías de la Información	N/A
	Decisión	<b>¿Es factible atender el requerimiento?</b> <b>SI:</b> Pasa a la siguiente decisión. Tipo de servidor. <b>NO:</b> Pasa a la actividad <b>11</b> . Redactar notificación.	Jefe de Infraestructura de Tecnologías de la Información	N/A
11	Notificar no factibilidad	Notificar por medio de correo electrónico o memorando al área requirente que no es factible atender el requerimiento.	Analista de Infraestructura de Tecnologías de la Información	Correo electrónico / Memorando
	Decisión	<b>Tipo de servidor:</b> <b>Virtual:</b> Pasa a la actividad <b>12</b> . Revisar entorno. <b>Físico:</b> Pasa a la siguiente decisión. ¿Existe conectividad?	Analista de Infraestructura de Tecnologías de la Información	N/A
12	Revisar entorno	Revisar el entorno virtual del servidor. <b>Pasa a la actividad 14.</b> Ejecutar requerimiento.	Analista de Infraestructura de Tecnologías de la Información	N/A
	Decisión	<b>¿Existe conectividad?</b> <b>SI:</b> Pasa a la actividad <b>14</b> . Ejecutar requerimiento. <b>NO:</b> Pasa a la actividad <b>13</b> . Revisar servidor en data center.	Analista de Infraestructura de Tecnologías de la Información	N/A
13	Revisar servidor	Revisar el servidor en data center.	Analista de Infraestructura de Tecnologías de la Información	N/A
14	Ejecutar requerimiento	Ejecutar el requerimiento solicitado con base en las especificaciones realizadas por el área requirente.	Analista de Infraestructura de Tecnologías de la Información	N/A
15	Revisar requerimiento	Revisar que el requerimiento haya sido atendido de manera correcta. <b>Fin del subproceso.</b>	Director(a) DITIC	N/A
16	Aprobar plan	<b>Planificado:</b> Aprobar el plan de mantenimiento de infraestructura de tecnologías de la información y reasignar el mismo a los analistas de la Unidad.	Jefe de Infraestructura de Tecnologías de la Información	Plan de mantenimiento aprobado

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------



17	Ejecutar mantenimiento	Ejecutar el mantenimiento de acuerdo a lo planificado.	Analista de Infraestructura de Tecnologías de la Información	N/A
18	Realizar informe	Realizar un informe acerca de la ejecución del plan de mantenimiento para la infraestructura de tecnologías de la información.	Analista de Infraestructura de Tecnologías de la Información	Informe de ejecución del plan de mantenimiento
19	Revisar informe	Revisar que el informe se encuentre bien realizado, una vez que el informe esté correcto, se aprueba. <b>Fin del subproceso.</b>	Jefe de Infraestructura de Tecnologías de la Información	N/A

#### 5.4.5. INDICADORES DEL SUBPROCESO DE ADMINISTRACIÓN DE INFRAESTRUCTURA

N°	Indicador	Fórmula de Cálculo	Unidad de Medida	Responsable de Medición	Fuente de Medición	Frecuencia de Medición
1	Porcentaje de disponibilidad de los servidores	$((\text{Tiempo total sondeo} - \text{tiempo no disponible}) / \text{tiempo total de sondeo}) * 100\%$	%	Responsable de la Unidad de Gestión de Infraestructura de TI	Reporte de Software Whatsup	Trimestral

#### 5.4.6. FORMATOS DEL SUBPROCESO DE ADMINISTRACIÓN DE INFRAESTRUCTURA

Nombre del Registro de Calidad	Código de Formato
N/A	N/A

#### 5.4.7. ANEXOS DEL SUBPROCESO DE ADMINISTRACIÓN DE INFRAESTRUCTURA

“No hay anexos.”

Elaborado por: PC	Revisado por: DIPLA - DIFI	Aprobado /Autorizado por: DIREJ	Registrado por: DIPLA, PC
----------------------	-------------------------------	------------------------------------	------------------------------

## 5.5. SUBPROCESO DE ADMINISTRACIÓN DE GESTIÓN DOCUMENTAL QUIPUX

### 5.5.1. FICHA TÉCNICA DEL SUBPROCESO DE ADMINISTRACIÓN DE GESTIÓN DOCUMENTAL QUIPUX

<b>Proceso:</b>	GESTIÓN DE INFRAESTRUCTURA DE TECNOLOGÍAS DE LA INFORMACIÓN
<b>Nombre del Subproceso:</b>	ADMINISTRACIÓN DE GESTIÓN DOCUMENTAL QUIPUX
<b>Código del Subproceso:</b>	DITIC-IT-SP5
<b>Descripción:</b>	<p><b>PROPÓSITO:</b></p> <p>Optimizar de la mejor manera el sistema gubernamental de cero papeles e implementar el sistema con mayor fluidez en trámites internos y externos.</p> <p><b>ALCANCE:</b></p> <p>Desde recibir, analizar y enviar el requerimiento para su respectivo análisis, hasta realizar la elaboración del informe del monitoreo continuo.</p> <p><b>DISPARADOR:</b></p> <ul style="list-style-type: none"> <li>• Memorando.</li> </ul> <p><b>PROVEEDORES:</b></p> <ul style="list-style-type: none"> <li>• Funcionarios del INEC.</li> </ul> <p><b>INSUMOS:</b></p> <ul style="list-style-type: none"> <li>• Memorando, correo electrónico, Resolución 084-DIREJ-DIJU-NI2014.</li> <li>• Requerimiento del sistema GLPI.</li> </ul>
<b>Clientes:</b>	<ul style="list-style-type: none"> <li>• Funcionarios del INEC</li> </ul>
<b>Salidas:</b>	<ul style="list-style-type: none"> <li>• Informe técnico.</li> <li>• Memorando de respuesta.</li> <li>• Respuesta en el sistema GLPI.</li> </ul>
<b>Tipo de Proceso:</b>	Adjetivo de Apoyo de Asesoría.
<b>Responsable del Proceso:</b>	Responsable de Gestión de Infraestructura de Tecnologías de la Información.
<b>Recursos:</b>	<p><b>MATERIALES:</b></p> <ul style="list-style-type: none"> <li>• Equipo de computación</li> <li>• Equipo y materiales de oficina.</li> </ul> <p><b>HUMANOS:</b></p> <ul style="list-style-type: none"> <li>• 1 Analista de Gestión de Infraestructura de TI SP1.</li> <li>• 1 Analista de Gestión de Infraestructura de TI SP5.</li> </ul> <p><b>TECNOLÓGICOS:</b></p> <ul style="list-style-type: none"> <li>• Correo Electrónico.</li> <li>• Software Ofimática.</li> <li>• Sistema GLPI.</li> </ul>

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------

**Controles/Marco Legal:**

- Norma de implementación y operación de gobiernos por resultados – Acuerdo Ministerial 1002 – art. 30, art. 31, art. 32

### 5.5.2. CONTROLES DEL SUBPROCESO DE ADMINISTRACIÓN DE GESTIÓN DOCUMENTAL QUIPUX

**Resolución 084-DIREJ-DIJU-NI2014 Uso del sistema de Gestión Documental Quipux, del Instituto Nacional de Estadística Y Censos**

**Sistema de Gestión Documental Quipux  
Sistema cero papeles**

**1. Objetivo**

Definir las reglas generales para establecer una adecuada distribución de la documentación interna y externa dentro del sistema cero papeles del INEC.

**2. Serán Responsables:**

Todo el personal del INEC debe manejar el sistema y la administración del área de DITIC para el proceso de la documentación interna y externa los terceros que interactúan de manera habitual u ocasional que estén vinculados a los procesos de transmisión de datos en el desarrollo de sus tareas habituales.

**3. Incumplimientos**

Las medidas disciplinarias serán aplicadas según resolución publicada, la normativa interna y las que determinaren las entidades de control del estado ecuatoriano.

**4. Definiciones**

Se define la aplicación del sistema dentro del margen de cero papeles las cuales se desarrollaran dentro de la estructura orgánica funcional para el procedimiento de la documentación interna es esto (Memorandos, Circulares, Oficios entre otros.)

Dentro del sistema de gestión documental se puede generar una política interna de direccionamiento ejecución de los procesos, actividades, institucionales.

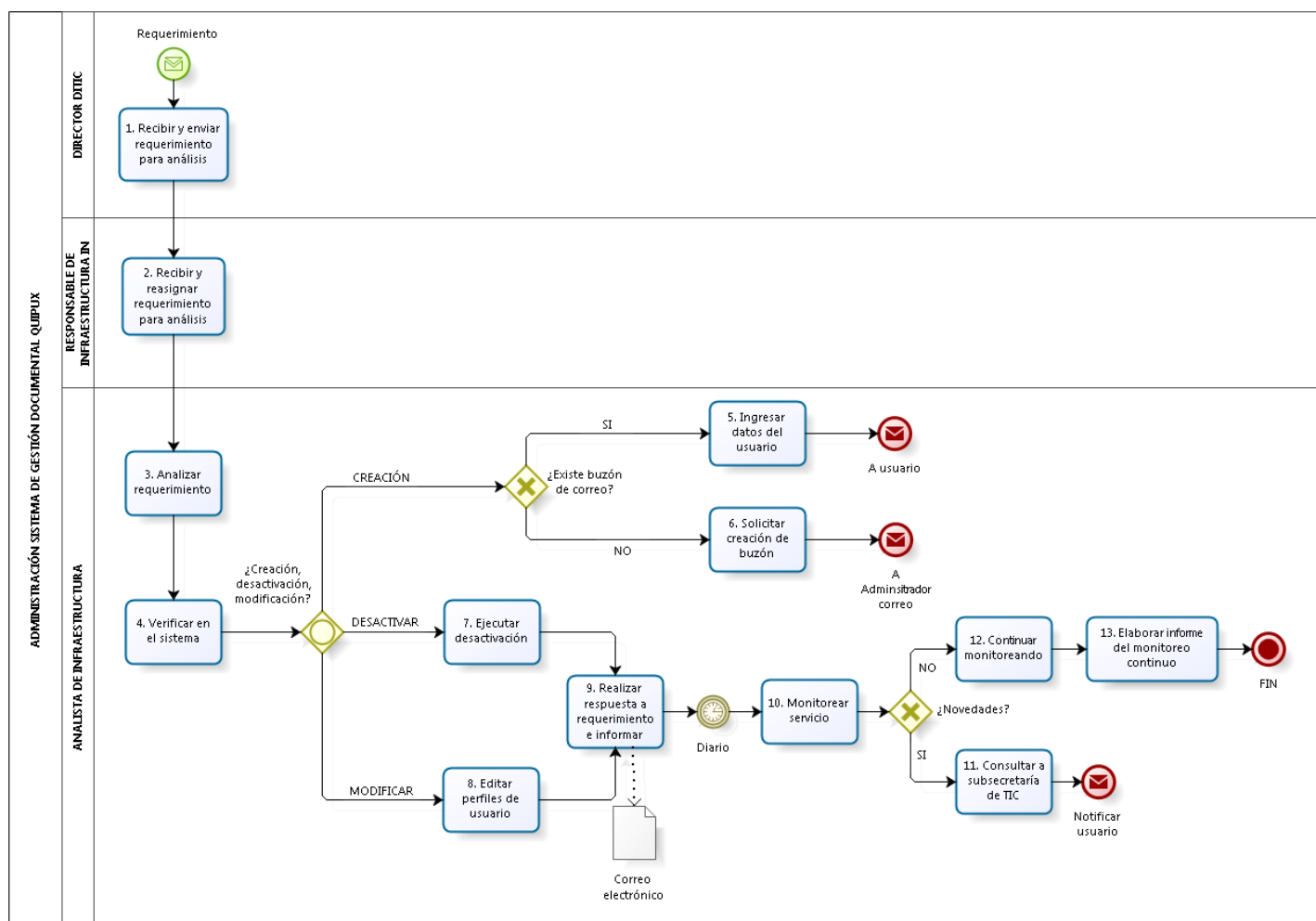
Utilizar el sistema para guardar la información con respecto a las actividades de proyectos, resoluciones o actividades de la institución.

Asegurarse que todas las conexiones externas con la red interna del INEC se realicen a través de puntos controlados, que deben contemplar entre otras cosas, puertos y estaciones de trabajo que simultáneamente esté conectada a la red interna y salida de internet para no tener problemas con la conexión al Quipux.

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------



### 5.5.3. DIAGRAMA DE FLUJO DEL SUBPROCESO DE ADMINISTRACIÓN DE GESTIÓN DOCUMENTAL QUIPUX



Elaborado por:	Revisado por:	Aprobado /Autorizado por:	Registrado por:
PC	DIPLA - DIFI	DIREJ	DIPLA, PC

#### 5.5.4. PROCEDIMIENTO DEL SUBPROCESO DE ADMINISTRACIÓN DE GESTIÓN DOCUMENTAL QUIPUX

#	ACTIVIDAD	DESCRIPCIÓN	ROL	DOCUMENTO GENERADO
1	Recibir y enviar requerimiento para análisis	Recibe, analiza y envía el requerimiento para su respectivo análisis.	Director DITIC	Memorando
2	Recibir y reasignar requerimiento para análisis	Recibe para realizar el análisis del requerimiento para reasignar el requerimiento para su análisis.	Responsable de Infraestructura IN	Memorando
3	Analizar requerimiento	Realiza el análisis del requerimiento para realizar la gestión.	Analista de Infraestructura	N/A
4	Verificar en el sistema	Realiza la verificación en el sistema para analizar estatus si es creación, desactivación o modificación.	Analista de Infraestructura	N/A
	Decisión	<b>¿Es creación, desactivación o modificación?</b> <b>Creación:</b> Continúa con la decisión <b>¿Existe buzón de correo?</b> <b>Desactivación:</b> Realiza la actividad <b>7.</b> Ejecutar desactivación. <b>Modificación:</b> Realiza la actividad <b>8.</b> Editar perfiles de usuarios.	Analista de Infraestructura	N/A
	Decisión	<b>CREACIÓN, ¿Existe buzón de correo?</b> <b>SI:</b> Realiza la actividad <b>5.</b> Ingresar datos del usuario. <b>NO:</b> Realiza la actividad <b>6.</b> Solicitar creación de buzón.	Analista de Infraestructura	N/A
5	Ingresar datos del usuario, fin	Realiza el ingreso de los datos del usuario e informa a usuario. <b>Fin del proceso.</b>	Analista de Infraestructura	N/A
6	Solicitar creación de buzón, fin	Realiza la solicitud para la creación del buzón e informa al administrador. <b>Fin del proceso.</b>	Analista de Infraestructura	N/A
7	DESACTIVAR, Ejecutar desactivación	Realiza la ejecución de la desactivación del usuario. Continúa con la actividad <b>9.</b>	Analista de Infraestructura	N/A
8	MODIFICAR, Editar perfiles de usuario	Realiza la edición de los perfiles del usuario, modificando según el requerimiento	Analista de Infraestructura	N/A
9	Realizar respuesta al requerimiento e informar	Realiza la respuesta al requerimiento solicitado e informa al responsable de la unidad o al director y al usuario solicitante.	Analista de Infraestructura	Correo electrónico
10	Monitorear servicio	<b>De manera diaria:</b>	Analista de	N/A

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------

		Realiza el monitoreo del servicio con un frecuencia diaria	Infraestructura	
	Decisión	<b>¿Existe novedades?</b> <b>SI:</b> Realiza la actividad <b>11.</b> Consultar a subsecretaría de TIC. <b>NO:</b> Realiza la actividad <b>12.</b> Continuar monitoreando.	Analista de Infraestructura	N/A
11	Consultar a subsecretaría de TIC	Realiza la consulta a la subsecretaria de TICs. <b>Fin del proceso.</b>	Analista de Infraestructura	N/A
12	Continuar monitoreando	Realiza el continuo monitoreo para mantener el correcto servicio informático	Analista de Infraestructura	N/A
13	Elaborar informe del monitoreo continuo, fin	Realiza la elaboración del informe del monitoreo continuo.	Analista de Infraestructura	Informe de monitorio

#### 5.5.5. INDICADORES DEL SUBPROCESO DE ADMINISTRACIÓN DE GESTIÓN DOCUMENTAL QUIPUX

N°	Indicador	Fórmula de Cálculo	Unidad de Medida	Responsable de Medición	Fuente de Medición	Frecuencia de Medición
1	Porcentaje de cumplimiento de la administración de gestión documental Quipux	$(\# \text{ de acciones ejecutadas de la gestión documental Quipux} / \# \text{ de acciones solicitadas de la gestión documental Quipux}) * 100\%$	%	Responsable de infraestructura	Informe técnico de ejecución	Trimestral

#### 5.5.6. FORMATOS DEL SUBPROCESO DE ADMINISTRACIÓN DE GESTIÓN DOCUMENTAL QUIPUX

Nombre del Registro de Calidad	Código de Formato
N/A	N/A

#### 5.5.7. ANEXOS DEL SUBPROCESO DE ADMINISTRACIÓN DE GESTIÓN DOCUMENTAL QUIPUX

“No hay anexos.”

Elaborado por: PC	Revisado por: DIPLA - DIFI	Aprobado /Autorizado por: DIREJ	Registrado por: DIPLA, PC
----------------------	-------------------------------	------------------------------------	------------------------------

## 5.6. SUBPROCESO DE ADMINISTRACIÓN DE BASE DE DATOS

### 5.6.1. FICHA TÉCNICA DEL SUBPROCESO DE ADMINISTRACIÓN DE BASE DE DATOS

<b>Proceso:</b>	GESTIÓN DE INFRAESTRUCTURA DE TECNOLOGÍAS DE LA INFORMACIÓN
<b>Nombre del Subproceso:</b>	ADMINISTRACIÓN DE BASE DE DATOS
<b>Código del Subproceso:</b>	DITIC-IT-SP6
<b>Descripción:</b>	<p><b>PROPÓSITO:</b> Mantener operativas, efectivas, eficientes, integra y seguras las bases de datos de la institución, de esta forma proveer la accesibilidad a la información que estas alojan a los usuarios internos y externos.</p> <p><b>ALCANCE:</b> Desde monitorear los servidores de bases de datos, hasta notificar a los usuarios que se atendió el requerimiento.</p> <p><b>DISPARADOR:</b></p> <ul style="list-style-type: none"> <li>• Memorando o correo electrónico</li> </ul> <p><b>PROVEEDORES:</b></p> <ul style="list-style-type: none"> <li>• Dirección de Registros Administrativos</li> <li>• Direcciones Productoras</li> </ul> <p><b>INSUMOS:</b></p> <ul style="list-style-type: none"> <li>• Requerimiento detallado</li> <li>• Autorización del Director/a de DITIC para atender el requerimiento.</li> </ul>
<b>Clientes:</b>	<ul style="list-style-type: none"> <li>• Direcciones Productoras de Información Estadística</li> </ul>
<b>Salidas:</b>	<ul style="list-style-type: none"> <li>• Requerimiento atendido</li> </ul>
<b>Tipo de Proceso:</b>	<ul style="list-style-type: none"> <li>• Adjetivo de asesoría</li> </ul>
<b>Responsable del Proceso:</b>	Responsable de la Unidad de Gestión de Infraestructura
<b>Recursos:</b>	<p><b>MATERIALES:</b></p> <ul style="list-style-type: none"> <li>• Equipo de computación</li> <li>• Equipo y materiales de oficina.</li> </ul> <p><b>HUMANOS:</b></p> <ul style="list-style-type: none"> <li>• 1 Analista de Gestión de Infraestructura de TI (SP7).</li> <li>• 4 Analistas de Gestión de Infraestructura de TI (SP5).</li> </ul> <p><b>TECNOLÓGICOS:</b></p> <ul style="list-style-type: none"> <li>• Correo Electrónico.</li> <li>• Software Ofimática.</li> </ul>

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------

**Controles/Marco Legal:**

- Esquema Gubernamental de Seguridad de la Información (EGSI). Gestión de Activos 3.1. Inventario de activos
- Esquema Gubernamental de Seguridad de la Información (EGSI). Gestión de comunicaciones y operaciones 6.4 literal c
- Esquema Gubernamental de Seguridad de la Información (EGSI). Control de acceso 7.3. Gestión de privilegios literal b
- Esquema Gubernamental de Seguridad de la Información (EGSI). Adquisición, desarrollo y mantenimiento de sistemas de información 8.6. Política sobre el uso de controles criptográficos literal b
- Esquema Gubernamental de Seguridad de la Información (EGSI). Adquisición, desarrollo y mantenimiento de sistemas de información 8.8. Control del software operativo literal c
- Esquema Gubernamental de Seguridad de la Información (EGSI). Adquisición, desarrollo y mantenimiento de sistemas de información 8.9. Protección de los datos de prueba del sistema literal a, b, c, d, f, i

### 5.6.2. CONTROLES DEL SUBPROCESO DE ADMINISTRACIÓN DE BASE DE DATOS

#### ACUERDO 166 DE LA SECRETARIA DE LA ADMINISTRACION PÚBLICA ESQUEMA GUBERNAMENTAL DE LA SEGURIDAD DE LA INFORMACION (EGSI)

#### 3 GESTIÓN DE LOS ACTIVOS

##### 3.1. Inventario de activos

Inventariar los activos referentes a la estructura organizacional:

a) Estructura organizacional del área de las TIC, con los cargos y nombres del personal: administrador (de servidores, de redes de datos, de respaldos de la información, de sistemas de almacenamiento, de bases de datos, de seguridades, de aplicaciones del negocio, de recursos informáticos, etc.), líder de proyecto, personal de capacitación, personal de mesa de ayuda, personal de aseguramiento de calidad, programadores (PHP, Java, etc.).

#### 6. GESTIÓN DE COMUNICACIONES Y OPERACIONES

6.4. Separación de las instancias de Desarrollo, Pruebas, Capacitación y Producción.

c) Controlar la instalación y uso de herramientas de desarrollo de software y/o acceso a bases de datos y redes en los equipos informáticos, salvo que sean parte de las herramientas de uso estándar o su instalación sea autorizada de acuerdo a un procedimiento expresamente definido.

#### 7. CONTROL DE ACCESO

##### 7.3. Gestión de privilegios

b) Mantener un cuadro de identificación de los usuarios y sus privilegios asociados con cada servicio o sistema operativo, sistema de gestión de base de datos y aplicaciones.

<b>Elaborado por:</b>	<b>Revisado por:</b>	<b>Aprobado /Autorizado por:</b>	<b>Registrado por:</b>
PC	DIPLA - DIFI	DIREJ	DIPLA, PC



## 8. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

### 8.6. Política sobre el uso de controles criptográficos

b) Utilizar controles criptográficos para la protección de claves de acceso a: sistemas, datos y servicios. Las claves deberán ser almacenadas de manera codificada, cifrada (encriptada) en la base de datos y/o en archivos de parámetros.

### 8.8. Control del software operativo

c) Ningún programador o analista de desarrollo y mantenimiento de aplicaciones podrá acceder a los ambientes de producción.

### 8.9. Protección de los datos de prueba del sistema

a) Identificar por cada sistema, los datos que pueden ser copiados de un ambiente de producción a un ambiente de pruebas.

b) Efectuar pruebas de los sistemas en el ambiente de pruebas, sobre datos extraídos del ambiente de producción.

c) Solicitar autorización formal para realizar una copia de la base de datos de producción como base de datos de prueba.

d) Personalizar los datos en el ambiente de pruebas, eliminando las contraseñas de producción y generando nuevas para pruebas.

f) Aplicar los mismos procedimientos de control de acceso que existen en la base de producción.

i) Controlar que la modificación, actualización o eliminación de los datos operativos (de producción) serán realizados a través de los sistemas que procesan esos datos, y de acuerdo al esquema de control de accesos implementado en los mismos.

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------

<b>Elaborado por:</b>	<b>Revisado por:</b>	<b>Aprobado /Autorizado por:</b>	<b>Registrado por:</b>
PC	DIPLA - DIFI	DIREJ	DIPLA, PC



#### 5.6.4. PROCEDIMIENTO DEL SUBPROCESO DE ADMINISTRACIÓN DE BASE DE DATOS

#	ACTIVIDAD	DESCRIPCIÓN	ROL	DOCUMENTO GENERADO
	Decisión	<b>Diariamente:</b> Pasa a la actividad <b>1.</b> Monitorear servidores. <b>Requerimiento:</b> Pasa a la actividad <b>4.</b> Analizar requerimiento.	Analista de Infraestructura de Tecnologías de la Información	N/A
1	Monitorear servidores	Realizar el monitoreo de los servidores de bases de datos. <b>Esta actividad se la realiza diariamente.</b>	Analista de Infraestructura de Tecnologías de la Información	N/A
	Decisión	<b>¿Existen novedades?</b> <b>SI:</b> Pasa a la actividad <b>2.</b> Elaborar la investigación en la base de datos. <b>NO:</b> Regresa a la actividad <b>1.</b> Analizar requerimiento.	Analista de Infraestructura de Tecnologías de la Información	N/A
2	Elaborar investigación	Elaborar la investigación pertinente en la base de datos.	Analista de Infraestructura de Tecnologías de la Información	N/A
3	Solucionar problemas	Solucionar los problemas encontrados en las bases de datos. <b>Fin del subproceso</b>	Analista de Infraestructura de Tecnologías de la Información	N/A
4	Analizar requerimiento	<b>Requerimiento:</b> Analizar la factibilidad de atender el requerimiento realizado por el usuario.	Director(a) DITIC	N/A
	Decisión	<b>¿Es factible atender el requerimiento?</b> <b>SI:</b> Pasa a la actividades <b>6.</b> Seleccionar servidor, <b>11</b> Administrar BDD, <b>16.</b> Respalidar BDD y <b>30.</b> Pruebas de Bases de Datos. <b>NO:</b> Pasa a la actividad <b>5.</b> Notificar que no es factible.	Director(a) DITIC	N/A
5	Notificar que no es factible	Realizar un informe en el cual se notifica al área requirente que no es factible dar atención a su requerimiento, dentro de la respuesta se explicarán las razones. <b>Fin del subproceso.</b>	Director(a) DITIC	Correo electrónico o memorando
6	Seleccionar servidor	Realizar la selección del servidor para respaldar correctamente la información que se vaya a almacenar.	Analista de Infraestructura de Tecnologías de la Información	N/A
	Decisión	<b>¿Está instalado el motor de la BDD?</b> <b>SI:</b> Pasa a la siguiente decisión. ¿Existe BDD?	Analista de Infraestructura de Tecnologías de la Información	N/A

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------

		<b>NO:</b> Pasa a la actividad <b>7</b> . Instalar, configurar BDD.		
7	Instalar, configurar BDD	Instalar, configurar y afinar el motor de base de datos. <b>Pasa a la actividad 8</b> . Crear BDD.	Analista de Infraestructura de Tecnologías de la Información	N/A
	Decisión	<b>¿Existe la base de datos?</b> <b>SI:</b> Pasa a la actividad <b>9</b> . Ejecutar script. <b>NO:</b> Pasa a la actividad <b>8</b> . Crear BDD.	Analista de Infraestructura de Tecnologías de la Información	N/A
8	Crear BDD	Crear la base de datos requerida.	Analista de Infraestructura de Tecnologías de la Información	N/A
9	Ejecutar script	Ejecutar el script de la base de datos.	Analista de Infraestructura de Tecnologías de la Información	N/A
10	Notificar	Notificar mediante correo electrónico a los usuarios que se atendió el requerimiento, con copia al Director del área requirente. <b>Fin del subproceso.</b>	Analista de Infraestructura de Tecnologías de la Información	Correo electrónico
11	Administrar BDD	Administrar las bases de datos para su normal ejecución. <b>Pasa a las actividades 12</b> Administrar usuarios, <b>13</b> Modificar base de datos, y <b>14</b> . Realizar reporte.	Analista de Infraestructura de Tecnologías de la Información	N/A
12	Administrar usuarios	Administrar los usuarios activos para acceder a la base de datos. <b>Pasa a la actividad 15</b> . Notificar al usuario.	Analista de Infraestructura de Tecnologías de la Información	N/A
13	Modificar BDD	Modificar la base de datos. <b>Pasa a la actividad 15</b> . Notificar al usuario.	Analista de Infraestructura de Tecnologías de la Información	N/A
14	Realizar reportes	Realizar reportes acerca de lo analizado de las bases de datos.	Analista de Infraestructura de Tecnologías de la Información	N/A
15	Notificar al usuario	Notificar mediante correo electrónico a los usuarios que se atendió el requerimiento, con copia al Director del área requirente. <b>Fin del subproceso.</b>	Analista de Infraestructura de Tecnologías de la Información	Correo electrónico
16	Respalidar BDD	Realizar el respaldo de la base de datos con base en el requerimiento que realizo la unidad solicitante.	Analista de Infraestructura de Tecnologías de la Información	N/A
	Decisión	<b>¿Es factible realizar el respaldo?</b> <b>SI:</b> Pasa a la siguiente decisión. ¿Restore o Backup?	Analista de Infraestructura de Tecnologías de la Información	N/A

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------

		<b>NO:</b> Pasa a la actividad <b>17</b> . Redactar notificación.		
17	Notificar al usuario	Notificar mediante correo electrónico a los usuarios que se atendió el requerimiento, con copia al Director del área requirente. <b>Fin del subproceso.</b>	Analista de Infraestructura de Tecnologías de la Información	Correo electrónico
	Decisión	<b>¿El requerimiento se trata de un Restore o Backup?</b> <b>Restore:</b> Pasa a la actividad <b>26</b> . Seleccionar respaldo. <b>Backup:</b> Pasa a la siguiente decisión. ¿Es respaldo programado o solicitado?	Analista de Infraestructura de Tecnologías de la Información	N/A
	Decisión	<b>Backup</b> <b>¿Es respaldo programado o solicitado?</b> <b>Programado:</b> Pasa a la decisión. <b>¿Creación o modificación de script?</b> <b>Solicitado:</b> Pasa a la actividad <b>18</b> . Ejecutar script.	Analista de Infraestructura de Tecnologías de la Información	N/A
18	Ejecutar script	<b>Backup solicitado:</b> Realizar la ejecución del respectivo script restore.	Analista de Infraestructura de Tecnologías de la Información	N/A
	Decisión	<b>¿Es script restore?</b> <b>SI:</b> Pasa a la actividad <b>28</b> . Ejecutar script restore. <b>NO:</b> Pasa a las actividades <b>19</b> . Notificar al usuario y <b>24</b> . Colocar en medio externo.	Analista de Infraestructura de Tecnologías de la Información	N/A
19	Notificar al usuario	Notificar mediante correo electrónico a los usuarios que se atendió el requerimiento, con copia al Director del área requirente. <b>Fin del subproceso.</b>	Analista de Infraestructura de Tecnologías de la Información	Correo electrónico
	Decisión	<b>Programado</b> <b>¿Se trata de una creación o modificación de script?</b> <b>Creación:</b> Pasa a la actividad <b>21</b> . Elaborar script. <b>Modificación:</b> Pasa a la actividad <b>20</b> . Modificar script.	Analista de Infraestructura de Tecnologías de la Información	N/A
20	Modificar script	Modificar el script de la base de datos con base en la especificado en el requerimiento. <b>Pasa a la actividad 23.</b> Ejecutar script.	Analista de Infraestructura de Tecnologías de la Información	N/A
21	Crear script	Crear el script para la base de datos en	Analista de Infraestructura	N/A

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------

		relación a lo solicitado.	de Tecnologías de la Información	
22	Programar periodicidad	Realizar la programación de la periodicidad de la ejecución del script.	Analista de Infraestructura de Tecnologías de la Información	Programación
23	Ejecutar script	Ejecutar el script de la base de datos según lo programado.	Analista de Infraestructura de Tecnologías de la Información	N/A
24	Colocar en medio externo	Colocar la base de datos en un medio externo o en el NAS.	Analista de Infraestructura de Tecnologías de la Información	N/A
25	Notificar al usuario	Notificar mediante correo electrónico a los usuarios que se atendió el requerimiento, con copia al Director del área requirente. <b>Fin del subproceso.</b>	Analista de Infraestructura de Tecnologías de la Información	Correo electrónico
26	Seleccionar respaldo	<b>Restore:</b> Seleccionar el respaldo de la información requerida.	Analista de Infraestructura de Tecnologías de la Información	N/A
27	Elaborar respaldos	Elaborar los respaldos de la información requerida.	Analista de Infraestructura de Tecnologías de la Información	N/A
28	Ejecutar script	Ejecutar el script restore correspondiente.	Analista de Infraestructura de Tecnologías de la Información	N/A
29	Notificar al usuario	Notificar mediante correo electrónico a los usuarios que se atendió el requerimiento, con copia al Director del área requirente. <b>Fin del subproceso.</b>	Analista de Infraestructura de Tecnologías de la Información	N/A
30	Recoger el "Back up"	<b>Prueba de Bases de datos:</b> Recoger el "back up" del servidor origen de Base de Datos al servidor de pruebas (destino).	Analista de Infraestructura de Tecnologías de la Información	N/A
31	Copiar el "Back up"	Copia el "back up" en la Unidad de pruebas seleccionada	Analista de Infraestructura de Tecnologías de la Información	N/A
32	Restaurar la base de datos	Restaurar la base de datos mediante script de BBDD	Analista de Infraestructura de Tecnologías de la Información	N/A
33	Analizar si restauró correctamente	Analiza si se restauró correctamente la Base de Datos.	Analista de Infraestructura de Tecnologías de la	N/A

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------

			Información	
	Decisión	<b>¿Se restauró correctamente?</b> <b>NO:</b> Realiza la actividad <b>34.</b> Notificar y guardar en bitácora. <b>SI:</b> Realiza la actividad <b>35.</b> Guardar en bitácora.	Analista de Infraestructura de Tecnologías de la Información	N/A
34	Guardar en bitácora	Guarda en bitácora la no restauración de la BBDD. <b>Fin del proceso.</b>	Analista de Infraestructura de Tecnologías de la Información	N/A
35	Guardar en bitácora y generar informe	Guarda en bitácora la restauración de la BBDD y generar el Informe trimestral de bases de datos testeadas. <b>Fin del proceso.</b>	Analista de Infraestructura de Tecnologías de la Información	Informe Trimestral de bases de datos Testeadas

#### 5.6.5. INDICADORES DEL SUBPROCESO DE ADMINISTRACIÓN DE BASE DE DATOS

N°	Indicador	Fórmula de Cálculo	Unidad de Medida	Responsable de Medición	Fuente de Medición	Frecuencia de Medición
1	Porcentaje de cumplimiento de la administración de base de datos	(# de requerimientos realizados de base de datos / # de requerimientos solicitadas de la base de datos) * 100%	%	Responsable de Infraestructura	Informe técnico de ejecución	Trimestral

#### 5.6.6. FORMATOS DEL SUBPROCESO DE ADMINISTRACIÓN DE BASE DE DATOS

Nombre del Registro de Calidad	Código de Formato
N/A	N/A

#### 5.6.7. ANEXOS DEL SUBPROCESO DE ADMINISTRACIÓN DE BASE DE DATOS

“No hay anexos.”

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------

## 5.7. SUBPROCESO DE ASESORAMIENTO TECNOLÓGICO DE INFRAESTRUCTURA

### 5.7.1. FICHA TÉCNICA DEL SUBPROCESO DE ASESORAMIENTO TECNOLÓGICO DE INFRAESTRUCTURA

<b>Proceso:</b>	GESTIÓN DE INFRAESTRUCTURA DE TECNOLOGÍAS DE LA INFORMACIÓN
<b>Nombre del Subproceso:</b>	ASESORAMIENTO TECNOLÓGICO DE INFRAESTRUCTURA
<b>Código del Subproceso:</b>	DITIC-TI-SP7
<b>Descripción:</b>	<p><b>PROPÓSITO:</b> Proporcionar asesoramiento tecnológico a los usuarios del INEC, además elaborar los documentos necesarios en base a formatos gubernamentales hasta la adquisición de un bien o servicio tecnológico.</p> <p><b>ALCANCE:</b> Desde analizar y reasignar el requerimiento o especificación, hasta aprobar y reasignar la documentación a la unidad ejecutora requirente.</p> <p><b>DISPARADOR:</b></p> <ul style="list-style-type: none"> <li>• Memorandos, correos electrónicos y sistema GLPI</li> </ul> <p><b>PROVEEDORES:</b></p> <ul style="list-style-type: none"> <li>• Procesos sustantivos y adjetivos del INEC</li> </ul> <p><b>INSUMOS:</b></p> <ul style="list-style-type: none"> <li>• Memorandos o correos electrónicos</li> <li>• Tickets de atención del GLPI</li> </ul>
<b>Clientes:</b>	<ul style="list-style-type: none"> <li>• Procesos sustantivos y adjetivos del INEC.</li> </ul>
<b>Salidas:</b>	<ul style="list-style-type: none"> <li>• TDRs</li> <li>• Comisiones AdHoc</li> <li>• Comisiones para presupuesto referencial.</li> <li>• Documentación de aprobación de organismos gubernamentales.</li> </ul>
<b>Tipo de Proceso:</b>	<ul style="list-style-type: none"> <li>• Adjetivo de asesoría</li> </ul>
<b>Responsable del Proceso:</b>	Responsable de Gestión de Infraestructura de Tecnologías de la Información
<b>Recursos:</b>	<p><b>MATERIALES:</b></p> <ul style="list-style-type: none"> <li>• Equipo de computación</li> <li>• Equipo y materiales de oficina.</li> </ul> <p><b>HUMANOS:</b></p> <ul style="list-style-type: none"> <li>• 2 Analistas de Gestión de Infraestructura de TI SP7.</li> <li>• 4 Analistas de Gestión de Infraestructura de TI SP5.</li> <li>• 1 Analista de Gestión de Infraestructura de TI SP1.</li> </ul>

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------

	<b>TECNOLÓGICOS:</b> <ul style="list-style-type: none"> <li>• Correo Electrónico.</li> <li>• Software Ofimática.</li> <li>• Acceso a internet.</li> </ul>
<b>Controles/Marco Legal:</b>	<ul style="list-style-type: none"> <li>• Resolución 030- DIREJ-DIJU-NI2012</li> </ul>

### 5.7.2. CONTROLES DEL SUBPROCESO DE ASESORAMIENTO TECNOLÓGICO DE INFRAESTRUCTURA

Resolución 030- DIREJ-DIJU-NI2012 Uso de Los servicios Tecnológicos y Políticas de la Dirección de Tecnologías de la Información y Comunicación del Instituto Nacional de Estadística Y Censos

- Normativa de Seguridad de La información, 410-11 Plan de contingencias

Plan de continuidad de las operaciones que contemplará la puesta en marcha de un centro de cómputo alternativo propio o de uso compartido en un Data Center Estatal, mientras dure la contingencia con el restablecimiento de las comunicaciones y recuperación de la información de los respaldos.

1. Objetivo.- definir las reglas generales para establecer una adecuada protección de los equipos informáticos en el Data Center del INEC.

2. Serán Responsables.- todo el personal del área de DITIC del INEC y los terceros que interactúan de manera habitual u ocasional que estén vinculados a los mantenimientos.

3. Incumplimientos.- las medidas disciplinarias serán aplicadas según resolución publicada, la normativa interna y las que determinaren las entidades de control del estado ecuatoriano.

4. Definiciones.- conexiones internas.- adicionalmente a las medidas de protección física y de acceso de usuarios ya definidas en las respectivas normas, se deben tener en cuenta las siguientes consideraciones adicionales:

- Verificar que el sistema de monitoreo y acceso al data center estén en perfecta condiciones.

- Mantener en perfecto estado los equipos de enfriamiento para no provocar un calentamiento en la granja de servidores.

- Mantener el sistema de monitoreo, motores para no tener complicaciones de alguna avería

- Asegurarse que todas las conexiones externas con la red interna del INEC se realicen a través de puntos controlados, que deben contemplar entre otras cosas, que estén conectadas a la red interna y el data center.

#### NORMAS DE CONTROL INTERNO DE LA CONTRALORIA GENERAL DEL ESTADO

##### 410-08 Adquisiciones de infraestructura tecnológica

La unidad de tecnología de información definirá, justificará, implantará y actualizará la infraestructura tecnológica de la organización para lo cual se considerarán los siguientes aspectos:

1. Las adquisiciones tecnológicas estarán alineadas a los objetivos de la organización, principios de calidad de servicio, portafolios de proyectos y servicios, y constarán en el plan anual de contrataciones aprobado de la institución, caso contrario serán autorizadas por la máxima autoridad previa justificación técnica documentada.

2. La unidad de tecnología de información planificará el incremento de capacidades, evaluará los riesgos tecnológicos, los costos y la vida útil de la inversión para futuras actualizaciones, considerando los requerimientos de carga de trabajo, de almacenamiento, contingencias y ciclos de vida de los recursos tecnológicos. Un análisis de costo beneficio para el uso compartido de Data Center con otras entidades del sector público, podrá ser considerado para optimizar los recursos invertidos.

<b>Elaborado por:</b>	<b>Revisado por:</b>	<b>Aprobado /Autorizado por:</b>	<b>Registrado por:</b>
PC	DIPLA - DIFI	DIREJ	DIPLA, PC



3. En la adquisición de hardware, los contratos respectivos, tendrán el detalle suficiente que permita establecer las características técnicas de los principales componentes tales como: marca, modelo, número de serie, capacidades, unidades de entrada/salida, entre otros, y las garantías ofrecidas por el proveedor, a fin de determinar la correspondencia entre los equipos adquiridos y las especificaciones técnicas y requerimientos establecidos en las fases precontractual y contractual, lo que será confirmado en las respectivas actas de entrega/recepción.

4. Los contratos con proveedores de servicio incluirán las especificaciones formales sobre acuerdos de nivel de servicio, puntualizando explícitamente los aspectos relacionados con la seguridad y confidencialidad de la información, además de los requisitos legales que sean aplicables. Se aclarará expresamente que la propiedad de los datos corresponde a la organización contratante.

#### 410-13 Monitoreo y evaluación de los procesos y servicios

Es necesario establecer un marco de trabajo de monitoreo y definir el alcance, la metodología y el proceso a seguir para monitorear la contribución y el impacto de tecnología de información en la entidad.

#### ACUERDO 166 EGS (ESQUEMA GUBERNAMENTAL DE SISTEMAS DE INFORMACION)

### 2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

2.4 Proceso de autorización para nuevos servicios de procesamiento de la información d) Evaluar la compatibilidad a nivel de hardware y software

### 5. SEGURIDAD FISICA Y DEL ENTORNO

a) Brindar mantenimientos periódicos a los equipos y dispositivos, de acuerdo a las especificaciones y recomendaciones del proveedor.

b) Realizar el mantenimiento de los equipos únicamente con personal calificado y autorizado.

c) Conservar los registros de los mantenimientos preventivos, correctivos y fallas relevantes o sospechosas.

d) Establecer controles apropiados para realizar mantenimientos programados y emergentes.

e) Gestionar mantenimientos planificados con hora de inicio, fin, impacto y responsables y poner previamente en conocimiento de administradores y usuarios finales.

### 6. GESTION DE OPERACIONES Y COMUNICACIONES

#### 6.7 Gestión de los cambios en los servicios ofrecidos por terceros

a) Establecer un proceso de gestión de cambios en los servicios ofrecidos por terceros, en el desarrollo de aplicaciones, provisión de servicios de hardware, software, redes, otros.

b) Coordinar el proceso de cambio cuando se necesita realizar cambios o mejoras a las redes y uso de nuevas tecnologías en los servicios ofrecidos por terceros.

c) Coordinar el proceso de cambio cuando se realice cambio de proveedores, cambio de ubicación física en los servicios ofrecidos por terceros.

#### 6.8 Gestión de la capacidad

a) Realizar proyecciones de los requerimientos de capacidad futura de recursos para asegurar el desempeño de los servicios y sistemas informáticos

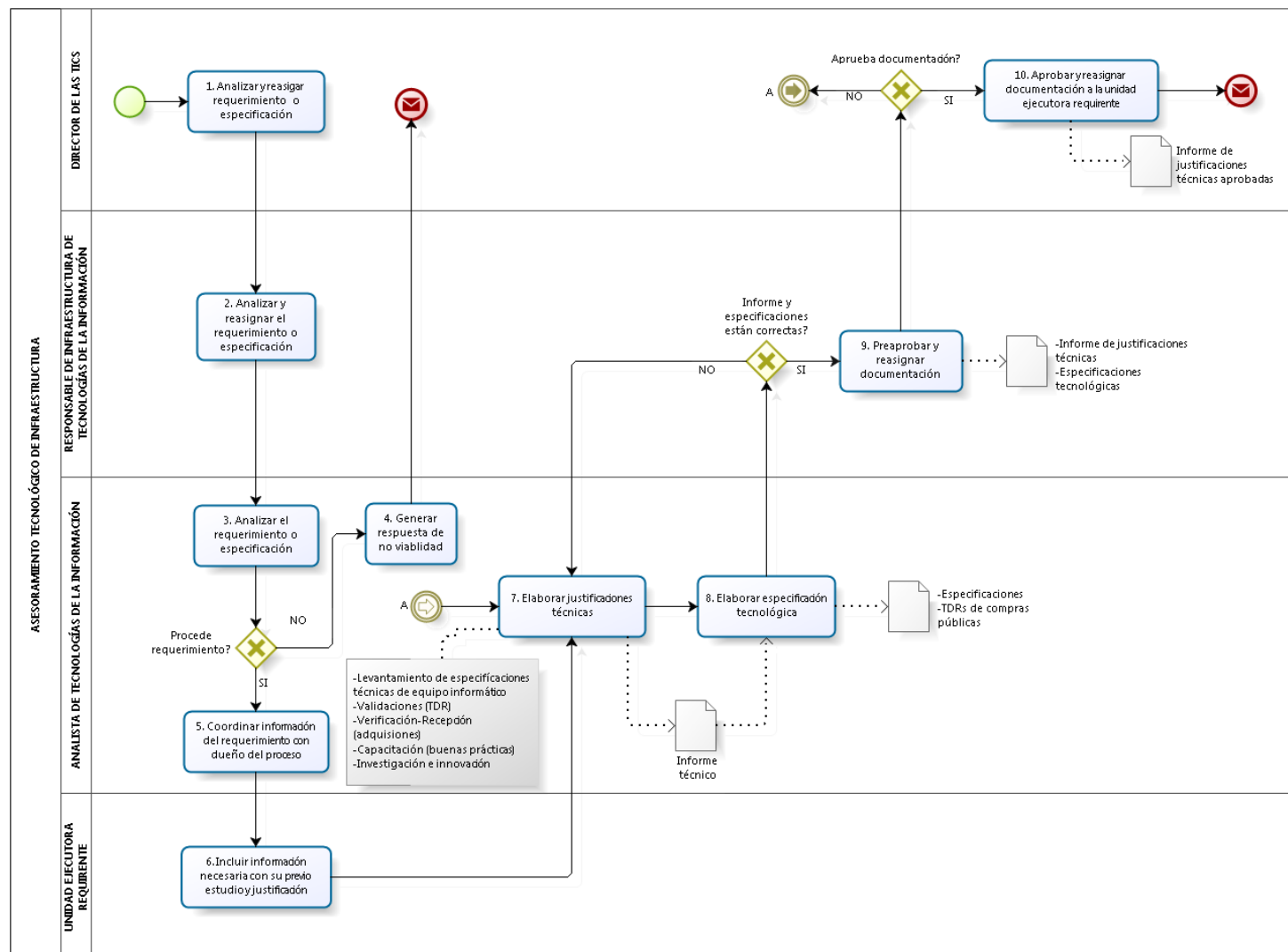
b) Monitorear los recursos asignados para garantizar la capacidad y rendimiento de los servicios y sistemas informáticos

c) Utilizar la información del monitoreo para la adquisición, asignación de recursos y evitar cuellos de botella.

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------



### 5.7.3. DIAGRAMA DE FLUJO DEL SUBPROCESO DE ASESORAMIENTO TECNOLÓGICO DE INFRAESTRUCTURA



<b>Elaborado por:</b>	<b>Revisado por:</b>	<b>Aprobado /Autorizado por:</b>	<b>Registrado por:</b>
PC	DIPLA - DIFI	DIREJ	DIPLA, PC

#### 5.7.4. PROCEDIMIENTO DEL SUBPROCESO DE ASESORAMIENTO TECNOLÓGICO DE INFRAESTRUCTURA

N	Actividad	Descripción	Rol	Documento generado
1	Analizar y reasignar requerimiento o especificación	Realiza el análisis y reasignación del requerimiento o especificación	Director de las TICS	N/A
2	Analizar y reasignar el requerimiento o especificación	Realiza el análisis y reasignación del requerimiento o especificación de la unidad ejecutora que realice el requerimiento	Responsable de Infraestructura de Tecnologías de la Información	N/A
3	Analizar el requerimiento o especificación	Realiza el análisis del requerimiento o especificación	Analista de tecnologías de la información	N/A
	Decisión	<b>¿Procede requerimiento?</b> <b>NO:</b> Pasa a la actividad 4. Generar respuesta de no viabilidad. <b>SI:</b> Pasa a la actividad 5. Coordinar información del requerimiento con dueño del proceso.	Analista de tecnologías de la información	N/A
4	Generar respuesta de no viabilidad	Realiza la generación a la respuesta de no viabilidad. <b>Termina el proceso.</b>	Analista de tecnologías de la información	N/A
5	Coordinar información del requerimiento con dueño del proceso	Realiza la coordinación de la información del requerimiento con el dueño del proceso	Analista de tecnologías de la información	N/A
6	Incluir información necesaria con su previo estudio y justificación	Realiza la inclusión de la información necesaria con su previo estudio y justificación	Unidad ejecutora requirente	N/A
7	Elaborar justificaciones técnicas	Realiza las justificaciones técnicas	Analista de tecnologías de la información	Informe técnico
8	Elaborar especificación tecnológica	Realiza la especificación tecnológica para su análisis	Analista de tecnologías de la información	Especificaciones TDRs de compras públicas
	Decisión	<b>¿Informe y especificaciones están correctos?</b> <b>NO:</b> Pasa a la actividad 7. Elaborar justificaciones técnicas. <b>SI:</b> Pasa a la actividad 9. Pre aprobar y reasignar documentación.	Responsable de Infraestructura de Tecnologías de la Información	N/A
9	Pre aprobar y reasignar documentación	Realiza la pre aprobación y reasignación del documento para su aprobación oficial	Responsable de Infraestructura de Tecnologías de la Información	TDR y/o informes de presupuesto referencial
	Decisión	<b>¿Aprueba documentación?</b> <b>NO,</b> Elaborar justificaciones té la actividad 7 <b>SI,</b> Aprobar y reasignar documentación a la	Responsable de Infraestructura de Tecnologías de la Información	N/A

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------



		unidad ejecutora requirente, fin. Pasar a la actividad 10		
10	Aprobar y reasignar documentación a la unidad ejecutora requirente, fin	Realiza la aprobación y reasignación del documento a la unidad ejecutora requirente	Director de las TICS	TDR y/o informes de presupuesto referencial

#### 5.7.5. INDICADORES DEL SUBPROCESO DE ASESORAMIENTO TECNOLÓGICO DE INFRAESTRUCTURA

N°	Indicador	Fórmula de Cálculo	Unidad de Medida	Responsable de Medición	Fuente de Medición	Frecuencia de Medición
1	Porcentaje de cumplimiento en la gestión de asesoramiento tecnológico	$(\# \text{ de requerimientos atendidos} / \# \text{ de requerimientos solicitados}) * 100\%$	Porcentaje	Responsable de Infraestructura	Informe técnico de ejecución	Trimestral

#### 5.7.6. FORMATOS DEL SUBPROCESO DE ASESORAMIENTO TECNOLÓGICO DE INFRAESTRUCTURA

Nombre del Registro de Calidad	Código de Formato
N/A	N/A

#### 5.7.7. ANEXOS DEL SUBPROCESO DE ASESORAMIENTO TECNOLÓGICO DE INFRAESTRUCTURA

“No hay anexos.”

Elaborado por: PC	Revisado por: DIPLA - DIFI	Aprobado /Autorizado por: DIREJ	Registrado por: DIPLA, PC
----------------------	-------------------------------	------------------------------------	------------------------------

## 5.8. SUBPROCESO DE SOPORTE A USUARIOS EN INFRAESTRUCTURA

### 5.8.1. FICHA TÉCNICA DEL SUBPROCESO DE SOPORTE A USUARIOS EN INFRAESTRUCTURA

<b>Proceso:</b>	GESTIÓN DE INFRAESTRUCTURA DE TECNOLOGÍAS DE LA INFORMACIÓN
<b>Nombre del Subproceso:</b>	SOPORTE A USUARIOS EN INFRAESTRUCTURA
<b>Código del Subproceso:</b>	DITIC-TI-SP8
<b>Descripción:</b>	<p><b>PROPÓSITO:</b> Brindar un óptimo servicio a los requerimientos tecnológicos de los usuarios internos para el desarrollo de las actividades de la institución.</p> <p><b>ALCANCE:</b> Desde enviar requerimiento según necesidad, hasta realizar el informe de soportes atendidos.</p> <p><b>DISPARADOR:</b></p> <ul style="list-style-type: none"> <li>• Correos, memorandos y sistema GLPI</li> </ul> <p><b>PROVEEDORES:</b></p> <ul style="list-style-type: none"> <li>• Procesos adjetivos y sustantivos del INEC.</li> </ul> <p><b>INSUMOS:</b></p> <ul style="list-style-type: none"> <li>• Correos</li> <li>• Memorandos</li> <li>• Tickets de atención al usuario del GLPI</li> </ul>
<b>Clientes:</b>	<ul style="list-style-type: none"> <li>• Procesos adjetivos y sustantivos del INEC</li> </ul>
<b>Salidas:</b>	<ul style="list-style-type: none"> <li>• Informe técnico de los soportes atendidos</li> </ul>
<b>Tipo de Proceso:</b>	<ul style="list-style-type: none"> <li>• Adjetivo de asesoría</li> </ul>
<b>Responsable del Proceso:</b>	Jefe de Gestión de Tecnologías de la Información y Comunicación.
<b>Recursos:</b>	<p><b>MATERIALES:</b></p> <ul style="list-style-type: none"> <li>• Equipo de computación</li> <li>• Equipo y materiales de oficina.</li> </ul> <p><b>HUMANOS:</b></p> <ul style="list-style-type: none"> <li>• 2 Analistas de Gestión de Infraestructura de TI SP7.</li> <li>• 4 Analistas de Gestión de Infraestructura de TI SP5.</li> <li>• 1 Analista de Gestión de Infraestructura de TI SP1.</li> </ul> <p><b>TECNOLÓGICOS:</b></p> <ul style="list-style-type: none"> <li>• Correo Electrónico.</li> <li>• Software Ofimática.</li> <li>• Acceso a internet.</li> <li>• Herramientas para soporte en redes.</li> </ul>

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------

<b>Controles/Marco Legal:</b>	<ul style="list-style-type: none"> <li>• Normas de Control Interno de la Contraloría General del Estado</li> <li>• CODIGO 410-12</li> </ul>

## 5.8.2. CONTROLES DEL SUBPROCESO DE SOPORTE A USUARIOS EN INFRAESTRUCTURA

### Normas de Control Interno de la Contraloría General del Estado CODIGO 410-12

6. Definición y manejo de niveles de servicio y de operación para todos los procesos críticos de tecnología de información sobre la base de los requerimientos de los usuarios o clientes internos y externos de la entidad y a las capacidades tecnológicas.

7. Alineación de los servicios claves de tecnología de información con los requerimientos y las prioridades de la organización sustentados en la revisión, monitoreo y notificación de la efectividad y cumplimiento de dichos acuerdos.

Esquema Gubernamental de Seguridad de la información

#### 3.1 Inventario de activos

e) Los manuales e instructivos de sistemas informáticos: instalación, guía de usuario, operación, administración, mantenimiento, entre otros.

f) De la operación de los aplicativos informáticos de los servicios informáticos: datos y meta- datos asociados, archivos de configuración, código fuente, respaldos, versiones, etc.

g) Del desarrollo de aplicativos de los servicios informáticos: actas de levantamiento de requerimientos, documento de análisis de requerimientos, modelos entidad – relación, diseño de componentes, casos de uso, diagramas de flujo y estado, casos de prueba, etc.

h) Del soporte de aplicativos de los servicios informáticos: tickets de soporte, reportes físicos y electrónicos, evaluaciones y encuestas, libros de trabajo para capacitación, etc.

j) Equipos móviles: teléfono inteligente (Smartphone), teléfono celular, tableta, computador portátil, asistente digital personal (PDA), etc.

k) Equipos fijos: servidor de torre, servidor de cuchilla, servidor de rack, computador de escritorio, computadoras portátiles, etc.

n) Periféricos y dispositivos de almacenamiento: sistema de almacenamiento (NAS, SAN), librería de cintas, cintas magnéticas, disco duro portátil, disco flexible, grabador de discos (CD, DVD, Blu-ray), CD, DVD, Blu-ray, memoria USB, etc.

o) Periféricos de comunicaciones: tarjeta USB para redes inalámbricas (Wi-Fi, Bluetooth, GPRS, HSDPA), tarjeta PCMCIA para redes inalámbricas (Wi-Fi, Bluetooth, GPRS, HSDPA), tarjeta USB para redes alámbricas/inalámbricas de datos y de telefonía, etc.

p) Tableros: de transferencia (bypass) de la unidad interrumpible de energía (UPS), de salidas de energía eléctrica, de transferencia automática de energía, etc.

q) Sistemas: de control de accesos, de aire acondicionado, automático de extinción de incendios, de circuito cerrado de televisión, etc.

r) Sistemas operativos.

s) Software de servicio, mantenimiento o administración de: gabinetes de servidores de cuchilla, servidores (estantería/rack, torre, virtuales), sistema de redes de datos, sistemas de almacenamiento (NAS, SAN), telefonía, sistemas (de UPS, grupo electrógeno, de aire acondicionado, automático de extinción de incendios, de circuito cerrado de televisión), etc.

t) Paquetes de software o software base de: suite de ofimática, navegador de Internet, cliente de correo electrónico, mensajería instantánea, edición de imágenes, vídeo conferencia, servidor (proxy, de archivos, de correo electrónico, de impresiones, de mensajería instantánea, de aplicaciones, de base de datos), etc.

<b>Elaborado por:</b>	<b>Revisado por:</b>	<b>Aprobado /Autorizado por:</b>	<b>Registrado por:</b>
PC	DIPLA - DIFI	DIREJ	DIPLA, PC



u) Aplicativos informáticos del negocio.

5.10 Mantenimiento de los equipos

d) Establecer controles apropiados para realizar mantenimiento.

6.8 Gestión de capacidad

a) Realizar proyecciones de los requerimientos de capacidad futura de recursos para asegurar el desempeño de los servicios y sistemas informáticos.

b) Monitorear los recursos asignados para garantizar la capacidad y rendimiento de los servicios y sistemas informáticos.

6.10. Controles contra código malicioso

d) Mantener los sistemas operativos y sistemas de procesamiento de información actualizados con las últimas versiones de seguridad disponibles.

e) Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos de la institución.

6.31 Sincronización de relojes

a) Sincronizar los relojes de los sistemas de procesamiento de información pertinentes con una fuente de tiempo exacta (ejemplo el tiempo coordinado universal o el tiempo estándar local).

En lo posible, se deberá sincronizar los relojes en base a un protocolo o servicio de tiempo de red para mantener todos los equipos sincronizados.

7.6 Uso de contraseñas

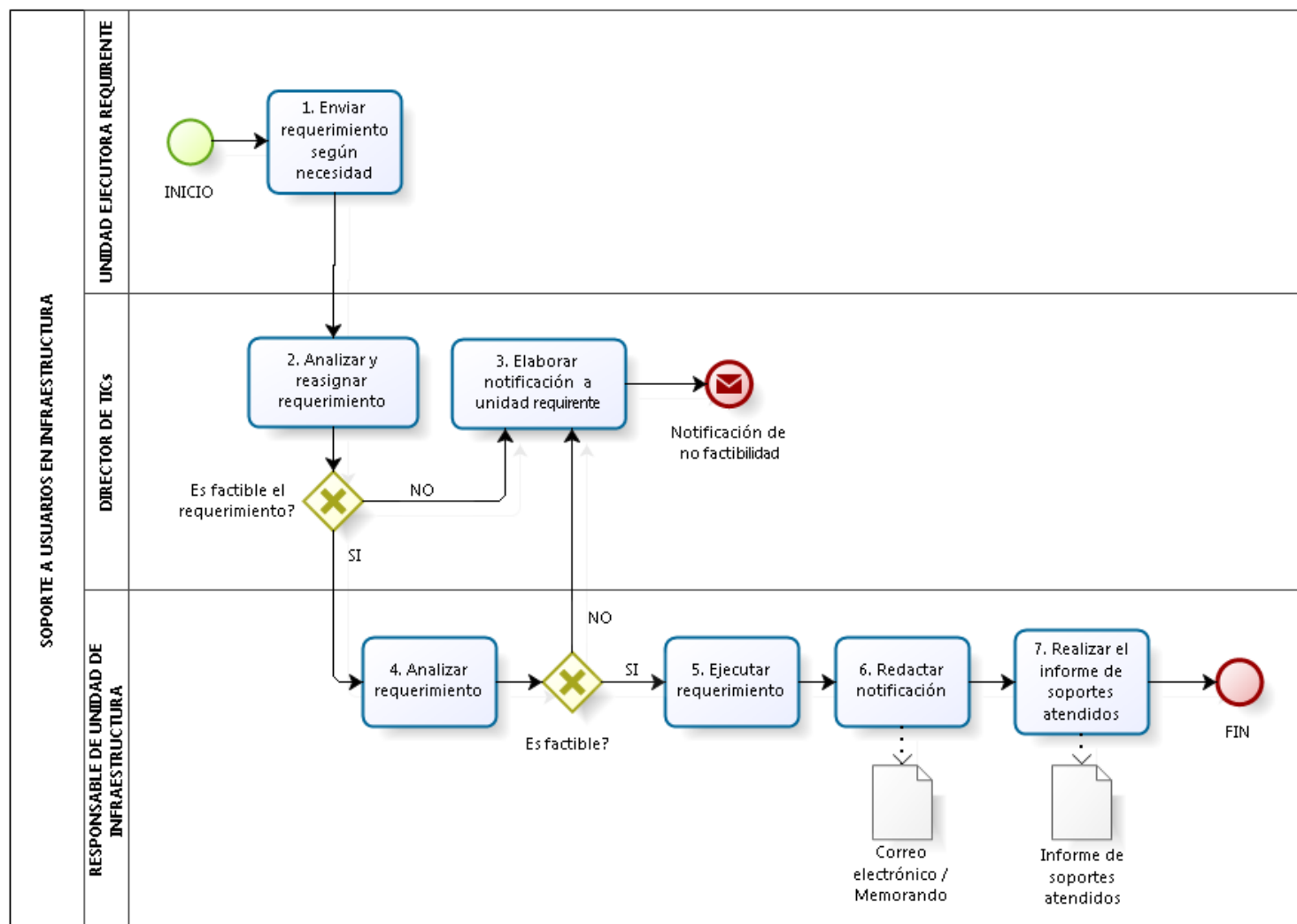
a) Documentar, en el procedimiento de accesos, las responsabilidades de los usuarios tanto internos como externos, sobre el uso de la cuenta y la contraseña asignada.

9.1 Reporte sobre los eventos de seguridad de la información

a) Instaurar un procedimiento formal para el reporte de los eventos de seguridad de la información junto con un procedimiento de escalada y respuesta ante el incidente, que establezca la acción que se ha de tomar al recibir el reporte sobre un evento que amenace la seguridad de la información.

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------

### 5.8.3. DIAGRAMA DE FLUJO DEL SUBPROCESO DE SOPORTE A USUARIOS EN INFRAESTRUCTURA



Elaborado por:  
PC

Revisado por:  
DIPLA - DIFI

Aprobado /Autorizado por:  
DIREJ

Registrado por:  
DIPLA, PC

#### 5.8.4. PROCEDIMIENTO DEL SUBPROCESO DE SOPORTE A USUARIOS EN INFRAESTRUCTURA

Nº	Actividad	Detalle de la actividad	Responsable	Documento Generado
1	Enviar requerimiento según necesidad	Envía el requerimiento según la necesidad informática que sea necesario	Unidad ejecutora	N/A
2	Analizar y reasignar requerimiento	Analiza y reasigna el requerimiento para identificar su ejecución o no	Director de TICs	N/A
	Decisión	<b>¿Es factible el requerimiento?</b> <b>NO:</b> Pasa a la actividad 3. Elaborar notificación a unidad requirente. <b>SI:</b> Pasa a la actividad 4. Analizar requerimiento.	Director de TICs	N/A
3	Elaborar notificación a unidad requirente	Elabora una notificación a la unidad requirente, informando la no factibilidad de ejecución del requerimiento solicitado. <b>Fin del proceso.</b>	Director de TICs	N/A
4	Analizar requerimiento	Analiza el tipo de requerimiento para identificar si es factible o no	Responsable de unidad de infraestructura	N/A
	Decisión	<b>¿Es factible?</b> <b>NO:</b> Regresa a la actividad 3. Notifica a la unidad requirente. <b>SI:</b> Pasar a la actividad 5. Atender el requerimiento.	Responsable de unidad de infraestructura	N/A
5	Atender el requerimiento	Realiza el soporte de infraestructura solicitado.	Analista de la Unidad de infraestructura	N/A
6	Elaborar notificación a unidad requirente	Elabora la respectiva notificación a la unidad requirente que solicitó el servicio informático mediante el sistema GLPI, correo electrónico o memorando	Analista de la Unidad de infraestructura	Correo electrónico / Memorando
7	Realizar el informe de soportes atendidos	Realiza la información de los soportes atendidos de manera trimestral	Analista de la Unidad de infraestructura	Informe de soportes atendidos

#### 5.8.5. INDICADORES DEL SUBPROCESO DE SOPORTE A USUARIOS EN INFRAESTRUCTURA

Nº	Indicador	Fórmula de Cálculo	Unidad de Medida	Responsable de Medición	Fuente de Medición	Frecuencia de Medición
1	Porcentaje de cumplimiento de soporte a usuarios internos	(# de acciones realizadas en soporte a usuarios internos / # de acciones solicitadas en soporte a usuarios internos)*100%	Porcentaje	Responsable de Infraestructura	Sistema GLPI	Trimestral

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------



#### 5.8.6. FORMATOS DEL SUBPROCESO DE SOPORTE A USUARIOS EN INFRAESTRUCTURA

Nombre del Registro de Calidad	Código de Formato
Informe de soportes atendidos	DIFI-IT-SP8-INF-01

#### 5.8.7. ANEXOS DEL SUBPROCESO DE SOPORTE A USUARIOS EN INFRAESTRUCTURA

“No hay anexos.”

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------

## 5.9. SUBPROCESO ADMINISTRACIÓN DE CORREO ELECTRÓNICO

### 5.9.1. FICHA TÉCNICA DEL SUBPROCESO DE ADMINISTRACIÓN DE CORREO ELECTRÓNICO

<b>Proceso:</b>	GESTIÓN DE INFRAESTRUCTURA DE TECNOLOGÍAS DE LA INFORMACIÓN
<b>Nombre del Subproceso:</b>	ADMINISTRACIÓN DE CORREO ELECTRÓNICO
<b>Código del Subproceso:</b>	DITIC-IT-SP9
<b>Descripción:</b>	<p><b>PROPÓSITO:</b></p> <p>Brindar a los usuarios de la institución la disponibilidad del envío y recepción de mensajes de correo electrónico, a través de la administración óptima del servidor.</p> <p><b>ALCANCE:</b></p> <p>Desde analizar el requerimiento y asignarlo, hasta informar al solicitante la respuesta a su requerimiento y realizar los respaldos de información.</p> <p><b>DISPARADOR:</b></p> <p>Solicitud de apertura de correo electrónico a usuario.</p> <p><b>PROVEEDORES:</b></p> <ul style="list-style-type: none"> <li>• Dirección de Administración de Recursos Humanos.</li> <li>• Dirección de Comunicación Social.</li> </ul> <p><b>INSUMOS:</b></p> <ul style="list-style-type: none"> <li>• Correo electrónico de solicitud.</li> </ul>
<b>Clientes:</b>	<ul style="list-style-type: none"> <li>• Unidades del INEC a nivel nacional.</li> </ul>
<b>Salidas:</b>	<ul style="list-style-type: none"> <li>• Informe de Disponibilidad del Correo Electrónico.</li> </ul>
<b>Tipo de Proceso:</b>	<ul style="list-style-type: none"> <li>• Adjetivo de asesoría.</li> </ul>
<b>Responsable del Proceso:</b>	Responsable de la Unidad de Gestión de Infraestructura de TI
<b>Recursos:</b>	<p><b>MATERIALES:</b></p> <ul style="list-style-type: none"> <li>• Equipo de computación</li> <li>• Equipo y materiales de oficina.</li> </ul> <p><b>HUMANOS:</b></p> <ul style="list-style-type: none"> <li>• 2 analistas de Gestión de Infraestructura de TI SP5.</li> <li>• 1 analista de Gestión de Infraestructura de TI SP7.</li> </ul> <p><b>TECNOLÓGICOS:</b></p> <ul style="list-style-type: none"> <li>• Correo Electrónico.</li> <li>• Software Ofimática.</li> <li>• Servidor de correo electrónico.</li> </ul>

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------

<b>Controles/Marco Legal:</b>	<ul style="list-style-type: none"> <li>• Firewall de correo electrónico.</li> </ul>
	<ul style="list-style-type: none"> <li>• Esquema gubernamental de seguridad de la información EGSI. gestión de los activos 3.1 literal t.</li> <li>• Esquema gubernamental de seguridad de la información EGSI. gestión de los activos 3.3 literal e y d.</li> <li>• Esquema gubernamental de seguridad de la información EGSI. gestión de los activos 3.3 literal e.</li> <li>• Esquema gubernamental de seguridad de la información EGSI. seguridad de los recursos humanos 4.9 literal a.</li> <li>• Esquema gubernamental de seguridad de la información EGSI. gestión de comunicaciones y operaciones 6.19 literal h.</li> <li>• Esquema gubernamental de seguridad de la información EGSI. gestión de comunicaciones y operaciones 6.20 literal d.</li> <li>• Esquema gubernamental de seguridad de la información EGSI. gestión de comunicaciones y operaciones 6.21 literal a.</li> <li>• Esquema gubernamental de seguridad de la información EGSI. gestión de comunicaciones y operaciones 6.22.</li> <li>• Esquema gubernamental de seguridad de la información EGSI. gestión de comunicaciones y operaciones 6.28 literal a.</li> <li>• Esquema gubernamental de seguridad de la información EGSI. control de acceso 7.4 literal a</li> <li>• Esquema gubernamental de seguridad de la información EGSI. adquisición, desarrollo y mantenimiento de sistemas de información 8.6 literal g.</li> <li>• Esquema gubernamental de seguridad de la información EGSI. adquisición, desarrollo y mantenimiento de sistemas de información 8.14 literal f.</li> <li>• Normas de control interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos. 403-13, transferencia de fondos por medios electrónicos.</li> <li>• Normas de control interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos. 410-14 sitio web, servicios de internet e intranet.</li> </ul>

### 5.9.2. CONTROLES DEL SUBPROCESO DE ADMINISTRACIÓN DE CORREO

#### 3 GESTIÓN DE LOS ACTIVOS

##### 3.1. Inventario de activos

t) Paquetes de software o software base de: suite de ofimática, navegador de Internet, cliente de correo electrónico, mensajería instantánea, edición de imágenes, vídeo conferencia, servidor (proxy, de archivos, de correo electrónico, de impresiones, de mensajería instantánea, de aplicaciones, de base de datos), etc.

##### 3.3. Uso aceptable de los activos

e) Reglamentar el acceso y uso de la Internet y sus aplicaciones/servicios (\*):

Todos los accesos deben poder ser sujetos de monitoreo y conservación permanente por parte de la institución.

d) Reglamentar el uso de correo electrónico institucional (\*):

- Este servicio debe utilizarse exclusivamente para las tareas propias de las funciones que se desarrollan en la institución y no debe utilizarse para ningún otro fin.
- Cada persona es responsable tanto del contenido del mensaje enviado como de cualquier otra información que adjunte.

<b>Elaborado por:</b>	<b>Revisado por:</b>	<b>Aprobado /Autorizado por:</b>	<b>Registrado por:</b>
PC	DIPLA - DIFI	DIREJ	DIPLA, PC

- Todos los mensajes deben poder ser monitoreados y conservados permanentemente por parte de la institución.
- Toda cuenta de correo electrónico debe estar asociada a una única cuenta de usuario.
- La conservación de los mensajes se efectuará en carpetas personales, para archivar la información de acceso exclusivo del usuario y que no debe compartirse con otros usuarios. Debe definirse un límite de espacio máximo.
- Toda la información debe ser gestionado de forma centralizados y no en las estaciones de trabajo de los usuarios.
- Todo sistema debe contar con las facilidades automáticas que notifiquen al usuario cuando un mensaje enviado por él no es recibido correctamente por el destinatario, describiendo detalladamente el motivo del error.
- Deben utilizarse programas que monitoreen el accionar de virus informáticos tanto en mensajes como en archivos adjuntos, antes de su ejecución.
- Todo usuario es responsable por la destrucción de los mensajes con origen desconocido, y asume la responsabilidad por las consecuencias que pueda ocasionar la ejecución de los archivos adjuntos. En estos casos, no deben contestar dichos mensajes y deben enviar una copia al Oficial de Seguridad de la Información para que efectúe el seguimiento y la investigación necesaria.
- Para el envío y la conservación de la información, debe implementarse el cifrado (criptografía) de datos.
- Todo usuario es responsable de la cantidad y tamaño de mensajes que envíe. Debe controlarse el envío no autorizado de correos masivos.

e) Reglamentar el acceso y uso de la Internet y sus aplicaciones/servicios (\*):

Se debe bloquear y prohibir el acceso y uso de servicios de correo electrónico de libre uso tales como: Gmail, Hotmail, Yahoo, Facebook, entre otros.

#### 4. SEGURIDAD DE LOS RECURSOS HUMANOS

##### 4.9. Retiro de los privilegios de acceso

a) Retirar los privilegios de acceso a los activos de información y a los servicios de procesamiento de información (ej., sistema de directorio, correo electrónico, accesos físicos, aplicaciones de software, etc.,) inmediatamente luego de que se comunique formalmente al Oficial de Seguridad de la Información formalmente la terminación de la relación laboral por parte del área correspondiente.

#### 6. GESTIÓN DE COMUNICACIONES Y OPERACIONES

##### 6.19. Políticas y procedimientos para el intercambio de información.

h) Definir directrices de retención y eliminación de la correspondencia incluyendo mensajes, según la normativa legal local.

##### 6.20. Acuerdos para el intercambio

d) Definir pautas para la identificación del prestador de servicio de correo.

##### 6.21. Medios físicos en tránsito

b) Establecer una lista de mensajería aprobada por la dirección

##### 6.22. Mensajería electrónica

a) Establecer lineamientos para proteger los mensajes contra los accesos no autorizados, modificación o denegación de los servicios.

b) Supervisar que la dirección y el transporte de mensajes sean correctos.

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------



c) Tomar en cuenta consideraciones legales como la de firmas electrónicas.

d) Encriptar los contenidos y/o información sensibles que puedan enviarse por mensajería electrónica; utilizando firmas electrónicas reconocidas por el Estado Ecuatoriano u otras tecnologías evaluadas y aprobadas por la entidad o el Gobierno Nacional.

e) Monitorear los mensajes de acuerdo al procedimiento que establezca la institución.

6.28. Protección del registro de la información.

a) Proteger de alteraciones en todos los tipos de mensaje que se registren.

7. Control de acceso

7.4. Gestión de contraseñas para usuarios

a) Establecer un proceso formal para la asignación y cambio de contraseñas (\*).

## **8. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN**

8.6. Política sobre el uso de controles criptográficos.

g) Los responsables del área de Tecnologías de la Información propondrán la siguiente asignación de funciones:

- Distribuir la primera clave a los usuarios, incluyendo la forma de activar y confirmar la recepción de la clave. Luego, a través de un correo electrónico recibirá un acceso al sistema, el cual validará la entrega de la clave y la obligatoriedad de cambiar dicha clave.

8.14. Fuga de información

f) Restringir el envío de información a correos externos no institucionales.

Normas de control interno para las entidades, organismos del sector público y personas jurídica de derecho privado que dispongan de recursos públicos.

403-13 Transferencia de fondos por medios electrónicos

Toda transferencia de fondos por medios electrónicos, estará sustentada en documentos que aseguren su validez y confiabilidad.

La utilización de medios electrónicos para las transferencias de fondos entre entidades agiliza la gestión financiera gubernamental. Si bien los mecanismos electrónicos dinamizan la administración de las transacciones financieras por la velocidad que imprimen, no generan documentación inmediata que sustente la validez, propiedad y corrección de cada operación; aspectos que limitan la aplicación de controles internos convencionales.

Es importante implementar controles adecuados a esta forma de operar, enfatizando los mecanismos de seguridad en el uso de claves, cuyo acceso será restringido y permitido solamente a las personas autorizadas. Nadie más conocerá la serie completa de claves utilizadas en una entidad.

Las cartas de confirmación que requieren las transacciones efectuadas mediante el sistema de transferencia electrónica de fondos serán verificadas y validadas por el signatario de las claves respectivas.

Cuando existen sistemas interconectados es posible que se obtengan reportes automáticos diarios, que constituirán uno de los elementos de evidencia inmediata de la transacción, que muestre los movimientos de las cuentas de salida y de destino de los recursos.

El uso del correo electrónico u otras formas de comunicación tecnológica es otro medio que permite contar de inmediato con documentos que sustenten la naturaleza y detalles de las operaciones, cuyo respaldo formal estará sujeto a la obtención de los documentos originales.

Por efectos de seguridad las entidades mantendrán archivos electrónicos y/o físicos.

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------



#### **410-14 Sitio web, servicios de internet e intranet**

Es responsabilidad de la unidad de tecnología de información elaborar las normas, procedimientos e instructivos de instalación, configuración y utilización de los servicios de internet, intranet, correo electrónico y sitio WEB de la entidad, a base de las disposiciones legales y normativas y los requerimientos de los usuarios externos e internos.

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------

#### 5.9.4. PROCEDIMIENTO DEL SUBPROCESO DE ADMINISTRACIÓN DE CORREO

#	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	DOCUMENTO GENERADO
1	Analizar requerimiento y asignarlo	Realiza el análisis del requerimiento y asignarlo a quien corresponda ejecutarlo	Director de tecnologías de la información	Correo electrónico
2	Solicitar ejecución de requerimiento	Realiza una solicitud de ejecución del requerimiento	Responsable de Infraestructura de Tecnologías de la Información	Correo electrónico
3	Verificar requerimiento y ejecutarlo	Realiza la verificación del requerimiento para analizarlo y poderlo ejecutar	Analista de Infraestructura de Tecnologías de la Información	N/A
	Decisión	<b>¿Creación, eliminación, modificación de buzón o modificar las reglas de transporte?</b> <b>Creación o modificación:</b> Realiza la actividad 4. Crear o modificar buzón. <b>Eliminación:</b> Realiza la actividad 7. Eliminar buzón. <b>Modificar las reglas de transporte:</b> Pasa a la actividad 8. Crear o modificar reglas de transporte. <b>Requiere realizar seguimiento a correo:</b> Pasa a la actividad 10. Realizar seguimiento.	Analista de Infraestructura de Tecnologías de la Información	N/A
4	Crear o modificar buzón	<b>Creación:</b> Realiza la creación o modificación del buzón según análisis realizado, y genera un correo electrónico informando sobre la creación del usuario.	Analista de Infraestructura de Tecnologías de la Información	Correo electrónico
5	Configurar buzón	Realiza la configuración del buzón según análisis realizado	Analista de Infraestructura de Tecnologías de la Información	Registro de buzones configurados
6	Elaborar información de respuesta al requerimiento a responsable de la unidad y al Director.	Elabora la información de repuesta al requerimiento de usuario o unidad ejecutor que haya requerido	Analista de Infraestructura de Tecnologías de la Información	Respuesta de correo electrónico
7	Eliminar buzón.	<b>Eliminación:</b> Realiza la eliminación del buzón según análisis efectuado.	Analista de Infraestructura de Tecnologías de la Información	N/A
8	Crear o modificar reglas de transporte	<b>Modificación de reglas de transporte:</b> Realiza la creación o modificación de las reglas de transporte informático en el sistema.	Analista de Infraestructura de Tecnologías de la Información	N/A

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------





**INSTITUTO NACIONAL DE ESTADÍSTICA Y CENSOS**  
**MANUAL DE PROCESOS Y PROCEDIMIENTOS DE LA**  
**DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y**  
**COMUNICACIÓN**

Versión: 2.0  
Código: DITIC-MPP-01  
Página: 85-171

9	Configurar reglas de transporte.	Realiza la configuración de las reglas de transporte informática	Analista de Infraestructura de Tecnologías de la Información	N/A
10	Realizar seguimiento de mensajes.	<b>Seguimiento a correo:</b> Realiza el seguimiento de los mensajes para verificar su estatus.	Analista de Infraestructura de Tecnologías de la Información	N/A
11	Generar respuesta a las solicitudes presentadas	Genera la respuesta a los requerimientos solicitados.	Analista de Infraestructura de Tecnologías de la Información	Correo electrónico
12	Monitorear y administrar sistema	Realiza el monitoreo y administración del sistema de manera diaria	Analista de Infraestructura de Tecnologías de la Información	N/A
	Decisión	<b>¿Réplica o Postmaster?</b> <b>Réplica:</b> Continúa con la decisión. <b>¿Está bien el servicio?</b> <b>Postmaster:</b> Realiza la actividad <b>17</b> . Revisar mensajes de correo.	Analista de Infraestructura de Tecnologías de la Información	N/A
	Decisión	<b>¿Está bien el servicio?</b> <b>NO,</b> Analizar problema, pasa a la actividad <b>14</b> <b>SI:</b> Realiza la actividad <b>13</b> . Continuar monitoreando.	Analista de Infraestructura de Tecnologías de la Información	N/A
13	Continuar monitoreando	Realiza el continuo monitoreo para verificación del estatus del sistema. Regresa a la actividad <b>12</b> .	Analista de Infraestructura de Tecnologías de la Información	N/A
14	Analizar problema	Realiza el análisis de los problemas detectados	Analista de Infraestructura de Tecnologías de la Información	N/A
15	Solucionar problema	Realiza la solución a los problemas identificados, revisando el daño en el plan de contingencia.	Analista de Infraestructura de Tecnologías de la Información	N/A
16	Subir servicios	Realiza la carga de los servicios al sistema. <b>Fin del proceso.</b>	Analista de Infraestructura de Tecnologías de la Información	N/A
17	Generar informe de novedades	Genera informe de novedades y lo remite a la responsable de la unidad para su revisión	Analista de Infraestructura de Tecnologías de la Información	Informe de novedades
18	Revisar informe de novedades	Revisa el informe de novedades y procede a archivarlo.	Responsable de Infraestructura de	N/A

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------

			Tecnologías de la Información	
	Decisión	<b>¿Está bien?</b> <b>NO:</b> Regresa a la actividad <b>17</b> . Generar informe. <b>SI:</b> Continúa con la decisión. <b>¿Es programado?</b>	Responsable de Infraestructura de Tecnologías de la Información	N/A
19	Revisar mensajes de correo	Realiza la revisión de los mensajes de correo	Analista de Infraestructura de Tecnologías de la Información	N/A
20	Eliminar mensajes de correo, fin	Realiza la eliminación de los mensajes del correo electrónico institucional	Analista de Infraestructura de Tecnologías de la Información	N/A
21	Reenviar mensajes de correo, fin	Realiza el reenvío de los mensajes del correo electrónico	Analista de Infraestructura de Tecnologías de la Información	N/A
	Decisión	<b>¿Es programado?</b> <b>NO:</b> Termina el proceso. <b>SI:</b> Realiza la actividad <b>22</b> . Respalda configuraciones.	Analista de Infraestructura de Tecnologías de la Información	N/A
22	Inicio programado, Respalda configuraciones, base de datos y logs del servidor del correo electrónico	Realiza los respaldos de las configuraciones en base a datos y Logs del servidor del correo electrónico	Analista de Infraestructura de Tecnologías de la Información	N/A
23	Subproceso, Respaldos de información, fin	Realiza los respaldos de información informática (Subproceso)	Analista de Infraestructura de Tecnologías de la Información	N/A

#### 5.9.5. INDICADORES DEL SUBPROCESO DE ADMINISTRACIÓN DE CORREO

N°	Indicador	Fórmula de Cálculo	Unidad de Medida	Responsable de Medición	Fuente de Medición	Frecuencia de Medición
1	Porcentaje de disponibilidad de correo electrónico	$((\text{Tiempo total sondeo} - \text{tiempo no disponible}) / \text{tiempo total de sondeo}) * 100\%$	%	Responsable de infraestructura	Reporte de software Whatsup	Trimestral

#### 5.9.6. FORMATOS DEL SUBPROCESO DE ADMINISTRACIÓN DE CORREO

Nombre del Registro de Calidad	Código de Formato
N/A	N/A

#### 5.9.7. ANEXOS DEL SUBPROCESO DE ADMINISTRACIÓN DE CORREO

“No hay anexos.”

Elaborado por: PC	Revisado por: DIPLA - DIFI	Aprobado /Autorizado por: DIREJ	Registrado por: DIPLA, PC
----------------------	-------------------------------	------------------------------------	------------------------------

## 5.10. SUBPROCESO DE ADMINISTRACIÓN DE SERVICIOS DE SEGURIDAD

### 5.10.1. FICHA TÉCNICA DEL SUBPROCESO DE ADMINISTRACIÓN DE SERVICIOS DE SEGURIDAD

<b>Proceso:</b>	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN
<b>Nombre del Subproceso:</b>	ADMINISTRACIÓN DE SERVICIOS DE SEGURIDAD
<b>Código del Subproceso:</b>	DITIC-TI-SP10
<b>Descripción:</b>	<p><b>PROPÓSITO:</b> Asegurar y garantizar una adecuada protección de los servicios como de la información en los procesos acceso a través de Internet, Datos y correo electrónico.</p> <p><b>ALCANCE:</b> Desde solicitar permisos de navegación, hasta enviar notificación a requirente.</p> <p><b>DISPARADOR:</b></p> <ul style="list-style-type: none"> <li>• Correos, memorandos y sistema GLPI</li> </ul> <p><b>PROVEEDORES:</b></p> <ul style="list-style-type: none"> <li>• Procesos adjetivos y sustantivos del INEC</li> </ul> <p><b>INSUMOS:</b></p> <ul style="list-style-type: none"> <li>• Correos</li> <li>• Memorandos</li> <li>• Tickets de atención al usuario del GLPI</li> </ul>
<b>Clientes:</b>	<ul style="list-style-type: none"> <li>• Direcciones del INEC.</li> </ul>
<b>Salidas:</b>	<ul style="list-style-type: none"> <li>• Informe de vulnerabilidades encontradas y bloqueadas.</li> </ul>
<b>Tipo de Proceso:</b>	<ul style="list-style-type: none"> <li>• Adjetivo de asesoría.</li> </ul>
<b>Responsable del Proceso:</b>	Jefe de Gestión de Infraestructura de Tecnologías de la Información.
<b>Recursos:</b>	<p><b>MATERIALES:</b></p> <ul style="list-style-type: none"> <li>• Equipo de computación</li> <li>• Equipo y materiales de oficina.</li> </ul> <p><b>HUMANOS:</b></p> <ul style="list-style-type: none"> <li>• 2 analistas de Gestión de Infraestructura de TI SP7.</li> <li>• 4 analistas de Gestión de Infraestructura de TI SP5.</li> <li>• 1 analista de Gestión de Infraestructura de TI SP1.</li> </ul> <p><b>TECNOLÓGICOS:</b></p> <ul style="list-style-type: none"> <li>• Correo Electrónico.</li> <li>• Software Ofimática.</li> <li>• Acceso a internet.</li> </ul>

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------



	<ul style="list-style-type: none"><li>Herramientas para soporte en redes.</li></ul>
<b>Controles/Marco Legal:</b>	<ul style="list-style-type: none"><li>Resolución 030- DIREJ-DIJU-NI2012</li></ul>

## 5.10.2. CONTROLES DEL SUBPROCESO DE ADMINISTRACIÓN DE SERVICIOS DE SEGURIDAD

### Resolución 030- DIREJ-DIJU-NI2012

Uso de Los servicios Tecnológicos y Políticas de la Dirección de Tecnologías de la Información y Comunicación del Instituto Nacional de Estadística Y Censos

- Normativa de Seguridad de La información
- Norma Comunicaciones

#### 1. Objetivo

Definir las reglas generales para establecer una adecuada protección de la información en los procesos de transmisión y recepción de datos en las redes internas y externas del INEC.

#### 2. Serán Responsables:

Todo el personal del área de DITIC del INEC y los terceros que interactúan de manera habitual u ocasional que estén vinculados a los procesos de transmisión de datos en el desarrollo de sus tareas habituales.

#### 3. Incumplimientos

Las medidas disciplinarias serán aplicadas según resolución publicada, la normativa interna y las que determinaren las entidades de control del estado ecuatoriano.

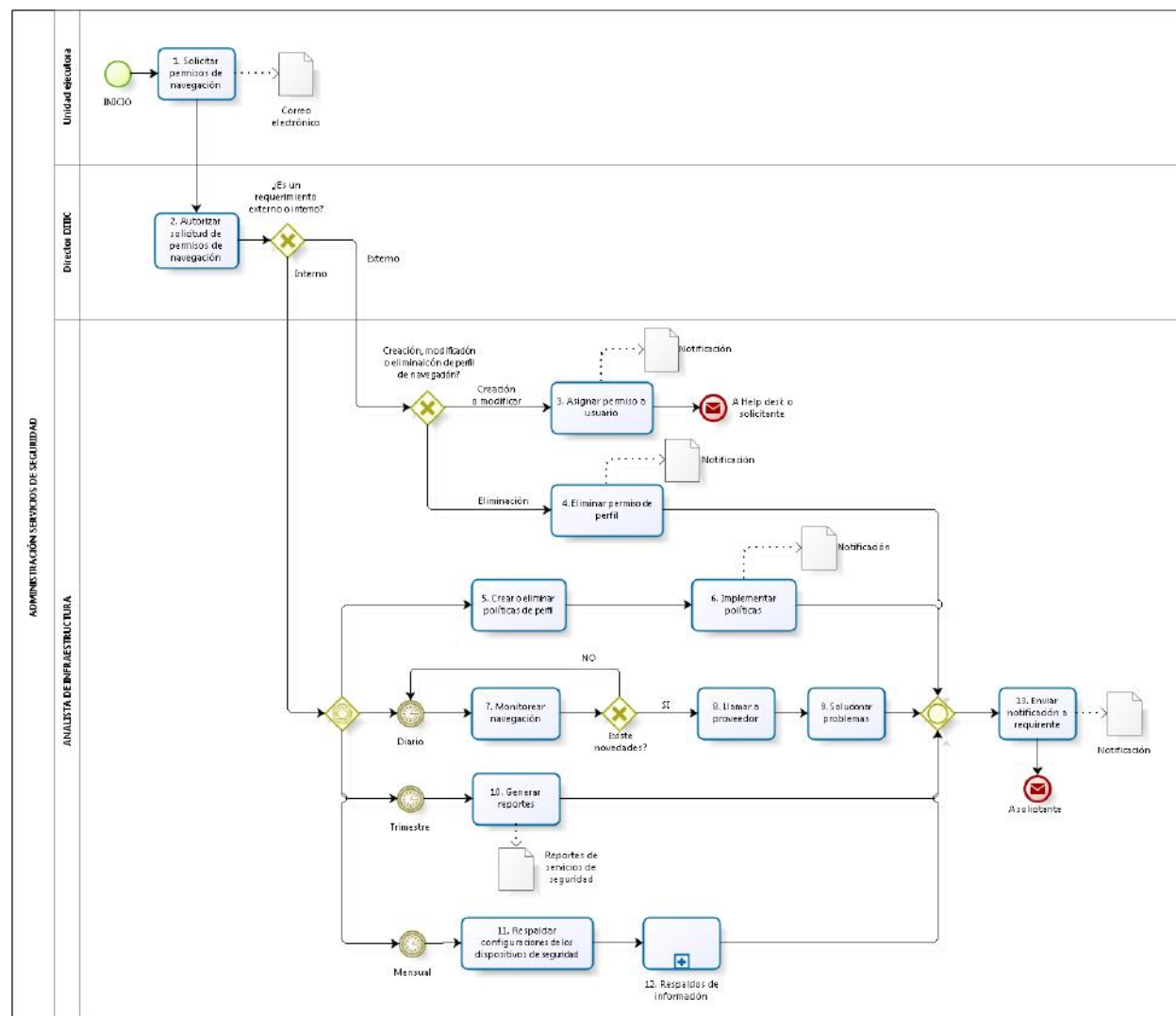
#### 4. Definiciones, conexiones internas:

Adicionalmente a las medidas de protección física y de acceso de usuarios ya definidas en las respectivas normas, se deben tener en cuenta las siguientes consideraciones adicionales:

- Utilizar switches, no sólo para conectar los distintos segmentos de la red interna, sino también para conectar las distintas estaciones de trabajo y servidores entre sí.
- Verificar que existan los adecuados mecanismos de encriptación para la información sensible propia de los sistemas (contraseñas, bases de datos de seguridad o similares).
- Documentar y utilizar un estándar de direccionamiento IP teniendo en cuenta las direcciones privadas definidas en normas internacionales para evitar que éstas sean accesibles desde el exterior.
- Utilizar sistemas de detección de intrusos que permitan la detección de posibles ataques y tomen acciones automáticas para prevenirlos.

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------

### 5.10.3. DIAGRAMA DE FLUJO DEL SUBPROCESO DE ADMINISTRACIÓN DE SERVICIOS DE SEGURIDAD



Elaborado por:  
PC

Revisado por:  
DIPLA - DIFI

Aprobado /Autorizado por:  
DIREJ

Registrado por:  
DIPLA, PC

#### 5.10.4. PROCEDIMIENTO DEL SUBPROCESO DE ADMINISTRACIÓN DE SERVICIOS DE SEGURIDAD

Nº	Actividad	Detalle de la actividad	Responsable	Documento Generado
1	Solicitar permisos de navegación	Realiza el requerimiento de permisos de navegación mediante memorando o correo electrónico	Unidad ejecutora	Correo electrónico
2	Autorizar solicitud de permisos de navegación	Analiza y reasigna la solicitud de permisos de navegación	Director DITIC	N/A
	Decisión	<b>¿Es un requerimiento externo o interno?</b> <b>Externo:</b> Continúa con la decisión. <b>¿Creación, modificación o eliminación de perfil de navegación?</b> <b>NO:</b>	Director DITIC	N/A
	Decisión	<b>¿Creación, modificación o eliminación de perfil de navegación?</b> <b>Creación o modificar:</b> Asignar permiso a usuario <b>1</b> <b>Eliminación de perfil de navegación:</b> Eliminar permiso de perfil <b>2</b>	Analista de infraestructura	N/A
3	Asignar permiso a usuario, fin	Realiza la asignación del permiso al usuario para su respectivo uso. <b>Fin del proceso.</b>	Analista de infraestructura	Notificación
4	Eliminar permiso de perfil	Realiza la eliminación del permiso del perfil	Analista de infraestructura	Notificación
5	Crear o eliminar políticas de perfil	Realiza la creación o eliminación de las políticas del perfil	Analista de infraestructura	N/A
6	Implementar políticas	Ejecuta las políticas de administración de servicios de seguridad	Analista de infraestructura	N/A
7	Monitorear navegación	<b>Diario:</b> Realiza el monitoreo de navegación con una frecuencia diaria	Analista de infraestructura	N/A
	Decisión	<b>¿Existe novedades?</b> <b>NO:</b> Monitorear navegación, pasa a la actividad 5 <b>SI:</b> Comunicar con proveedor, pasa a la actividad 6	Analista de infraestructura	N/A
8	Comunicar con proveedor	Realiza la comunicación con el proveedor en caso de problemas que no se solucionen dentro de la institución	Analista de infraestructura	N/A
9	Solucionar problemas	Realiza la solución de los problemas según el análisis que se hizo al equipo informático	Analista de infraestructura	N/A
10	Generar reportes trimestrales	<b>Trimestralmente:</b> Realiza la generación de los reportes trimestralmente para dar a conocer la	Analista de infraestructura	Reportes de servicios de seguridad

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------

		gestión realizada		
11	Respaldo configuraciones de los dispositivos de seguridad	<b>Mensualmente:</b> Realiza el respaldo de las configuraciones de los dispositivos de seguridad	Analista de infraestructura	N/A
12	Subproceso, Respaldos de información, fin	Realiza los respaldos de la información (subproceso)	Analista de infraestructura	N/A
13	Enviar notificación a requirente	Realiza el envío de la notificación al usuario o unidad requirente	Analista de infraestructura	Notificación

#### 5.10.5. INDICADORES DEL SUBPROCESO DE ADMINISTRACIÓN DE SERVICIOS DE SEGURIDAD

N°	Indicador	Fórmula de Cálculo	Unidad de Medida	Responsable de Medición	Fuente de Medición	Frecuencia de Medición
1	Porcentaje de cumplimiento de servicios de seguridad	(# de vulnerabilidades bloqueadas/# de vulnerabilidades detectadas) *100%	Porcentaje	Responsable de Gestión de Infraestructura	GLPI	Trimestral

#### 5.10.6. FORMATOS DEL SUBPROCESO DE ADMINISTRACIÓN DE SERVICIOS DE SEGURIDAD

Nombre del Registro de Calidad	Código de Formato
N/A	N/A

#### 5.10.7. ANEXOS DEL SUBPROCESO DE ADMINISTRACIÓN DE SERVICIOS DE SEGURIDAD

“No hay anexos.”

Elaborado por: PC	Revisado por: DIPLA - DIFI	Aprobado /Autorizado por: DIREJ	Registrado por: DIPLA, PC
----------------------	-------------------------------	------------------------------------	------------------------------

## 5.11. SUBPROCESO DE ADMINISTRACIÓN DE CONFIGURACIÓN DE USUARIOS

### 5.11.1. FICHA TÉCNICA DEL SUBPROCESO DE ADMINISTRACIÓN DE CONFIGURACIÓN DE USUARIOS

<b>Proceso:</b>	GESTIÓN DE INFRAESTRUCTURA DE TECNOLOGÍAS DE LA INFORMACIÓN		
<b>Nombre del Subproceso:</b>	ADMINISTRACIÓN DE CONFIGURACIÓN DE USUARIOS		
<b>Código del Subproceso:</b>	DITIC-IT-SP11		
<b>Descripción:</b>	<p><b>PROPÓSITO:</b> Establecer el procedimiento requerido para atender las peticiones de configuración de nuevas cuentas de usuarios y así enmarcar las acciones para la correcta administración de las cuentas ya creadas.</p> <p><b>ALCANCE:</b> Desde realizar la creación, modificación o eliminación del usuario, hasta realizar los respaldos de información.</p> <p><b>DISPARADOR:</b></p> <ul style="list-style-type: none"> <li>• Correo electrónico.</li> </ul> <p><b>PROVEEDORES:</b></p> <ul style="list-style-type: none"> <li>• Dirección de Administración de Recursos Humano.</li> <li>• Gestión de Soporte a Usuarios.</li> </ul> <p><b>INSUMOS:</b></p> <ul style="list-style-type: none"> <li>• Correo electrónico.</li> <li>• Matriz de información requerida para nuevo usuario.</li> </ul>		
<b>Clientes:</b>	<ul style="list-style-type: none"> <li>• Dirección de Tecnologías de la Información y Comunicación.</li> </ul>		
<b>Salidas:</b>	<ul style="list-style-type: none"> <li>• Informe técnico de configuración de usuarios.</li> </ul>		
<b>Tipo de Proceso:</b>	<ul style="list-style-type: none"> <li>• Adjetivo de Asesoría.</li> </ul>		
<b>Responsable del Proceso:</b>	Responsable de la Unidad de Gestión de Infraestructura de TI		
<b>Recursos:</b>	<p><b>MATERIALES:</b></p> <ul style="list-style-type: none"> <li>• Equipo de computación</li> <li>• Equipo y materiales de oficina.</li> </ul> <p><b>HUMANOS:</b></p> <ul style="list-style-type: none"> <li>• 2 analistas de Gestión de Infraestructura de TI SP5.</li> <li>• 1 analista de Gestión de Infraestructura de TI SP7.</li> </ul> <p><b>TECNOLÓGICOS:</b></p> <ul style="list-style-type: none"> <li>• Servidor de Usuarios.</li> <li>• Software Ofimática.</li> </ul>		
<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC



**Controles/Marco Legal:**

- Norma de Administración de Usuarios de TIC's, Versión 1.0
- Acuerdo 166 EGSI, sección 7.2, literal a, párrafos 3,4,5,6
- Acuerdo 166 EGSI, sección 7.4, literal a
- Acuerdo 166 EGSI, sección 7.6, literales a, b, c, d
- Acuerdo 166 EGSI, sección 7.7, literal a
- Acuerdo 166 EGSI, sección 7.8, literales a, c, g, i
- Acuerdo 166 EGSI, sección 7.16, literales a, d, e

### 5.11.2. CONTROLES DEL SUBPROCESO DE ADMINISTRACIÓN DE CONFIGURACIÓN DE USUARIOS

**Norma de administración de usuarios de TIC's, versión 1.0**

**Consideraciones generales**

- Alta de un perfil de usuario: cuando el mismo ingresa al INEC en modalidad de nombramiento, contrato o consultaría.
- Modificación de un perfil de usuario: cuando el mismo requiere nuevos permisos de acceso al recurso informático.
- Baja de un perfil de usuario: cuando el mismo deja de pertenecer a la Institución o se termina un contrato o consultaría especializada.

**Principios generales**

- Los usuarios sólo, no deben tener permisos de accesos a ningún recurso excepto para aquellos que estén debidamente autorizados.
- Los accesos deben seguir el principio de "camino forzoso" permitiendo al usuario acceder exclusivamente a los recursos para los cuales tiene permiso sin acceder por la misma vía a otros recursos.

**Compromiso del usuario**

- Todo usuario debe firmar un compromiso de responsabilidad y confidencialidad del uso de su cuenta de usuario, de la respectiva contraseña asignada y de la información de los sistemas informáticos a los que acceda. Este compromiso debe ser renovado anualmente.

**Restricciones adicionales**

- Restringir la cuenta de usuario a una sola sesión de trabajo, siempre y cuando se dispongan de las herramientas automáticas para realizarlo. Las excepciones deberán ser aprobadas por el Jefe de Administración de Servicios Tecnológicos.
- Restringir el uso de la cuenta de usuario a determinados días y horas, siempre y cuando se dispongan de las herramientas automáticas para realizarlo.

**Pantalla de inicio de acceso a los sistemas del INEC**

- Se debe implementar de manera automática en el sistema un mensaje al momento de ingresar el usuario a los sistemas.
- El mensaje debe manifestar que el sistema sólo puede ser utilizado para los propósitos autorizados para sus tareas y que el usuario tiene el compromiso de responsabilidad y confidencialidad de su cuenta de usuario asignada y de la información a la que accede.

**Desconexión**

- Se debe desconectar o bloquear toda sesión activa cuando la estación de trabajo no verifique uso durante 30 minutos, siempre y cuando se dispongan de las herramientas automáticas para hacerlo.

**Protector de Pantalla**

- Se deberá utilizar las facilidades de protector de pantalla con contraseña para las estaciones de trabajo, con activación automática a los 15 minutos de inactividad en el sistema, siempre y cuando se dispongan de las herramientas automáticas para hacerlo.

<b>Elaborado por:</b>	<b>Revisado por:</b>	<b>Aprobado /Autorizado por:</b>	<b>Registrado por:</b>
PC	DIPLA - DIFI	DIREJ	DIPLA, PC

Acuerdo 166 de la secretaria de la administración pública esquema gubernamental de la seguridad de la información (EGSI)

Sección 7.2, literal a, párrafos 3, 4, 5, 6

- Crear los accesos para los usuarios, para lo cual la institución debe generar convenios de confidencialidad y responsabilidad con el usuario solicitante; además, validar que el usuario tenga los documentos de ingreso con Recursos Humanos (o quien haga estas funciones) en orden y completos.
- Modificar los accesos de los usuarios;
- Eliminar los accesos de los usuarios;
- Suspender temporalmente los accesos de los usuarios en caso de vacaciones, comisiones, licencias, es decir, permisos temporales;

Sección 7.4, literal a

- a) Establecer un proceso formal para la asignación cambio de contraseñas

Sección 7.6, literales a, b, c, d

- a) Documentar, en el procedimiento de accesos, las responsabilidades de los usuarios tanto internos como externos, sobre el uso de la cuenta y la contraseña asignadas.
- b) Recomendar la generación de contraseñas con letras mayúsculas, minúsculas, con caracteres especiales, difíciles de descifrar, es decir, que cumplen una complejidad media y alta.
- c) Evitar contraseñas en blanco o que viene por defecto según el sistema el fabricante del producto, puesto que son fácilmente descifrables; por ejemplo: admin, administrador, administrador, user, usuario, entre otros.
- d) Controlar el cambio periódico de contraseñas de los usuarios.

Sección 7.7, literal a

- a) Implementar medidas para que, en un determinado tiempo (ej., no mayor a 10 minutos) si el usuario no está realizando ningún trabajo en el equipo, este se bloquee, y se desbloquee únicamente si el usuario ingresa nuevamente su clave.

Sección 7.8, literales a, c, g, i

- a) El Oficial de Seguridad de la Información deberá gestionar actividades periódicas (una vez cada mes como mínimo) para la revisión al contenido de las pantallas de los equipos, con el fin de que no se encuentren iconos y accesos innecesarios, y carpetas y archivos que deben ubicarse en la carpeta de documentos del usuario.
- c) Desconectar de la red, servicio o sistema, las computadoras personales, terminales, impresoras asignadas a funciones críticas, cuando se encuentren desatendidas. Por ejemplo, haciendo uso de protectores de pantalla con clave.
- g) Retirar información sensible, como las claves, de sus escritorios y pantallas.
- i) Cifrar los discos duros de los computadores personales (escritorio, portátiles, etc.) y otros dispositivos que se considere necesarios, de las máximas autoridades de la institución.

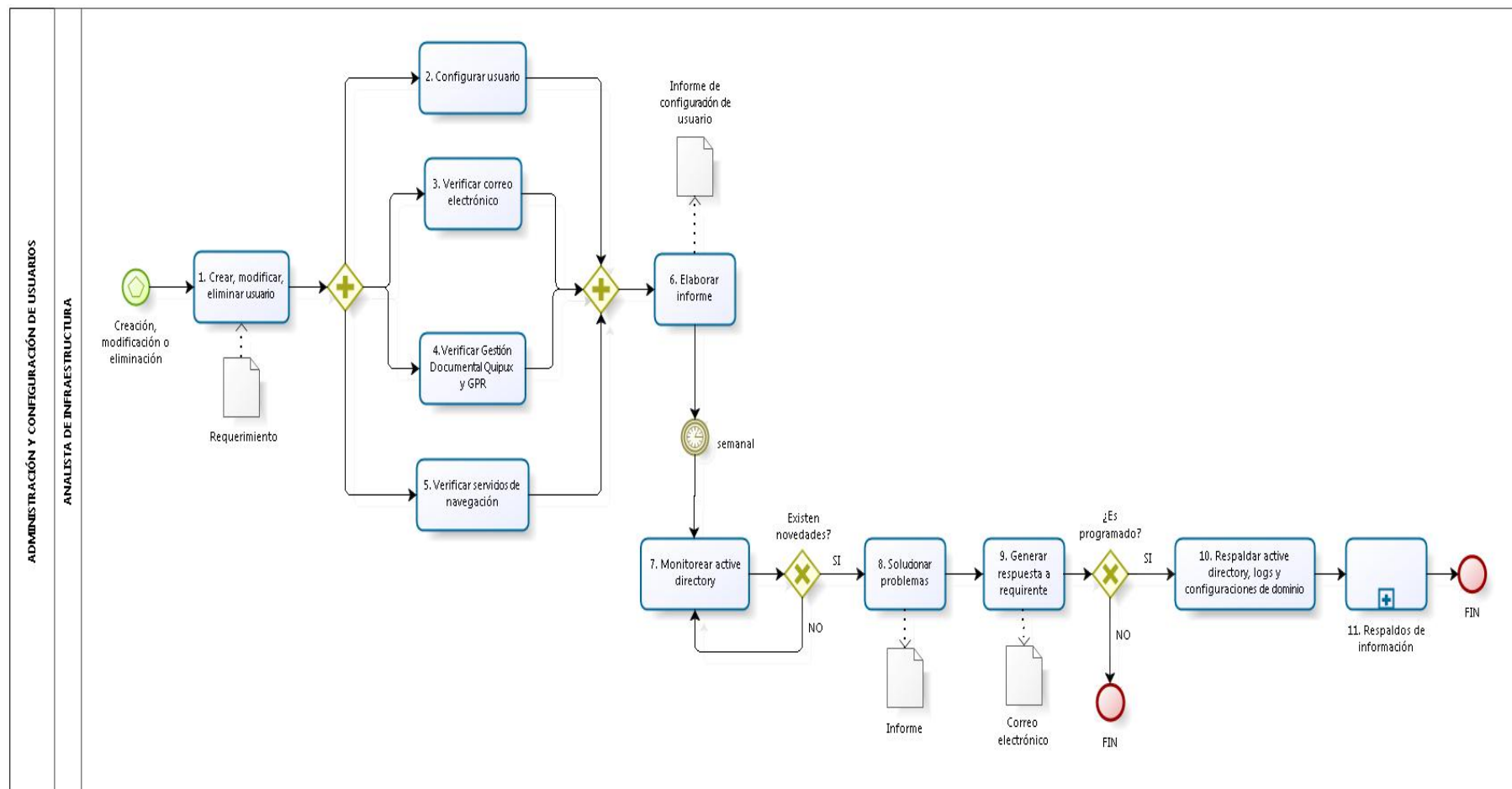
Sección 7.16, literal a, d, e

- a) Autenticar usuarios autorizados, de acuerdo a la política de control de acceso de la institución, que deberá estar documentada, definida y socializada
- d) Utilizar mecanismos como: uso de dominios de autenticación, servidores de control de acceso y directorios.

Restringir el tiempo de conexión de los usuarios, considerando las necesidades de la institución.

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------

### 5.11.3. DIAGRAMA DE FLUJO DEL SUBPROCESO DE ADMINISTRACIÓN DE CONFIGURACIÓN DE USUARIOS



**Elaborado por:**  
PC

**Revisado por:**  
DIPLA - DIFI

**Aprobado /Autorizado por:**  
DIREJ

**Registrado por:**  
DIPLA, PC

#### 5.11.4. PROCEDIMIENTO DEL SUBPROCESO DE ADMINISTRACIÓN DE CONFIGURACIÓN DE USUARIOS

N	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	DOCUMENTO GENERADO
1	Crear modificar eliminar usuario	Realiza la creación, modificación o eliminación del usuario	Analista de infraestructura	Requerimiento
2	Configurar usuario	Realiza la configuración del usuario según el requerimiento	Analista de infraestructura	N/A
3	Verificar correo electrónico	Realiza la verificación del correo electrónico	Analista de infraestructura	N/A
4	Verificar Gestión Documental Quipux y GPR	Realiza la verificación de la gestión documental Quipux y la Gestión por Resultados	Analista de infraestructura	N/A
5	Verificar servicios de navegación	Realiza la verificación de los servicios de navegación de los equipos informáticos	Analista de infraestructura	N/A
6	Elaborar informe	Realiza la elaboración del informe de la configuración del usuario según requerimiento	Analista de infraestructura	Informe de configuración de usuario
7	Monitorear active directory (semanalmente)	Realiza el monitoreo del active directory con frecuencia semanal	Analista de infraestructura	N/A
	Decisión	<b>¿Existen novedades?</b> <b>NO:</b> Regresa a la actividad 7. Monitorear active directory. <b>SI:</b> Realiza la actividad 8. Solucionar problemas	Analista de infraestructura	N/A
8	Solucionar problemas, fin	Realiza la solución de los problemas según los requerimientos	Analista de infraestructura	Informe
9	Generar respuesta a requirente	Generar respuesta a requirente informando que se atendió el requerimiento.	Analista de infraestructura	Correo electrónico
10	Inicio 2 programado, Respaldo active directory, logs y configuraciones de dominio	Realiza la programación de los respaldos de active directory logs y de las configuraciones de dominio.	Analista de infraestructura	N/A
11	Subproceso, Respaldo de información, fin	Realiza los respaldos de la información según estipula el proceso.	Analista de infraestructura	Ticket de respaldo

#### 5.11.5. INDICADORES DEL SUBPROCESO DE ADMINISTRACIÓN DE CONFIGURACIÓN DE USUARIOS

N°	Indicador	Fórmula de Cálculo	Unidad de Medida	Responsable de Medición	Fuente de Medición	Frecuencia de Medición
1	Porcentaje de cumplimiento en la configuración a usuarios	$(\# \text{ de peticiones atendidas} / \# \text{ de peticiones solicitadas}) * 100\%$	%	Responsable de infraestructura	Informe técnico de ejecución	Trimestral

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------

#### 5.11.6. FORMATOS DEL SUBPROCESO DE ADMINISTRACIÓN DE CONFIGURACIÓN DE USUARIOS

Nombre del Registro de Calidad	Código de Formato
N/A	N/A

#### 5.11.7. ANEXOS DEL SUBPROCESO DE ADMINISTRACIÓN DE CONFIGURACIÓN DE USUARIOS

“No hay anexos.”

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------

## 5.12. SUBPROCESO DE ADMINISTRACIÓN DE CONEXIÓN REMOTA

### 5.12.1. FICHA TÉCNICA DEL SUBPROCESO DE ADMINISTRACIÓN DE CONEXIÓN REMOTA

<b>Proceso:</b>	GESTIÓN DE INFRAESTRUCTURA DE TECNOLOGÍAS DE LA INFORMACIÓN
<b>Nombre del Subproceso:</b>	ADMINISTRACIÓN DE CONEXIÓN REMOTA
<b>Código del Subproceso:</b>	DITIC-IT-SP12
<b>Descripción:</b>	<p><b>PROPÓSITO:</b></p> <ul style="list-style-type: none"> <li>Asegurar y garantizar una adecuada protección de los servicios de conexión remota.</li> </ul> <p><b>ALCANCE:</b> Desde analizar el requerimiento, hasta dar mantenimiento preventivo a la herramienta.</p> <p><b>DISPARADOR:</b></p> <ul style="list-style-type: none"> <li>Memorando, correo electrónico.</li> </ul> <p><b>PROVEEDORES:</b></p> <ul style="list-style-type: none"> <li>Unidades del INEC.</li> </ul> <p><b>INSUMOS:</b></p> <ul style="list-style-type: none"> <li>Correo electrónico.</li> <li>Autorización por Director de DITIC.</li> </ul>
<b>Clientes:</b>	<ul style="list-style-type: none"> <li>Unidades del INEC.</li> </ul>
<b>Salidas:</b>	<ul style="list-style-type: none"> <li>Correo electrónico.</li> </ul>
<b>Tipo de Proceso:</b>	<ul style="list-style-type: none"> <li>Adjetivo de Asesoría.</li> </ul>
<b>Responsable del Proceso:</b>	Responsable de la Unidad de Gestión de Infraestructura de TI
<b>Recursos:</b>	<p><b>MATERIALES:</b></p> <ul style="list-style-type: none"> <li>Equipo de computación</li> <li>Equipo y materiales de oficina.</li> </ul> <p><b>HUMANOS:</b></p> <ul style="list-style-type: none"> <li>2 analistas de Gestión de Infraestructura de TI SP5.</li> <li>2 analistas de Gestión de Infraestructura de TI SP7.</li> </ul> <p><b>TECNOLÓGICOS:</b></p> <ul style="list-style-type: none"> <li>Software Ofimática.</li> <li>Servidor de conexión remota.</li> </ul>

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------

**Controles/Marco Legal:**

- Resolución 030-DIREJ-DIJU-NI2012 uso de los servicios tecnológicos y políticas de la dirección de tecnologías de la información y comunicación del instituto nacional de estadística y censos
- Normativa de seguridad de la información
- Norma comunicaciones
- Norma correo electrónico y uso del internet
- Normas de control interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos- de la contraloría
- 410 norma de tecnología de la información
- 410-10 seguridad de tecnología de información
- 410-12 administración de soporte de tecnología de información
- 410-13 monitoreo y evaluación de los procesos y servicios
- Acuerdo 166 de la secretaria de la administración pública esquema gubernamental de la seguridad de la información (EGSI)
- Política de seguridad de la información
- Organización de la seguridad de la información
- Gestión de los activos
- Seguridad de los recursos humanos
- Seguridad física y del entorno
- Gestión de comunicaciones y operaciones
- Control de acceso
- Adquisición, desarrollo y mantenimiento de sistemas de información
- Gestión de los incidentes de la seguridad de la información
- Gestión de la continuidad del negocio
- Cumplimiento

### 5.12.2. CONTROLES DEL SUBPROCESO DE ADMINISTRACIÓN DE CONEXIÓN REMOTA

Resolución 030- direj-diju-ni2012 uso de los servicios tecnológicos y políticas de la dirección de tecnologías de la información y comunicación del instituto nacional de estadística y censos

- Normativa de Seguridad de La información
- Norma Comunicaciones

1. Objetivo.- definir las reglas generales para establecer una adecuada protección de la información en los procesos de transmisión y recepción de datos en las redes internas y externas del INEC.

2. Serán Responsables: todo el personal del área de DITIC del INEC y los terceros que interactúan de manera habitual u ocasional que estén vinculados a los procesos de transmisión de datos en el desarrollo de sus tareas habituales.

3. Incumplimientos.- las medidas disciplinarias serán aplicadas según resolución publicada, la normativa interna y las que determinaren las entidades de control del estado ecuatoriano.

4. Definiciones, conexiones internas

Adicionalmente a las medidas de protección física y de acceso de usuarios ya definidas en las respectivas normas, se deben tener en cuenta las siguientes consideraciones adicionales:

- Utilizar switches, no sólo para conectar los distintos segmentos de la red interna, sino también para conectar las distintas estaciones de trabajo y servidores entre sí.

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------

- Verificar que existan los adecuados mecanismos de encriptación para la información sensible propia de los sistemas (contraseñas, bases de datos de seguridad o similares).
- Documentar y utilizar un estándar de direccionamiento IP teniendo en cuenta las direcciones privadas definidas en normas internacionales para evitar que éstas sean accesibles desde el exterior.

#### Consideraciones generales para el uso del correo electrónico

- El usuario debe tener en cuenta que el correo electrónico debe ser de tipo memorando, por lo que debe plantear adecuadamente el mensaje, en términos de destinatario, asunto y cuerpo del mensaje.

#### Tipos de correos electrónicos

Se deben aplicar las medidas de seguridad para todo el servicio de correo electrónico, que comprende el uso de las cuentas de usuarios de los sistemas para el envío y recepción de mensajes electrónicos en:

- la red interna para usuarios propios del INEC, o
- para otros usuarios a través del uso de internet.

Normas de control interno para las entidades, organismos del sector público y persona jurídica de derecho privado que dispongan de recursos públicos- de la contraloría.

- **410 NORMA DE TECNOLOGIA DE LA INFORMACION**

#### 410-10 Seguridad de tecnología de información

La unidad de tecnología de información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos, para ello se aplicarán al menos las siguientes medidas:

1. Ubicación adecuada y control de acceso físico a la unidad de tecnología de información y en especial a las áreas de: servidores, desarrollo y bibliotecas;
2. Definición de procedimientos de obtención periódica de respaldos en función a un cronograma definido y aprobado;
3. En los casos de actualización de tecnologías de soporte se migrará la información a los medios físicos adecuados y con estándares abiertos para garantizar la perpetuidad de los datos y su recuperación;
4. Almacenamiento de respaldos con información crítica y/o sensible en lugares externos a la organización;
5. Implementación y administración de seguridades a nivel de software y hardware, que se realizará con monitoreo de seguridad, pruebas periódicas y acciones correctivas sobre las vulnerabilidades o incidentes de seguridad identificados.

- **410-12 Administración de soporte de tecnología de información**

La unidad de tecnología de información definirá, aprobará y difundirá procedimientos de operación que faciliten una adecuada administración del soporte tecnológico y garanticen la seguridad, integridad, confiabilidad y disponibilidad de los recursos y datos, tanto como la oportunidad de los servicios tecnológicos que se ofrecen.

Los aspectos a considerar son:

1. Revisiones periódicas para determinar si la capacidad y desempeño actual y futura de los recursos tecnológicos son suficientes para cubrir los niveles de servicio acordados con los usuarios.
2. Seguridad de los sistemas bajo el otorgamiento de una identificación única a todos los usuarios internos, externos y temporales que interactúen con los sistemas y servicios de tecnología de información de la entidad.
3. Estandarización de la identificación, autenticación y autorización de los usuarios, así como la administración de sus cuentas.

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------



- **410-13 Monitoreo y evaluación de los procesos y servicios**

Es necesario establecer un marco de trabajo de monitoreo y definir el alcance, la metodología y el proceso a seguir para monitorear la contribución y el impacto de tecnología de información en la entidad.

La unidad de tecnología de información definirá sobre la base de las operaciones de la entidad, indicadores de desempeño y métricas del proceso para monitorear la gestión y tomar los correctivos que se requieran.

Acuerdo 166 de la secretaria de la administración pública esquema gubernamental de la seguridad de la información (EGSI).

### 3. GESTIÓN DE LOS ACTIVOS

#### 3.3. Uso aceptable de los activos

d) Reglamentar el uso de correo electrónico institucional:

- Este servicio debe utilizarse exclusivamente para las tareas propias de las funciones que se desarrollan en la institución y no debe utilizarse para ningún otro fin.
- Cada persona es responsable tanto del contenido del mensaje enviado como de cualquier otra información que adjunte.
- Todos los mensajes deben poder ser monitoreados y conservados permanentemente por parte de las instituciones.
- Toda cuenta de correo electrónico debe estar asociada a una única cuenta de usuario.
- La conservación de los mensajes se efectuará en carpetas personales, para archivar la información de acceso exclusivo del usuario y que no debe compartirse con otros usuarios.

### 4. Seguridad de los recursos humanos

#### 4.9. Retiro de los privilegios de acceso

a) Retirar los privilegios de acceso a los activos de información y a los servicios de procesamiento de información (ej., sistema de directorio, correo electrónico, accesos físicos, aplicaciones de software, etc.,) inmediatamente luego de que se comunique formalmente al Oficial de Seguridad de la Información formalmente la terminación de la relación laboral por parte del área correspondiente.

### 7. CONTROL DE ACCESO

#### 7.10. Autenticación de usuarios para conexiones Externas

- a) Generar mecanismos para asegurar la información transmitida por los canales de conexión remota, utilizando técnicas como encriptación de datos, implementación de redes privadas virtuales (VPN) y Servicio de Acceso Remoto (SAR).
- b) Realizar un mecanismo diferenciado para la autenticación de los usuarios que requieren conexiones remotas, que permita llevar control de registros (logs) y que tenga limitaciones de accesos en los segmentos de red.

#### 7.26. Trabajo remoto

- a) Las instituciones podrán autorizar la modalidad de trabajo remoto en circunstancias específicas, siempre que en la institución se apliquen las disposiciones de seguridad y los controles establecidos, cumpliendo con la política de seguridad de la información.
- b) El funcionario deberá observar la seguridad física de la edificación y del entorno local existente en el sitio de trabajo remoto.
- c) Deberá evitarse la conexión a redes inalámbricas que no presten la seguridad de acceso y autenticación adecuados.
- d) No se permite el uso de equipo de propiedad privada que no esté bajo el control y monitoreo de la institución .

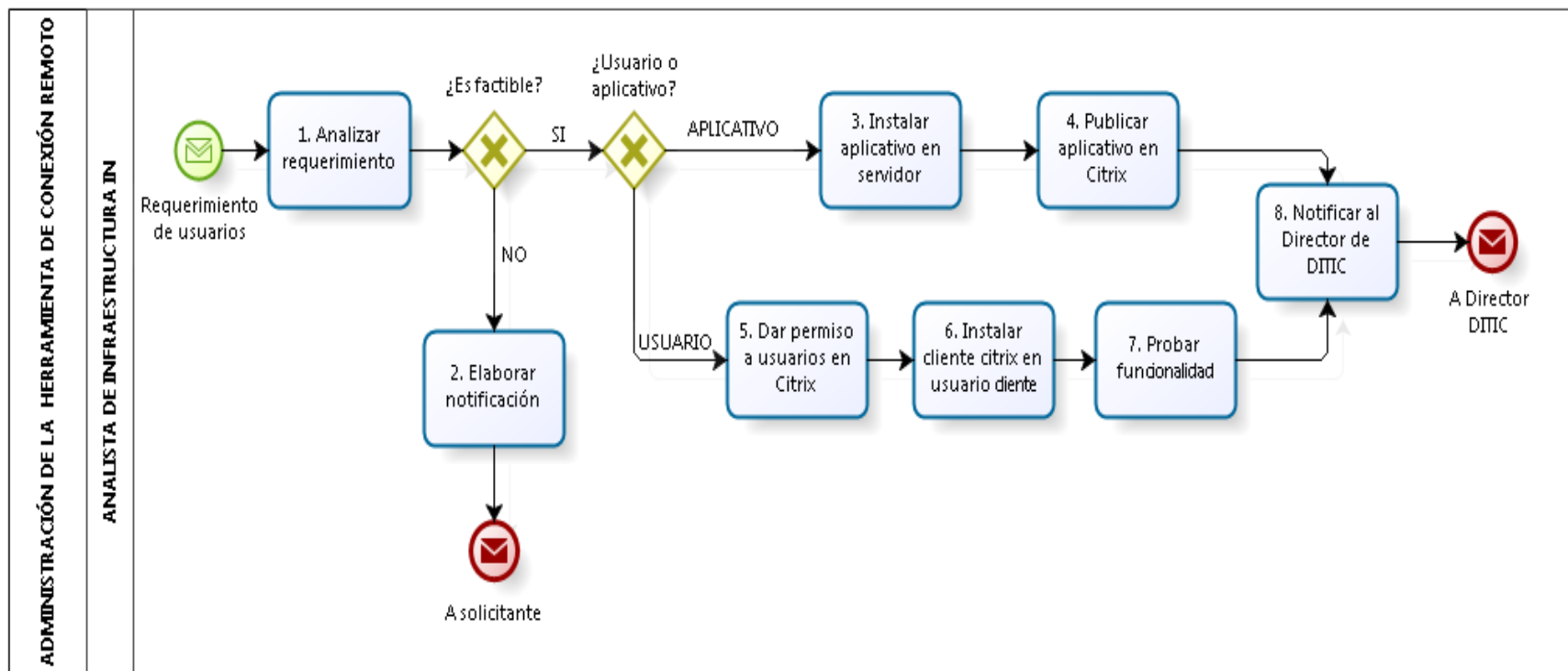
<b>Elaborado por:</b>	<b>Revisado por:</b>	<b>Aprobado /Autorizado por:</b>	<b>Registrado por:</b>
PC	DIPLA - DIFI	DIREJ	DIPLA, PC



- e) Deberá definirse el trabajo que se permite realizar, las horas laborables, la confidencialidad de la información que se conserva y los sistemas y servicios internos para los cuales el trabajador tiene acceso autorizado.
- f) Deberá considerarse la protección de antivirus y reglas del Firewall.
- g) Deberán estar documentadas las reglas y directrices sobre el acceso de familiares y visitantes al equipo y a la información.
- h) La institución deberá observar la disposición de una póliza de seguros para esos equipos.
- i) Determinar procesos de monitoreo y auditoría de la seguridad del trabajo remoto que se realice.
  - j) Permitir al personal realizar trabajo remoto empleando tecnologías de comunicaciones cuando requiere hacerlo desde un lugar fijo fuera de su institución.

Elaborado por:	Revisado por:	Aprobado /Autorizado por:	Registrado por:
PC	DIPLA - DIFI	DIREJ	DIPLA, PC

### 5.12.3. DIAGRAMA DE FLUJO DEL SUBPROCESO DE ADMINISTRACIÓN DE CONEXIÓN REMOTA



Elaborado por:  
PC

Revisado por:  
DIPLA - DIFI

Aprobado /Autorizado por:  
DIREJ

Registrado por:  
DIPLA, PC

#### 5.12.4. PROCEDIMIENTO DEL SUBPROCESO DE ADMINISTRACIÓN DE CONEXIÓN REMOTA

N	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	DOCUMENTO GENERADO
1	Analizar requerimiento	Realiza el respectivo análisis del requerimiento recibido	Analista de Infraestructura de Tecnologías de la Información	Correo electrónico
	Decisión	<b>¿Es factible?</b> <b>NO:</b> Realiza la actividad 2. Elaborar notificación. <b>SI:</b> Continúa con la decisión. <b>¿Usuario o aplicativo?</b>	Analista de Infraestructura de Tecnologías de la Información	N/A
2	Elaborar notificación, fin	Realiza la notificación indicando que no será posible ejecutar acción alguna por el estado en que se encuentre el equipo informático y se informa al usuario. <b>Fin del proceso.</b>	Analista de Infraestructura de Tecnologías de la Información	Correo electrónico
	Decisión	<b>¿Usuario o aplicativo?</b> <b>APLICATIVO:</b> Realiza la actividad 3. Instalar aplicativo en servidor. <b>USUARIO:</b> Realiza la actividad 5. Dar permiso a usuarios en Citrix.	Analista de Infraestructura de Tecnologías de la Información	N/A
3	Instalar aplicativo en servidor	Realiza la instalación del aplicativo en el servidor	Analista de Infraestructura de Tecnologías de la Información	N/A
4	Publicar aplicativo en Citrix	Realiza la publicación del aplicativo en el Citrix. Continúa con la actividad 8.	Analista de Infraestructura de Tecnologías de la Información	N/A
5	Dar permiso a usuarios en Citrix	Realiza el permiso a los usuarios en el Citrix	Analista de Infraestructura de Tecnologías de la Información	N/A
6	Instalar cliente Citrix en usuario cliente	Realiza la instalación del cliente Citrix en el usuario cliente	Analista de Infraestructura de Tecnologías de la Información	N/A
7	Probar funcionalidad, fin	Realiza prueba de la funcionalidad del sistema.	Analista de Infraestructura de Tecnologías de la Información	N/A
8	Notificar al Director de DITIC	Notifica al Director de DITIC que se ha realizado el requerimiento para que informe al solicitante.	Analista de Infraestructura de Tecnologías de la Información	Correo electrónico

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------



#### 5.12.5. INDICADORES DEL SUBPROCESO DE ADMINISTRACIÓN DE CONEXIÓN REMOTA

N°	Indicador	Fórmula de Cálculo	Unidad de Medida	Responsable de Medición	Fuente de Medición	Frecuencia de Medición
1	Porcentaje de disponibilidad de conexión remota	$((\text{Tiempo total sondeo} - \text{tiempo no disponible}) / \text{tiempo total de sondeo}) * 100\%$	%	Responsable de infraestructura	Reporte de software Whatsup	Trimestral

#### 5.12.6. FORMATOS DEL SUBPROCESO DE ADMINISTRACIÓN DE CONEXIÓN REMOTA

Nombre del Registro de Calidad	Código de Formato
N/A	N/A

#### 5.12.7. ANEXOS DEL SUBPROCESO DE ADMINISTRACIÓN DE CONEXIÓN REMOTA

“No hay anexos.”

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------

### 5.13. SUBPROCESO DE ADMINISTRACIÓN DE HERRAMIENTAS DE MONITOREO

#### 5.13.1. FICHA TÉCNICA DEL SUBPROCESO DE ADMINISTRACIÓN DE HERRAMIENTAS DE MONITOREO

<b>Proceso:</b>	GESTIÓN DE INFRAESTRUCTURA DE TECNOLOGÍA DE LA INFORMACIÓN
<b>Nombre del Subproceso:</b>	ADMINISTRACIÓN DE HERRAMIENTAS DE MONITOREO
<b>Código del Subproceso:</b>	DITIC-IT-SP13
<b>Descripción:</b>	<p><b>PROPÓSITO:</b> Establecer el procedimiento requerido para la administración de las diferentes herramientas de monitoreo indispensables para la detección de fallas en la infraestructura tecnológica.</p> <p><b>ALCANCE:</b> Desde analizar el tipo de monitoreo a realizar, hasta enviar informe.</p> <p><b>DISPARADOR:</b></p> <ul style="list-style-type: none"> <li>Alarmas generadas por los equipos.</li> </ul> <p><b>PROVEEDORES:</b></p> <ul style="list-style-type: none"> <li>Unidades del INEC.</li> </ul> <p><b>INSUMOS:</b></p> <ul style="list-style-type: none"> <li>Correo electrónico.</li> <li>Autorización por Director de DITIC.</li> </ul>
<b>Clientes:</b>	<ul style="list-style-type: none"> <li>Todas las direcciones del INEC</li> </ul>
<b>Salidas:</b>	<ul style="list-style-type: none"> <li>Informe de alarmas generadas y atendidas.</li> </ul>
<b>Tipo de Proceso:</b>	<ul style="list-style-type: none"> <li>Adjetivo asesor.</li> </ul>
<b>Responsable del Proceso:</b>	Responsable de Gestión de Infraestructura de TI
<b>Recursos:</b>	<p><b>MATERIALES:</b></p> <ul style="list-style-type: none"> <li>Equipo de computación</li> <li>Equipo y materiales de oficina.</li> </ul> <p><b>HUMANOS:</b></p> <ul style="list-style-type: none"> <li>2 analistas de Gestión de Infraestructura de TI SP7.</li> <li>4 analistas de Gestión de Infraestructura de TI SP5.</li> <li>1 analista de Gestión de Infraestructura de TI SP1.</li> </ul> <p><b>TECNOLÓGICOS:</b></p> <ul style="list-style-type: none"> <li>Correo Electrónico.</li> <li>Software Ofimática.</li> <li>Acceso a internet.</li> </ul>

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------

	<ul style="list-style-type: none"> <li>Herramientas para soporte en redes.</li> <li>Sistema de monitoreo.</li> </ul>
<b>Controles/Marco Legal:</b>	<ul style="list-style-type: none"> <li>Acuerdo 166 de la secretaria de la administración pública esquema gubernamental de la seguridad de la información (EGSI).</li> </ul>

### 5.13.2. CONTROLES DEL SUBPROCESO DE ADMINISTRACIÓN DE HERRAMIENTAS DE MONITOREO

#### Acuerdo 166 de la secretaria de la administración pública esquema gubernamental de la seguridad de la información (EGSI)

- Sección 7.11, literal a, se tiene identificado y documentado todos los equipos que componen la infraestructura de red.
- Acuerdo 166 EGSI, sección 7.13, literal a, los activos que se han identificado para monitorear su operación y tener en tiempo real el control y acciones de administración.

Gestión de eventos: monitorear todos los eventos que ocurren en la infraestructura de TI para permitir su operación normal a través de la detección y escalación de condiciones que causen un impacto mayor.

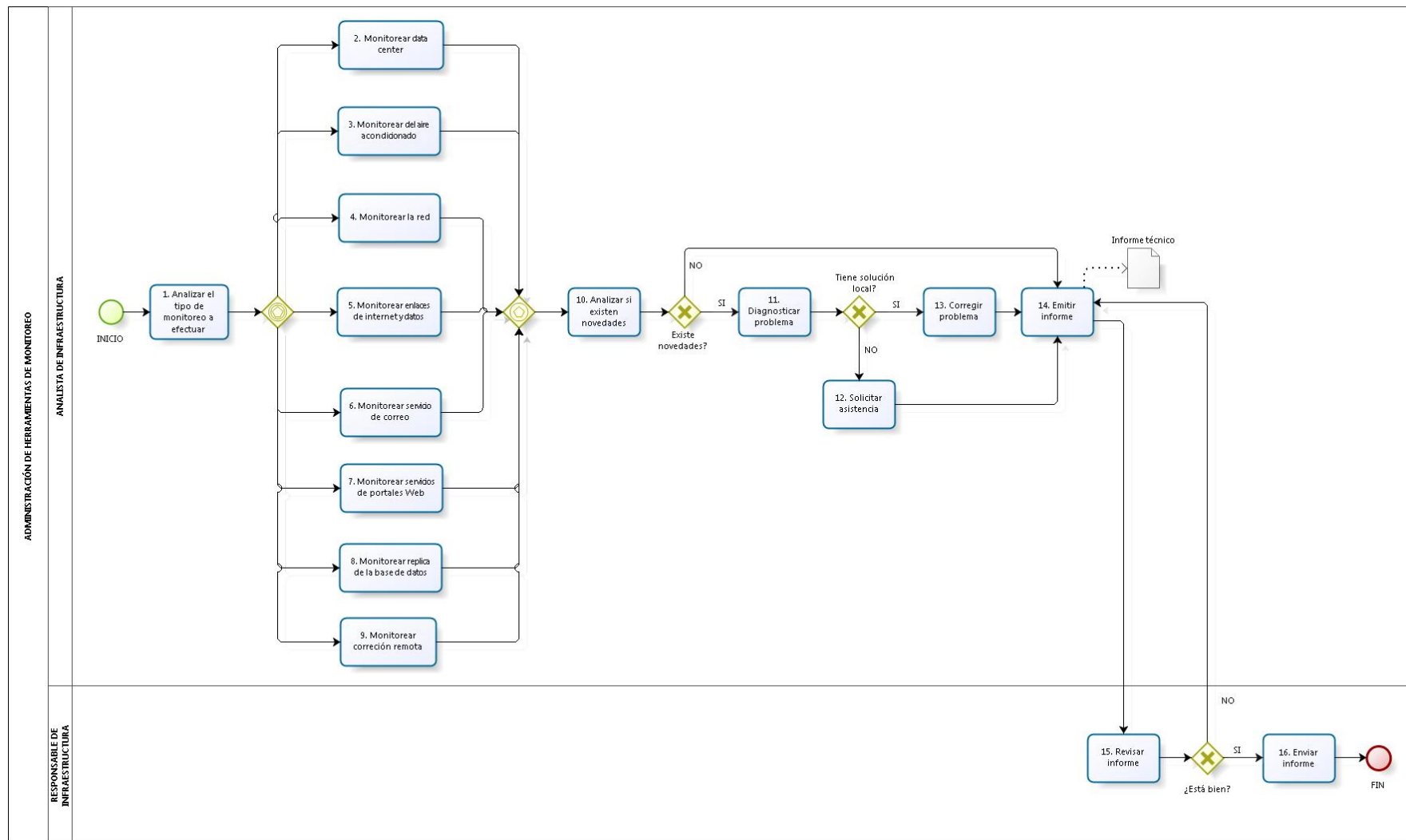
La gestión de eventos depende del conocimiento del estado de la infraestructura de TI a través de la detección oportuna de cualquier interrupción en la operación normal o esperada, para lo cual se hace uso de sistemas de control a nivel de software y hardware.

1) Sistemas de monitoreo activo, que censan la infraestructura de TI del INEC, para determinar su estado y disponibilidad. Cualquier interrupción generará una alerta para tomar acciones preventivas o correctivas. En esta gestión de eventos se automatiza las actividades que se mencionan a continuación y que son responsabilidad del personal encargado de la infraestructura tecnológica.

- Ocurrencia del evento: Los eventos ocurren constantemente, para ello se ha identificado los tipos de eventos que necesitan ser detectados.
  - Eventos del Data Center
  - Eventos del Sistema de Aire Acondicionado
  - Eventos de la Infraestructura de Red
  - Eventos de los Enlaces de Internet y Datos
  - Eventos del Servidor de correo electrónico
  - Eventos del Servidor de portal web
  - Eventos del Servicio de Replica de Bases de Datos
- Notificación del evento: de acuerdo a las configuraciones de los equipos que son monitoreados, se usa el protocolo SNMP para la administración de los dispositivos de red.
- Detección del evento: la notificación del evento se detecta mediante la configuración de agentes y “sondas” configuradas en los dispositivos que están siendo monitoreado.
- Filtrado de eventos: el filtrado consiste en decidir cuáles eventos serán notificados y detectados por las distintas herramientas de monitoreo.
- Acciones de revisión: con la cantidad de eventos que se generan cada día, es imposible revisar cada uno de ellos de manera individual. Sin embargo, es necesario asegurarse que aquellos eventos significativos hayan sido tratados de manera apropiada.
- Cierre del evento: consiste en la resolución de un evento cuando éste ha sido solucionado.

<b>Elaborado por:</b>	<b>Revisado por:</b>	<b>Aprobado /Autorizado por:</b>	<b>Registrado por:</b>
PC	DIPLA - DIFI	DIREJ	DIPLA, PC

### 5.13.3. DIAGRAMA DE FLUJO DEL SUBPROCESO DE ADMINISTRACIÓN DE HERRAMIENTAS DE MONITOREO



Elaborado por:

PC

Revisado por:

DIPLA - DIFI

Aprobado /Autorizado por:

DIREJ

Registrado por:

DIPLA, PC



#### 5.13.4. PROCEDIMIENTO DEL SUBPROCESO DE ADMINISTRACIÓN DE HERRAMIENTAS DE MONITOREO

Nº	Actividad	Detalle de la actividad	Responsable	Documento Generado
1	Analizar el tipo de monitoreo a efectuar	Analiza el tipo de monitoreo a realizar	Analista de infraestructura	N/A
2	Monitorear data center	Realiza el monitoreo del data center para medir su estatus de acción	Analista de infraestructura	N/A
3	Monitorear del aire acondicionado	Realiza el monitoreo del aire acondicionado para saber si se puede manipular el equipo	Analista de infraestructura	N/A
4	Monitorear la red	Realiza el monitoreo de la red para identificar su estado actual	Analista de infraestructura	N/A
5	Monitorear enlaces de internet y datos	Realiza el monitoreo de los enlaces de internet y datos en los equipos informáticos	Analista de infraestructura	N/A
6	Monitorear servicio de correo	Realiza el monitoreo del servicio del correo electrónico en los equipos informáticos	Analista de infraestructura	N/A
7	Monitorear servicios de portales Web	Realiza el monitoreo de los servicios de portales Web	Analista de infraestructura	N/A
8	Monitorear réplica de la base de datos	Realiza el monitoreo de réplica de la base de datos	Analista de infraestructura	N/A
9	Monitorear corrección remota	Realiza el monitoreo de la corrección remota	Analista de infraestructura	N/A
10	Analizar si existen novedades	Analiza si existen novedades en el monitoreo realizado, con el fin de tomar medidas.	Analista de infraestructura	N/A
	Decisión	<b>¿Existen novedades?</b> <b>NO:</b> Pasar a la actividad 14. Emitir informe. <b>SI:</b> Pasa a la actividad 11. Diagnosticar problema.	Analista de infraestructura	N/A

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------

11	Diagnosticar problema informático	Realiza el diagnóstico del problema informático en los equipos	Analista de infraestructura	N/A
	Decisión	<b>¿Tiene solución local?</b> <b>NO:</b> Pasa a la actividad <b>12.</b> Solicitar asistencia. <b>SI:</b> Pasa a la actividad <b>13.</b> Corregir problema.	Analista de infraestructura	N/A
12	Solicitar asistencia	Realiza la solicitud de la asistencia para los equipos informáticos. Continúa con la actividad <b>14.</b>	Analista de infraestructura	N/A
13	Corregir problema	Realiza la corrección del problema en los equipos informáticos	Analista de infraestructura	N/A
14	Emitir informe	Realiza la emisión del informe de cómo se encuentra el equipo informático	Analista de infraestructura	Informe técnico
15	Revisar informe	Realiza la revisión del informe para tener documentada la acción realizada	Responsable de infraestructura	N/A
	Decisión	<b>¿Está bien?</b> <b>NO:</b> Regresa a la actividad <b>14.</b> Emitir informe. <b>SI:</b> Realiza la actividad <b>16.</b> Enviar informe.	Responsable de infraestructura	N/A
16	Enviar informe	Realiza el envío del informe para la notificación de que el requerimiento está ejecutado. <b>Fin del proceso.</b>	Responsable de infraestructura	N/A

#### 5.13.5. INDICADORES DEL SUBPROCESO DE ADMINISTRACIÓN DE HERRAMIENTAS DE MONITOREO

N°	Indicador	Fórmula de Cálculo	Unidad de Medida	Responsable de Medición	Fuente de Medición	Frecuencia de Medición
1	Porcentaje de cumplimiento en la administración de herramientas de monitoreo	$(\# \text{ de alarmas atendidas} / \# \text{ de alarmas generadas}) * 100\%$	Porcentaje	Responsable de Infraestructura de TI	Sistemas de monitoreo	Trimestral

#### 5.13.6. FORMATOS DEL SUBPROCESO DE ADMINISTRACIÓN DE HERRAMIENTAS DE MONITOREO

Nombre del Registro de Calidad	Código de Formato
Informe técnico	DITIC-TI-SP13-INF-01

#### 5.13.7. ANEXOS DEL SUBPROCESO DE ADMINISTRACIÓN DE HERRAMIENTAS DE MONITOREO

“No hay anexos.”

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------

## 5.14. SUBPROCESO DE ADMINISTRACIÓN DE SERVICIOS DE VIDEO CONFERENCIA

### 5.14.1. FICHA TÉCNICA DEL SUBPROCESO DE ADMINISTRACIÓN DE SERVICIOS DE VIDEO CONFERENCIA

<b>Proceso:</b>	GESTIÓN DE INFRAESTRUCTURA DE TECNOLOGÍAS DE LA INFORMACIÓN
<b>Nombre del Subproceso:</b>	ADMINISTRACIÓN DE SERVICIOS DE VIDEO CONFERENCIA
<b>Código del Subproceso:</b>	DITIC-IT-SP14
<b>Descripción:</b>	<p><b>PROPÓSITO:</b> Proporcionar un excelente servicio de videoconferencia para las necesidades de la institución, así como la resolución de incidentes de la misma.</p> <p><b>ALCANCE:</b> Desde analizar el requerimiento, hasta informar a los solicitantes.</p> <p><b>DISPARADOR:</b></p> <ul style="list-style-type: none"> <li>• Tickets.</li> <li>• Correo electrónico.</li> </ul> <p><b>PROVEEDORES:</b></p> <ul style="list-style-type: none"> <li>• Funcionarios del INEC.</li> </ul> <p><b>INSUMOS:</b></p> <ul style="list-style-type: none"> <li>• Tickets.</li> <li>• Correo electrónico.</li> </ul>
<b>Clientes:</b>	<ul style="list-style-type: none"> <li>• Funcionarios del INEC.</li> </ul>
<b>Salidas:</b>	<ul style="list-style-type: none"> <li>• Informe de Requerimientos de Videoconferencia.</li> </ul>
<b>Tipo de Proceso:</b>	<ul style="list-style-type: none"> <li>• Adjetivo de Asesoría.</li> </ul>
<b>Responsable del Proceso:</b>	Responsable de la Unidad de Gestión de Infraestructura de TI
<b>Recursos:</b>	<p><b>MATERIALES:</b></p> <ul style="list-style-type: none"> <li>• Equipo de computación</li> <li>• Equipo y materiales de oficina.</li> </ul> <p><b>HUMANOS:</b></p> <ul style="list-style-type: none"> <li>• 1 Analista de Gestión de Infraestructura de TI SP1.</li> <li>• 2 Analistas de Gestión de Infraestructura de TI SP5.</li> </ul> <p><b>TECNOLÓGICOS:</b></p> <ul style="list-style-type: none"> <li>• Correo Electrónico.</li> <li>• Software Ofimática.</li> <li>• Videoconferencia.</li> </ul>

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------

<b>Controles/Marco Legal:</b>	<ul style="list-style-type: none"> <li>Esquema Gubernamental de Seguridad de la información (EGSI)Cap. 3.3 literal f.</li> </ul>
-------------------------------	--

#### 5.14.2. CONTROLES DEL SUBPROCESO DE ADMINISTRACIÓN DE SERVICIOS DE VIDEO CONFERENCIA

Acuerdo 166 de la secretaria de la Administración Pública esquema gubernamental de la seguridad de la información (EGSI)

3.3 Uso aceptable de los activos

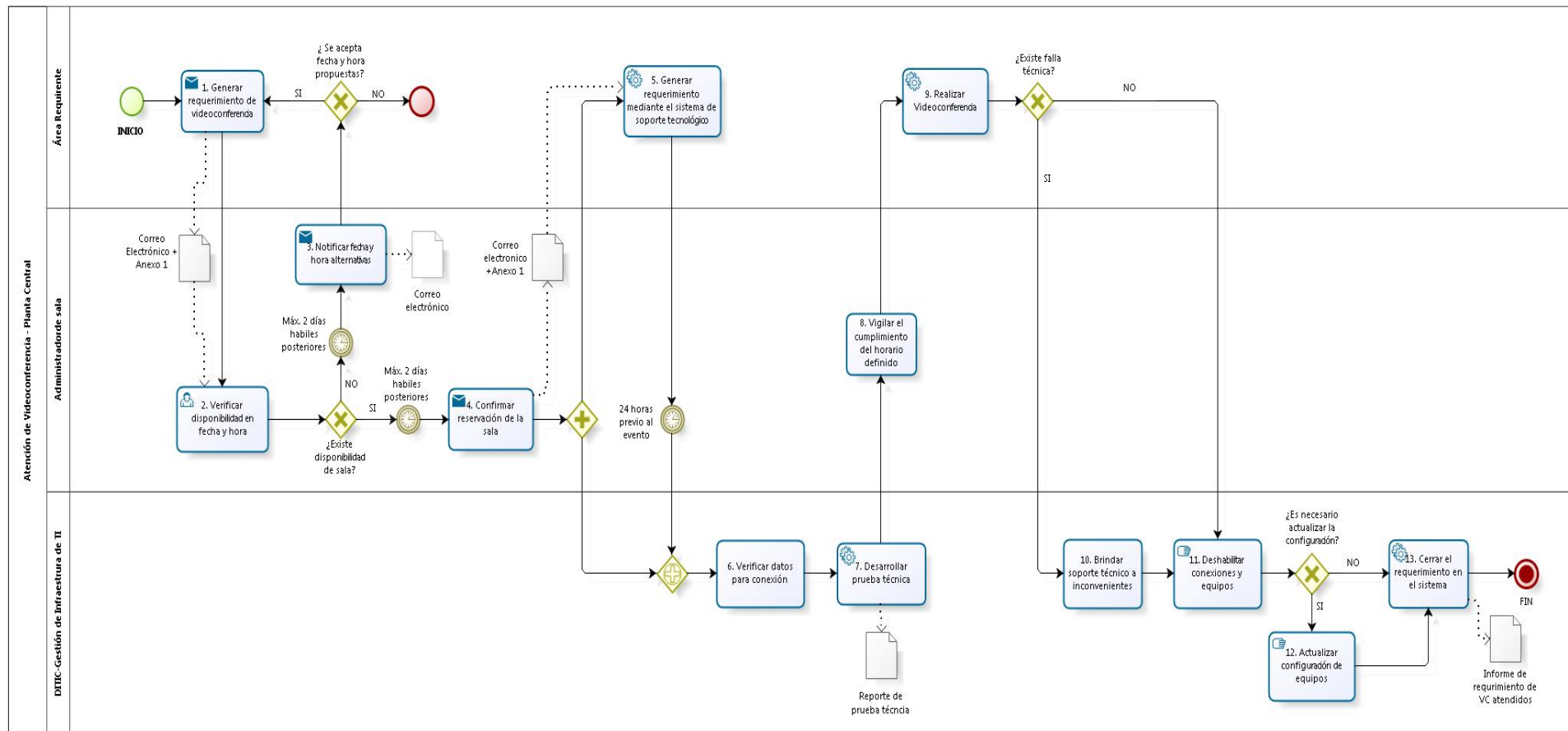
f) Reglamentar el uso de los sistemas de video-conferencia (\*):

- Definir un responsable para administrar la video-conferencia
- Definir y documentar el procedimiento de acceso a los ambientes de pruebas

Deshabilitar la respuesta automática de los equipos de video-conferencia.

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------

### 5.14.3. DIAGRAMA DE FLUJO DEL SUBPROCESO DE ADMINISTRACIÓN DE SERVICIOS DE VIDEO CONFERENCIA



<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DIFI	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	--------------------------------------	---	-------------------------------------

#### 5.14.4. PROCEDIMIENTO DEL SUBPROCESO DE ADMINISTRACIÓN DE SERVICIOS DE VIDEO CONFERENCIA

N	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	DOCUMENTO GENERADO
1	Generar requerimiento de videoconferencia	Genera el requerimiento para hacer uso de la videoconferencia al administrador de la sala.	Área requirente	Correo electrónico / Anexo 1
2	Verificar disponibilidad en fecha y hora	Revisa el requerimiento recibido, para confirmar disponibilidad en hora y fecha de la sala.	Administrador de sala	N/A
	Decisión	<b>¿Existe disponibilidad de sala?</b> <b>NO:</b> Realiza la actividad <b>3</b> . Notificar fecha y hora. <b>SI:</b> Realiza la actividad <b>4</b> . Confirmar reservación de la sala.	Administrador de sala	N/A
3	Notificar fecha y hora alternativas	<b>En máximo 2 días hábiles posteriores:</b> Notifica al área requirente la fecha y hora alternativa para poder realizar la videoconferencia.	Administrador de sala	Correo electrónico
	Decisión	<b>¿Se acepta fecha y hora propuestas?</b> <b>NO: Fin del proceso.</b> <b>SI:</b> Regresa a la actividad <b>1</b> . Generar requerimiento de videoconferencia.	Área requirente	N/A
4	Confirmar reservación de la sala	<b>En máximo 2 días hábiles posteriores:</b> Confirma la reservación de la sala para la videoconferencia solicitada.	Administrador de sala	Correo electrónico / Anexo 1
5	Generar requerimiento mediante el sistema de soporte tecnológico	<b>Paralelamente:</b> Genera requerimiento mediante el sistema de soporte tecnológico.	Área requirente	N/A
6	Verificar datos para conexión	Verifica los datos para realizar la conexión pertinente.	Gestión de Infraestructura de IT	N/A
7	Desarrollar prueba técnica	Desarrolla la prueba técnica	Gestión de Infraestructura de IT	Reporte de prueba técnica
8	Vigilar el cumplimiento del horario definido	Vigila el cumplimiento del horario definido	Administrador de sala	N/A
9	Realizar videoconferencia	Realiza la videoconferencia requerida	Área requirente	N/A
	Decisión	<b>¿Existe falta técnica?</b> <b>SI:</b> Realiza la actividad <b>10</b> . Brinda soporte técnico a inconvenientes. <b>NO:</b> Realiza la actividad <b>11</b> . Deshabilitar conexiones y equipos.	Área requirente	N/A
10	Brindar soporte técnico a inconvenientes	Brinda soporte técnico a inconvenientes presentados durante la videoconferencia	Gestión de Infraestructura de IT	N/A

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

11	Deshabilitar conexiones y equipos	Deshabilita las conexiones y equipos con el fin de buscar soluciones	Gestión de Infraestructura de IT	N/A
	Decisión	<b>¿Es necesario actualizar la configuración?</b> <b>SI:</b> Realiza la actividad <b>12.</b> Actualizar configuración de equipos. <b>NO:</b> Realiza la actividad <b>13.</b> Cerrar el requerimiento en el sistema.	Gestión de Infraestructura de IT	N/A
12	Actualizar configuración de equipos	Actualiza la configuración de los equipos. Continúa con la actividad <b>13.</b>	Gestión de Infraestructura de IT	N/A
13	Cerrar el requerimiento en el sistema	Cierra el requerimiento en el sistema. <b>Fin del proceso.</b>	Gestión de Infraestructura de IT	Informe de requerimiento de VC atendidos

#### 5.14.5. INDICADORES DEL SUBPROCESO DE ADMINISTRACIÓN DE SERVICIOS DE VIDEO CONFERENCIA

N°	Indicador	Fórmula de Cálculo	Unidad de Medida	Responsable de Medición	Fuente de Medición	Frecuencia de Medición
1	Número de servicios de video conferencia brindados	(Sumatoria de video conferencias atendidas )	Número	Responsable de infraestructura	Informe de técnico de ejecución	Trimestral

#### 5.14.6. FORMATOS DEL SUBPROCESO DE ADMINISTRACIÓN DE SERVICIOS DE VIDEO CONFERENCIA

Nombre del Registro de Calidad	Código de Formato
N/A	N/A

#### 5.14.7. ANEXOS DEL SUBPROCESO DE ADMINISTRACIÓN DE SERVICIOS DE VIDEO CONFERENCIA

“No hay anexos.”

Elaborado por: PC	Revisado por: DIPLA - DITIC	Aprobado /Autorizado por: DIREJ	Registrado por: DIPLA, PC
----------------------	--------------------------------	------------------------------------	------------------------------

## 5.15. SUBPROCESO DE GENERACIÓN DE RESPALDOS DE INFORMACIÓN

### 5.15.1. FICHA TÉCNICA DEL SUBPROCESO DE GENERACIÓN DE RESPALDOS DE INFORMACIÓN

<b>Proceso:</b>	GESTIÓN DE INFRAESTRUCTURA DE TECNOLOGÍAS DE LA INFORMACIÓN
<b>Nombre del Subproceso:</b>	GENERACIÓN DE RESPALDOS DE INFORMACIÓN
<b>Código del Subproceso:</b>	DITIC-TI-SP15
<b>Descripción:</b>	<p><b>PROPÓSITO:</b> Asegurar que la información generada por las diferentes unidades institucionales, no sufra pérdidas se pierda y esté disponible en caso de cualquier contingencia, como daño en los servidores, unidades de almacenamiento y la posible eliminación accidental de la Información.</p> <p><b>ALCANCE:</b> Desde la elaboración del requerimiento de respaldo de información, hasta la elaboración de atención del mismo.</p> <p><b>DISPARADOR:</b></p> <ul style="list-style-type: none"> <li>• Memorando o correo electrónico.</li> </ul> <p><b>PROVEEDORES:</b></p> <ul style="list-style-type: none"> <li>• Todas las gestiones del INEC.</li> </ul> <p><b>INSUMOS:</b></p> <ul style="list-style-type: none"> <li>• Información a respaldar.</li> </ul>
<b>Clientes:</b>	<ul style="list-style-type: none"> <li>• Todas las direcciones del INEC</li> </ul>
<b>Salidas:</b>	<ul style="list-style-type: none"> <li>• Respallos de información (carpetas compartidas, correos, servidores, bases de datos).</li> </ul>
<b>Tipo de Proceso:</b>	<ul style="list-style-type: none"> <li>• Adjetivo de Asesoría.</li> </ul>
<b>Responsable del Proceso:</b>	Responsable de Gestión de Infraestructura de Tecnologías de la Información
<b>Recursos:</b>	<p><b>MATERIALES:</b></p> <ul style="list-style-type: none"> <li>• Equipo de computación</li> <li>• Equipo y materiales de oficina.</li> <li>• Librería robótica.</li> </ul> <p><b>HUMANOS:</b></p> <ul style="list-style-type: none"> <li>• 1 Analista de Gestión de Infraestructura de TI 3 (SP7)</li> <li>• 4 Analistas de Gestión de Infraestructura de TI 2 (SP5)</li> </ul> <p><b>TECNOLÓGICOS:</b></p> <ul style="list-style-type: none"> <li>• Correo Electrónico.</li> <li>• Software Ofimática.</li> <li>• HP Data Protector</li> </ul>

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------



**Controles/Marco Legal:**

- Normas de control interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos- de la contraloría
- Acuerdo 166 de la secretaria de la administración pública esquema gubernamental de la seguridad de la información (EGSI)

### 5.15.2. CONTROLES DEL SUBPROCESO DE GENERACIÓN DE RESPALDOS DE INFORMACIÓN

#### ACUERDO 166 DE LA SECRETARIA DE LA ADMINISTRACION PÚBLICA ESQUEMA GUBERNAMENTAL DE LA SEGURIDAD DE LA INFORMACION (EGSI)

#### 3 GESTIÓN DE LOS ACTIVOS

##### 3.1. Inventario de activos

Inventariar los activos referentes a la estructura organizacional:

a) Estructura organizacional del área de las TIC, con los cargos y nombres del personal: administrador (de servidores, de redes de datos, de respaldos de la información, de sistemas de almacenamiento, de bases de datos, de seguridades, de aplicaciones del negocio, de recursos informáticos, etc.), líder de proyecto, personal de capacitación, personal de mesa de ayuda, personal de aseguramiento de calidad, programadores (PHP, Java, etc.).

#### 6. GESTIÓN DE COMUNICACIONES Y OPERACIONES

##### 6.4. Separación de las instancias de Desarrollo, Pruebas, Capacitación y Producción.

c) Controlar la instalación y uso de herramientas de desarrollo de software y/o acceso a bases de datos y redes en los equipos informáticos, salvo que sean parte de las herramientas de uso estándar o su instalación sea autorizada de acuerdo a un procedimiento expresamente definido.

#### 7. CONTROL DE ACCESO

##### 7.3. Gestión de privilegios

b) Mantener un cuadro de identificación de los usuarios y sus privilegios asociados con cada servicio o sistema operativo, sistema de gestión de base de datos y aplicaciones.

#### 8. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

##### 8.6. Política sobre el uso de controles criptográficos

b) Utilizar controles criptográficos para la protección de claves de acceso a: sistemas, datos y servicios. Las claves deberán ser almacenadas de manera codificada, cifrada (encriptada) en la base de datos y/o en archivos de parámetros.

##### 8.8. Control del software operativo

c) Ningún programador o analista de desarrollo y mantenimiento de aplicaciones podrá acceder a los ambientes de producción.

##### 8.9. Protección de los datos de prueba del sistema

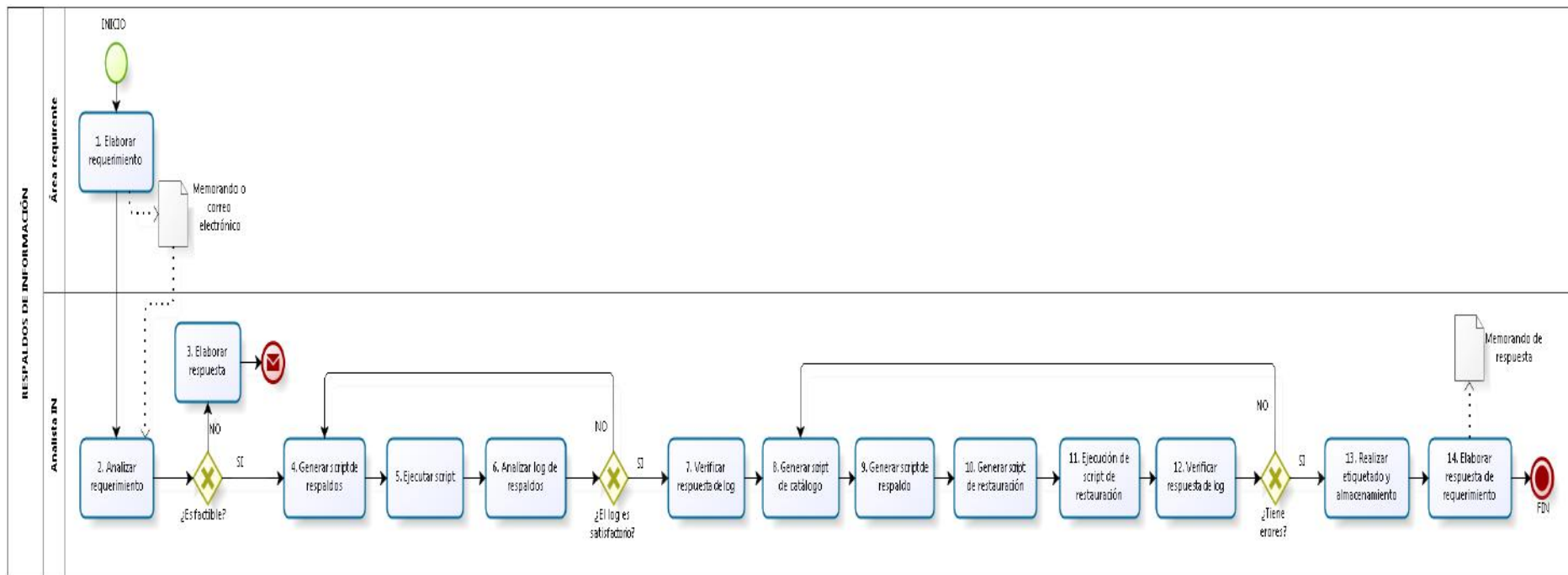
<b>Elaborado por:</b>	<b>Revisado por:</b>	<b>Aprobado /Autorizado por:</b>	<b>Registrado por:</b>
PC	DIPLA - DITIC	DIREJ	DIPLA, PC



- a) Identificar por cada sistema, los datos que pueden ser copiados de un ambiente de producción a un ambiente de pruebas.
- b) Efectuar pruebas de los sistemas en el ambiente de pruebas, sobre datos extraídos del ambiente de producción.
- c) Solicitar autorización formal para realizar una copia de la base de datos de producción como base de datos de prueba.
- d) Personalizar los datos en el ambiente de pruebas, eliminando las contraseñas de producción y generando nuevas para pruebas.
- f) Aplicar los mismos procedimientos de control de acceso que existen en la base de producción.
- i) Controlar que la modificación, actualización o eliminación de los datos operativos (de producción) serán realizados a través de los sistemas que procesan esos datos, y de acuerdo al esquema de control de accesos implementado en los mismos.

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

### 5.15.3. DIAGRAMA DE FLUJO DEL SUBPROCESO DE GENERACIÓN DE RESPALDOS DE INFORMACIÓN



<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

#### 5.15.4. PROCEDIMIENTO DEL SUBPROCESO DE GENERACIÓN DE RESPALDOS DE INFORMACIÓN

Nº	Actividad	Detalle de la actividad	Responsable	Documento Generado
1	Elaborar requerimiento	Elaborar el requerimiento para solicitar el servicio para solucionar el inconveniente con el equipo informático.	Área requirente	Memorando o correo electrónico
2	Analizar requerimiento	Analizar la factibilidad de ejecución del requerimiento realizado por el área solicitante.	Analista de Infraestructura de Tecnologías de la Información	N/A
	Decisión	<b>¿Es factible realizar el requerimiento?</b> <b>SI:</b> Pasa a la actividad 4. Generar script. <b>NO:</b> Pasa a la actividad 3. Elaborar respuesta de NO factibilidad.	Analista de Infraestructura de Tecnologías de la Información	N/A
3	Elaborar respuesta de no factibilidad	Elaborar y remitir una respuesta al área requirente en la cual se expliquen cuales con las razones para que no se pueda atender el requerimiento.	Analista de Infraestructura de Tecnologías de la Información	Respuesta de NO factibilidad
4	Generar script	Realizar un script para la generación de los respaldos respectivos.	Analista de Infraestructura de Tecnologías de la Información	N/A
5	Ejecutar script	Ejecutar el script para determinar el estado actual.	Analista de Infraestructura de Tecnologías de la Información	N/A
6	Analizar log	Analizar el log de los respaldos para verificar si estos se encuentran en estado satisfactorio.	Analista de Infraestructura de Tecnologías de la Información	N/A
	Decisión	<b>¿Los respaldos se encuentran en estado satisfactorio?</b> <b>SI:</b> Pasa a la actividad 7. Verificar respuesta. <b>NO:</b> Regresa a la actividad 4. Generar script.	Analista de Infraestructura de Tecnologías de la Información	N/A
7	Verificar respuesta	Verificar que la respuesta del log permita generar los scripts.	Analista de Infraestructura de Tecnologías de la Información	N/A
8	Generar script de catálogo	Generar el script del catálogo informático.	Analista de Infraestructura de Tecnologías de la Información	N/A
Elaborado por: PC		Revisado por: DIPLA - DITIC	Aprobado /Autorizado por: DIREJ	Registrado por: DIPLA, PC

9	Generar script de respaldo	Generar el script del respaldo de la información.	Analista de Infraestructura de Tecnologías de la Información	N/A
10	Generar script de restauración	Generar el script de la restauración.	Analista de Infraestructura de Tecnologías de la Información	N/A
11	Ejecutar script	Ejecutar el script de restauración.	Analista de Infraestructura de Tecnologías de la Información	N/A
12	Verificar respuesta	Verificar la respuesta del log para constatar si existen errores o no.	Analista de Infraestructura de Tecnologías de la Información	N/A
	Decisión	<b>¿La respuesta del Log tiene errores?</b> <b>SI:</b> Pasa a la actividad <b>13</b> . Realizar etiquetado. <b>NO:</b> Regresa a la actividad <b>8</b> . Generar script de catálogo.	Analista de Infraestructura de Tecnologías de la Información	N/A
13	Realizar etiquetado	Realizar el etiquetado y almacenamiento de los respaldos para en caso de que exista un siniestro volverlos a cargar.	Analista de Infraestructura de Tecnologías de la Información	N/A
14	Elaborar respuesta	Elaborar la respuesta del requerimiento para comunicar lo ejecutado. <b>Fin del subproceso.</b>	Analista de Infraestructura de Tecnologías de la Información	N/A

#### 5.15.5. INDICADORES DEL SUBPROCESO DE GENERACIÓN DE RESPALDOS DE INFORMACIÓN

N°	Indicador	Fórmula de Cálculo	Unidad de Medida	Responsable de Medición	Fuente de Medición	Frecuencia de Medición
1	Porcentaje de cumplimiento en respaldos de información	(# de respaldos realizadas / # total de respaldos planificados)*100%	Porcentaje	Jefe Gestión de Infraestructura de Tecnologías de la Información	Informe técnico de ejecución	Trimestral

#### 5.15.6. FORMATOS DEL SUBPROCESO DE GENERACIÓN DE RESPALDOS DE INFORMACIÓN

Nombre del Registro de Calidad	Código de Formato
N/A	N/A

#### 5.15.7. ANEXOS DEL SUBPROCESO DE GENERACIÓN DE RESPALDOS DE INFORMACIÓN

“No hay anexos.”

Elaborado por: PC	Revisado por: DIPLA - DITIC	Aprobado /Autorizado por: DIREJ	Registrado por: DIPLA, PC
----------------------	--------------------------------	------------------------------------	------------------------------

## 6. DESCRIPCIÓN DE PROCESOS DE GESTIÓN DE SOPORTE A USUARIOS

### 6.1. SUBPROCESO DE ASESORAMIENTO TECNOLÓGICO

#### 6.1.1. FICHA TÉCNICA DEL SUBPROCESO DE ASESORAMIENTO TECNOLÓGICO

Proceso:	GESTIÓN DE SOPORTE A USUARIOS		
Nombre del Subproceso:	ASESORAMIENTO TECNOLÓGICO		
Código del Subproceso:	DITIC-SU-SP1		
Descripción:	<p><b>PROPÓSITO:</b> Brindar asesoramiento en el ámbito tecnológico para optimizar de forma integral la infraestructura de la institución, tomando en cuenta las necesidades, presupuesto y las últimas tecnologías.</p> <p><b>ALCANCE:</b> Desde revisar el requerimiento solicitado por una unidad ejecutora, hasta analizar y remitir el informe técnico para su revisión.</p> <p><b>DISPARADOR:</b></p> <ul style="list-style-type: none"><li>• Requerimiento GLPI</li><li>• Correos Electrónicos</li><li>• Memorandos</li></ul> <p><b>PROVEEDORES:</b></p> <ul style="list-style-type: none"><li>• Procesos Sustantivos y Adjetivos</li><li>• Usuarios</li></ul> <p><b>INSUMOS:</b></p> <ul style="list-style-type: none"><li>• Requerimientos</li></ul>		
Clientes:	<ul style="list-style-type: none"><li>• Procesos Sustantivos y Adjetivos</li><li>• Usuarios</li></ul>		
Salidas:	<ul style="list-style-type: none"><li>• Informe técnico de asesoramiento tecnológico</li><li>• Tabla de especificaciones técnicas</li><li>• Términos de referencia</li></ul>		
Tipo de Proceso:	Adjetivo de asesoría.		
Responsable del Proceso:	Responsable de Gestión de Soporte a Usuarios		
Recursos:	<p><b>MATERIALES:</b></p> <ul style="list-style-type: none"><li>• Muebles de Oficina</li><li>• Insumos de Oficina</li><li>• Equipo de Oficina</li></ul> <p><b>HUMANOS:</b></p> <ul style="list-style-type: none"><li>• 1 Servidor Público 5</li></ul>		
Elaborado por:	Revisado por:	Aprobado /Autorizado por:	Registrado por:
PC	DIPLA - DITIC	DIREJ	DIPLA, PC

	<ul style="list-style-type: none"> <li>• 2 Servidores Públicos 3</li> <li>• 1 Servidor Público 2</li> <li>• 2 Servidores Públicos 1</li> </ul> <p><b>TECNOLÓGICOS:</b></p> <ul style="list-style-type: none"> <li>• Correo Electrónico.</li> <li>• Software de ofimática</li> <li>• Ordenadores</li> <li>• Impresoras</li> <li>• Sistema GLPI</li> </ul>
<b>Controles/Marco Legal:</b>	<ul style="list-style-type: none"> <li>• Anexo 1 del Acuerdo No. 166 del 19 de septiembre de 2013 (EGSI)</li> <li>• Normas de Control Interno de la Contraloría General del Estado</li> </ul>

### 6.1.2. CONTROLES DEL SUBPROCESO DE ASESORAMIENTO TECNOLÓGICO

#### Anexo 1 del Acuerdo No. 166 del 19 de septiembre de 2013 (EGSI)

#### 4.8. Devolución de activos.

b) Aplicar los debidos procesos para garantizar que toda la información generada por el empleado, contratista o usuario de terceras partes dentro de la institución, sea transferida, archivada o eliminada con seguridad.

#### Normas de Control Interno de la Contraloría General del Estado

- 410 TECNOLOGÍA DE LA INFORMACIÓN

- 410-01 Organización informática

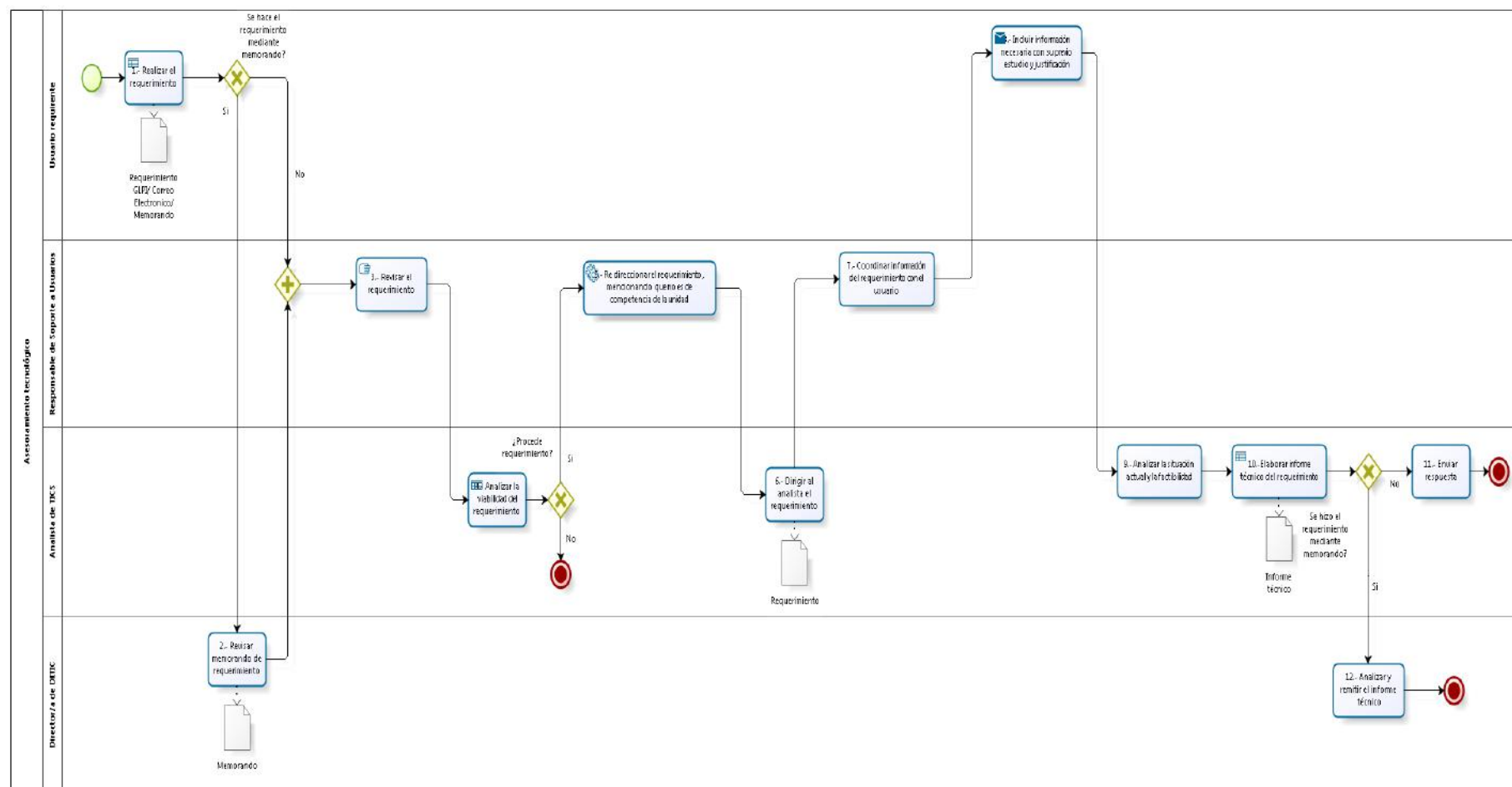
Las entidades y organismos del sector público deben estar acopladas en un marco de trabajo para procesos de tecnología de información que aseguren la transparencia y el control, así como el involucramiento de la alta dirección, por lo que las actividades y procesos de tecnología de información de la organización deben estar bajo la responsabilidad de una unidad que se encargue de regular y estandarizar los temas tecnológicos a nivel institucional.

- 410-12 Administración de soporte de tecnología de información.

La unidad de tecnología de información definirá, aprobará y difundirá procedimientos de operación que faciliten una adecuada administración del soporte tecnológico y garanticen la seguridad, integridad, confiabilidad y disponibilidad de los recursos y datos, tanto como la oportunidad de los servicios tecnológicos que se ofrecen.

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

### 6.1.3. DIAGRAMA DE FLUJO DEL SUBPROCESO DE ASESORAMIENTO TECNOLÓGICO



**Elaborado por:**  
PC

**Revisado por:**  
DIPLA - DITIC

**Aprobado /Autorizado por:**  
DIREJ

**Registrado por:**  
DIPLA, PC



#### 6.1.4. PROCEDIMIENTO DEL SUBPROCESO DE ASESORAMIENTO TECNOLÓGICO

Nº	Actividad	Detalle de la actividad	Responsable	Documento Generado
1	Realizar el requerimiento	Realizar el requerimiento a través de correo, memorando o mediante el GLPI	Usuario requirente	Requerimiento GLPI/ Correo Electrónico/ Memorando
	Decisión	<b>¿Se hace el requerimiento mediante memorando?</b> <b>SI:</b> Pasar a la actividad 2. Revisar memorando de requerimiento. <b>NO:</b> Pasar a la actividad 3. Revisar el requerimiento.	Responsable de Soporte a Usuarios	N/A
2	Revisar memorando de requerimiento	Revisa el memorando con el requerimiento solicitado por una unidad ejecutora de la institución	Director/a de DITIC	Memorando
3	Revisar el requerimiento	Revisa el requerimiento solicitado por una unidad ejecutora de la institución ya sea por el sistema GLPI, correo electrónico o memorando	Responsable de Soporte a Usuarios	N/A
4	Analizar la viabilidad del requerimiento	Analiza la viabilidad del requerimiento de una unidad ejecutora de la institución	Analista de TICS	N/A
	Decisión	<b>¿Procede requerimiento?</b> <b>SI:</b> Pasa a la actividad 6. Dirigir al analista el requerimiento. <b>NO:</b> Pasa a la actividad 5. Re direccionar el requerimiento.	Analista de TICS	N/A
5	Re direccionar el requerimiento , mencionando que no es de competencia de la unidad	Re direcciona el requerimiento, mencionando que no es de competencia de la unidad. <b>Fin del proceso.</b>	Analista de TICS	N/A
6	Dirigir al analista el requerimiento	Dirigir el requerimiento al analista de Soporte a Usuarios pertinente	Responsable de Soporte a Usuarios	Requerimiento GLPI/ Correo Electrónico/ Memorando
7	Coordinar información del requerimiento con el usuario	Coordina la información del requerimiento con el dueño del proceso	Analista de TICS	N/A
8	Incluir información necesaria con su previo estudio y justificación	Incluye la información necesaria con el previo estudio y justificativo	Usuario requirente	N/A

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

9	Analizar la situación actual y la factibilidad	Analiza la situación actual y la factibilidad de ejecución	Analista de TICS	N/A
10	Elaborar informe técnico del requerimiento	Elabora el informe técnico del requerimiento de una unidad ejecutora de la institución	Analista de TICS	Informe técnico
	Decisión	<b>¿Se hizo el requerimiento mediante memorando?</b> <b>SI:</b> Pasar a la actividad <b>12</b> . Analizar y remitir el informe técnico <b>NO:</b> Pasar a la actividad <b>11</b> . Enviar respuesta	Analista de TICS	N/A
11	Enviar respuesta	Solventar el requerimiento y enviar respuesta	Analista de TICS	N/A
12	Analizar y remitir el informe técnico	Analiza y remite el informe técnico para su verificación	Director/a de DITIC	N/A

#### 6.1.5. INDICADORES DEL SUBPROCESO DE ASESORAMIENTO TECNOLÓGICO

N°	Indicador	Fórmula de Cálculo	Unidad de Medida	Responsable de Medición	Fuente de Medición	Frecuencia de Medición
1	Porcentaje de requerimientos de asesoría información atendidos oportunamente	(Número de requerimientos atendidos oportunamente / Número de requerimientos solicitados)*100	Porcentaje	Jefe de Soporte a Usuarios	Informes técnicos, correos electrónicos y reportes del GLPI	Trimestral

#### 6.1.6. FORMATOS DEL SUBPROCESO DE ASESORAMIENTO TECNOLÓGICO

Nombre del Registro de Calidad	Código de Formato
Informe técnico	DITIC-SU-SP1-FOR-01

#### 6.1.7. ANEXOS DEL SUBPROCESO DE ASESORAMIENTO TECNOLÓGICO

“No hay anexos.”

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

## 6.2. SUBPROCESO DE MANTENIMIENTO PREVENTIVO DE EQUIPOS TECNOLÓGICOS

### 6.2.1. FICHA TÉCNICA DEL SUBPROCESO DE MANTENIMIENTO PREVENTIVO DE EQUIPOS TECNOLÓGICOS

<b>Proceso:</b>	GESTIÓN DE SOPORTE A USUARIOS
<b>Nombre del Subproceso:</b>	MANTENIMIENTO PREVENTIVO DE EQUIPOS TECNOLÓGICOS
<b>Código del Subproceso:</b>	DITIC-SU-SP2
<b>Descripción:</b>	<p><b>PROPÓSITO:</b> Garantizar el correcto funcionamiento de los equipos informáticos, planificando y coordinando de manera oportuna la revisión, reparación y /o cambio de piezas de acuerdo al estado de cada uno de los componentes del parque informático con el que cuenta la institución; con el fin de que las actividades de los funcionarios se realicen sin interrupciones.</p> <p><b>ALCANCE:</b> Desde coordinar con el funcionario el mantenimiento del equipo, hasta revisar y aprobar el informe.</p> <p><b>DISPARADOR:</b></p> <ul style="list-style-type: none"> <li>• Requerimiento GLPI</li> <li>• Correos Electrónicos</li> <li>• Plan de mantenimiento de equipos</li> </ul> <p><b>PROVEEDORES:</b></p> <ul style="list-style-type: none"> <li>• Director de Tecnologías de la Información y Comunicación</li> <li>• Almacén General</li> </ul> <p><b>INSUMOS:</b></p> <ul style="list-style-type: none"> <li>• Inventario de activos fijos</li> <li>• Plan de mantenimiento</li> </ul>
<b>Clientes:</b>	<ul style="list-style-type: none"> <li>• Procesos Sustantivos y Adjetivos</li> <li>• Jefe de Soporte a Usuarios</li> <li>• Director de Tecnologías de la Información y Comunicación</li> </ul>
<b>Salidas:</b>	<ul style="list-style-type: none"> <li>• Ficha de mantenimiento de equipos</li> <li>• Reporte de satisfacción del equipo</li> <li>• Informe de mantenimiento de equipos</li> </ul>
<b>Tipo de Proceso:</b>	Adjetivo
<b>Responsable del Proceso:</b>	Responsable de Gestión de Soporte a Usuarios
<b>Recursos:</b>	<p><b>MATERIALES:</b></p> <ul style="list-style-type: none"> <li>• Muebles de Oficina</li> <li>• Insumos de Oficina</li> </ul>

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

	<ul style="list-style-type: none"> <li>Equipo de Oficina: Aspiradora, Sopladora, Kit de mantenimiento, herramientas, pasta térmica</li> </ul> <p><b>HUMANOS:</b></p> <ul style="list-style-type: none"> <li>1 Servidor Público 5 (SP5)</li> <li>2 Servidores Públicos 3 (SP3)</li> <li>2 Servidor Público 1 (SP1)</li> <li>1 Servidor Público 2 (SP2)</li> </ul> <p><b>TECNOLÓGICOS:</b></p> <ul style="list-style-type: none"> <li>Hardware: Computador, impresoras</li> <li>Software: GLPI, Software de Ofimática, Mcafee, Utilitarios, Wise Care, C Cleaner</li> </ul>
<b>Controles/Marco Legal:</b>	<ul style="list-style-type: none"> <li>Anexo 1 del Acuerdo No. 166 del 19 de septiembre de 2013 (EGSI)</li> <li>Normas de Control Interno de la Contraloría General del Estado</li> </ul>

## 6.2.2. CONTROLES DEL SUBPROCESO DE MANTENIMIENTO PREVENTIVO DE EQUIPOS TECNOLÓGICO

### Anexo 1 del Acuerdo No. 166 del 19 de septiembre de 2013 (EGSI)

#### 5.10. Mantenimiento de los Equipos.

- Brindar mantenimientos periódicos a los equipos y dispositivos, de acuerdo a las especificaciones y recomendaciones del proveedor.
- Realizar el mantenimiento de los equipos únicamente con personal calificado y autorizado.
- Conservar los registros de los mantenimientos preventivos, correctivos y fallas relevantes o sospechosas.
- Establecer controles apropiados para realizar mantenimientos programados y emergentes.
- Gestionar mantenimientos planificados con hora de inicio, fin, impacto y responsables y poner previamente en conocimiento de administradores y usuarios finales.

### Normas de Control Interno de la Contraloría General del Estado

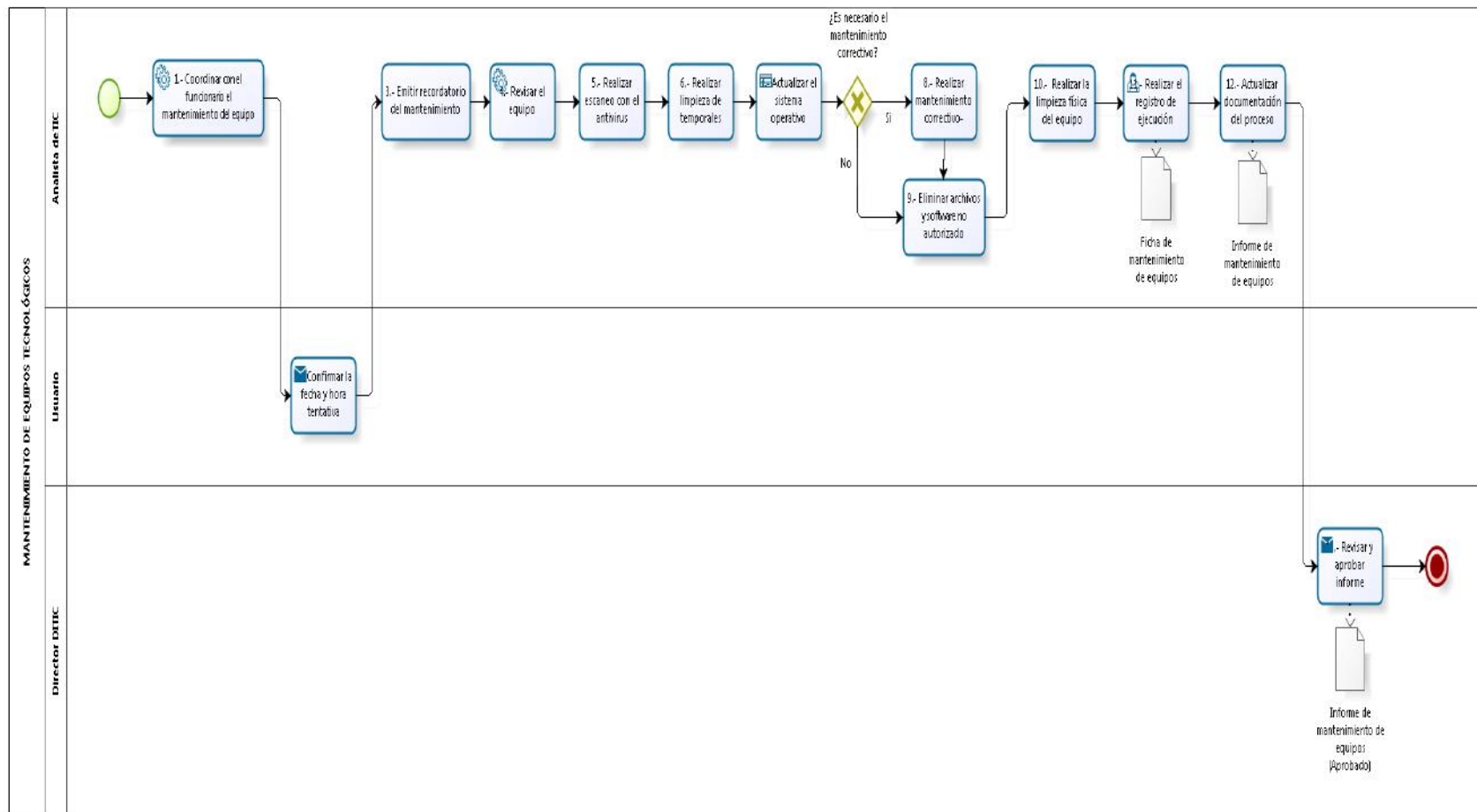
#### 410 TECNOLOGÍA DE LA INFORMACIÓN

##### 410-09 Mantenimiento y control de la infraestructura tecnológica informática

Las entidades y organismos del sector público deben estar acopladas en un marco de trabajo para procesos de tecnología de información que aseguren la transparencia y el control, así como el involucramiento de la alta dirección, por lo que las actividades y procesos de tecnología de información de la organización deben estar bajo la responsabilidad de una unidad que se encargue de regular y estandarizar los temas tecnológicos a nivel institucional.

<b>Elaborado por:</b>	<b>Revisado por:</b>	<b>Aprobado /Autorizado por:</b>	<b>Registrado por:</b>
PC	DIPLA - DITIC	DIREJ	DIPLA, PC

### 6.2.3. DIAGRAMA DE FLUJO DEL SUBPROCESO DE MANTENIMIENTO PREVENTIVO DE EQUIPOS TECNOLÓGICOS



<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

#### 6.2.4. PROCEDIMIENTO DEL SUBPROCESO DE MANTENIMIENTO PREVENTIVO DE EQUIPOS TECNOLÓGICOS

Nº	Actividad	Detalle de la actividad	Responsable	Documento Generado
1	Coordinar con el funcionario el mantenimiento del equipo	Coordina con el funcionario y comunica la fecha y hora tentativa para el mantenimiento. Continúa con la actividad 3	Analista de Soporte a Usuarios	N/A
	Confirmar la fecha y hora tentativa	El usuario confirma la fecha y hora para realizar el mantenimiento	Usuario	N/A
	Emitir recordatorio del mantenimiento	Envía mediante correo electrónico recordando que existe el mantenimiento el día previo al mantenimiento	Analista de Soporte a Usuarios	N/A
3	Revisar el equipo	Realiza la revisión del equipo para identificar su estado	Analista de Soporte a Usuarios	N/A
4	Realizar escaneo con el antivirus	Realiza el escaneo del equipo para verificar virus o amenazas.	Analista de Soporte a Usuarios	N/A
5	Realizar limpieza de temporales	Realiza la limpieza de los temporales del equipo de cómputo.	Analista de Soporte a Usuarios	N/A
6	Actualizar el sistema operativo	Realiza las actualizaciones de los parches tanto para el antivirus y las aplicaciones del equipo de cómputo, en esta instancia se determina si es necesario realizar un mantenimiento correctivo	Analista de Soporte a Usuarios	N/A
	Decisión	<b>¿Es necesario el mantenimiento correctivo?</b> <b>SI:</b> Pasa a la actividad 7. Realizar mantenimiento correctivo. <b>NO:</b> Pasa a la actividad 8. Eliminar archivos y software no autorizado	Analista de Soporte a Usuarios	N/A
7	Realizar mantenimiento correctivo	Como parte del mantenimiento correctivo se puede formatear el equipo o restaurar el sistema operativo	Analista de Soporte a Usuarios	N/A
8	Eliminar archivos y software no autorizado	Elimina los archivos y el software no autorizado a estar colocado en el equipo de computo	Analista de Soporte a Usuarios	N/A
9	Realizar física del equipo limpieza de Equipo	Realiza una revisión y análisis del estado del equipo de computo	Analista de Soporte a Usuarios	N/A
10	Realizar el registro de ejecución, fin	Realiza el registro de la ejecución realizada para constancia y cerrar el ticket en el GLPI	Analista de Soporte a Usuarios	Ficha de mantenimiento de equipos
11	Actualizar documentación del proceso	Actualiza la documentación de la gestión del proceso realizado	Analista de Soporte a Usuarios	Informe de mantenimiento de equipos
12	Revisar y aprobar informe	Analiza y aprueba el informe de mantenimientos preventivos y correctivos realizados de manera trimestral	Responsable de Soporte a Usuarios	Informe de mantenimiento de equipos (Aprobado)

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

### 6.2.5. INDICADORES DEL SUBPROCESO DE MANTENIMIENTO PREVENTIVO DE EQUIPOS TECNOLÓGICOS

N°	Indicador	Fórmula de Cálculo	Unidad de Medida	Responsable de Medición	Fuente de Medición	Frecuencia de Medición
1	Porcentaje de mantenimiento realizados a equipos de cómputo oportunamente	$(\text{Número de mantenimientos realizados oportunamente} / \text{Número de mantenimientos planificados}) * 100$	Porcentaje	Jefe de Gestión de Soporte a Usuarios	Informe de mantenimiento de equipos	Trimestral

### 6.2.6. FORMATOS DEL SUBPROCESO DE MANTENIMIENTO PREVENTIVO DE EQUIPOS TECNOLÓGICOS

Nombre del Registro de Calidad	Código de Formato
Ficha de mantenimiento de equipos	DITIC-SU-SP2-FOR-01
Informe de mantenimiento de equipos	DITIC-SU-SP2-FOR-02

### 6.2.7. ANEXOS DEL SUBPROCESO DE MANTENIMIENTO PREVENTIVO DE EQUIPOS TECNOLÓGICOS

“No hay anexos.”

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

### 6.3. SUBPROCESO DE SOPORTE TÉCNICO

#### 6.3.1. FICHA TÉCNICA DEL SUBPROCESO DE SOPORTE TÉCNICO

<b>Proceso:</b>	GESTIÓN DE SOPORTE A USUARIOS
<b>Nombre del Subproceso:</b>	SOPORTE TÉCNICO
<b>Código del Subproceso:</b>	DITIC-SU-SP3
<b>Descripción:</b>	<p><b>PROPÓSITO:</b> Brindar de manera oportuna e inmediata la asistencia técnica en respuesta a los requerimientos e incidencias generadas por los usuarios cotidianamente en problemas con los equipos; respaldando y asegurando la información que día a día es creada por el usuario.</p> <p><b>ALCANCE:</b> Desde analizar el requerimiento de la unidad ejecutora requirente, hasta revisar y aprobar el informe de atención de requerimientos.</p> <p><b>DISPARADOR:</b></p> <ul style="list-style-type: none"> <li>Requerimiento GLPI, Correo electrónico</li> </ul> <p><b>PROVEEDORES:</b></p> <ul style="list-style-type: none"> <li>Procesos Sustantivos y Adjetivos</li> </ul> <p><b>INSUMOS:</b></p> <ul style="list-style-type: none"> <li>Requerimientos</li> </ul>
<b>Clientes:</b>	<ul style="list-style-type: none"> <li>Procesos Sustantivos y Adjetivos</li> <li>Director DITIC</li> <li>Jefe de Soporte a Usuarios</li> </ul>
<b>Salidas:</b>	<ul style="list-style-type: none"> <li>Matriz de registro de respaldos de información</li> </ul>
<b>Tipo de Proceso:</b>	Adjetivo de asesoría.
<b>Responsable del Proceso:</b>	Responsable de Gestión de Soporte a Usuarios
<b>Recursos:</b>	<p><b>MATERIALES:</b></p> <ul style="list-style-type: none"> <li>Muebles de Oficina</li> <li>Insumos de Oficina</li> <li>Equipo de Oficina</li> <li>Herramientas tecnológicas</li> </ul> <p><b>HUMANOS:</b></p> <ul style="list-style-type: none"> <li>1 Servidor Público 5 (SP5)</li> <li>2 Servidores Públicos 3 (SP3)</li> <li>2 Servidor Público 1 (SP1)</li> <li>1 Servidor Público 2 (SP2)</li> </ul>

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------



	<b>TECNOLÓGICOS:</b> <ul style="list-style-type: none"> <li>Hardware: Computador, impresora</li> <li>Software: GLPI, Software de Ofimática</li> </ul>
<b>Controles/Marco Legal:</b>	<ul style="list-style-type: none"> <li>Anexo 1 del Acuerdo No. 166 del 19 de septiembre de 2013 (EGSI)</li> <li>Normas de Control Interno de la Contraloría General del Estado</li> </ul>

### 6.3.2. CONTROLES DEL SUBPROCESO DE SOPORTE TÉCNICO

#### Anexo 1 del Acuerdo No. 166 del 19 de septiembre de 2013 (EGSI)

##### 3.1. Mantenimiento de los Equipos.

a) Brindar mantenimientos periódicos a los equipos y dispositivos, de acuerdo a las especificaciones y recomendaciones del proveedor.

#### Normas de Control Interno de la Contraloría General del Estado

### 4. SEGURIDAD DE LOS RECURSOS HUMANOS.

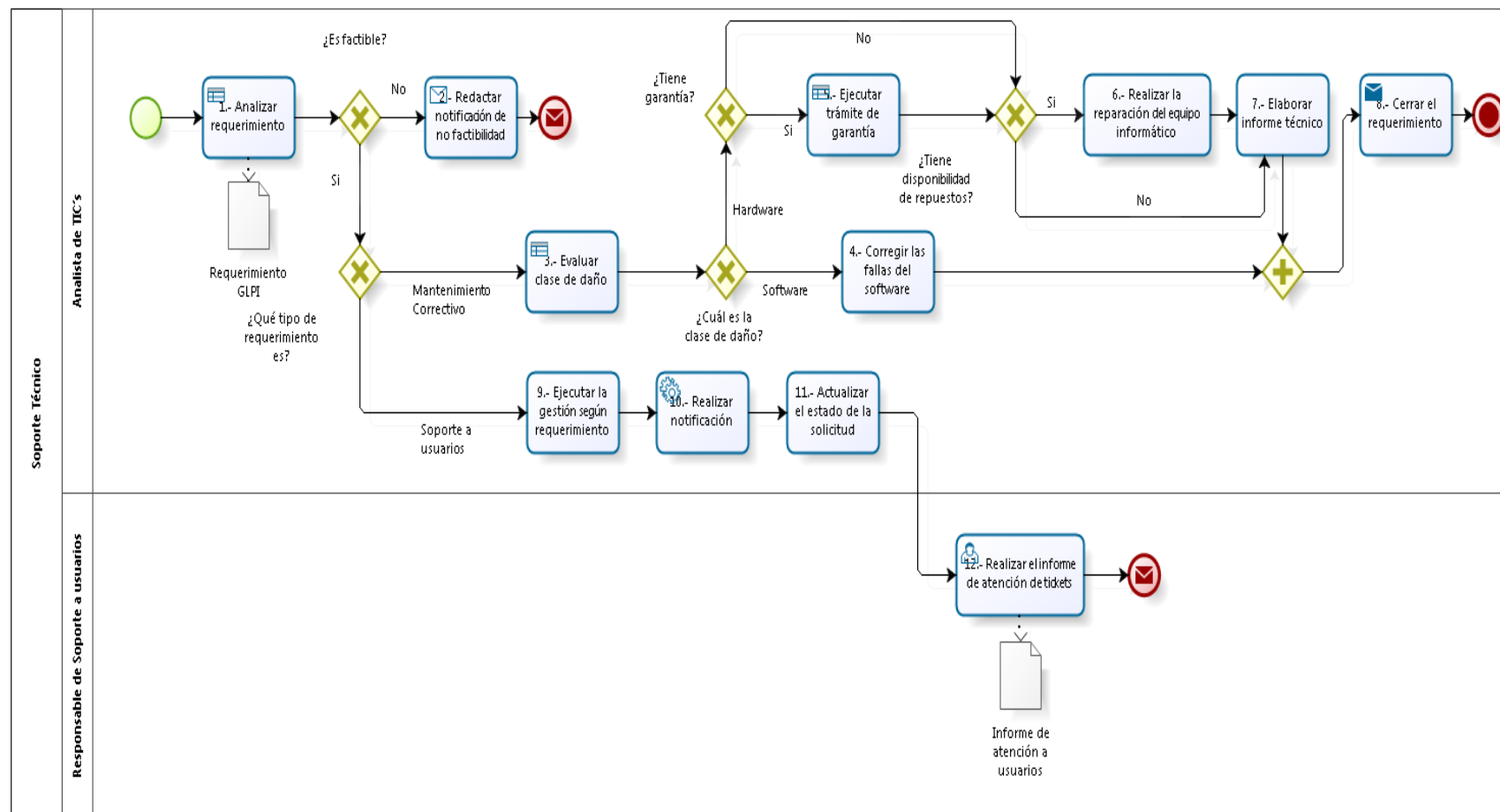
#### 410-01 Organización informática

Las entidades y organismos del sector público deben estar acopladas en un marco de trabajo para procesos de tecnología de información que aseguren la transparencia y el control, así como el involucramiento de la alta dirección, por lo que las actividades y procesos de tecnología de información de la organización deben estar bajo la responsabilidad de una unidad que se encargue de regular y estandarizar los temas tecnológicos a nivel institucional.

.

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

### 6.3.3. DIAGRAMA DE FLUJO DEL SUBPROCESO DE SOPORTE TÉCNICO



**Elaborado por:**  
PC

**Revisado por:**  
DIPLA - DITIC

**Aprobado /Autorizado por:**  
DIREJ

**Registrado por:**  
DIPLA, PC

#### 6.3.4. PROCEDIMIENTO DEL SUBPROCESO DE SOPORTE TÉCNICO

Nº	Actividad	Detalle de la actividad	Responsable	Documento Generado
1	Analizar requerimiento	Recibe y analiza el requerimiento de la unidad ejecutora requirente	Analista de Soporte a Usuarios	Requerimiento GLPI
	Decisión	<b>¿Es factible?</b> <b>SI:</b> Pasa a la siguiente decisión, <b>¿Qué tipo de requerimiento es?</b> <b>NO:</b> Redactar notificación, fin	Analista de Soporte a Usuarios	N/A
2	Redactar notificación de no factibilidad	Genera la notificación de no factibilidad y comunica al área requirente	Analista de Soporte a Usuarios	N/A
	Decisión	<b>¿Qué tipo de requerimiento es?</b> <b>MANTENIMIENTO CORRECTIVO</b> - Pasa a la actividad 3. <b>SOPORTE A USUARIO</b> - Pasa a la actividad 9	Analista de Soporte a Usuarios	N/A
3	<b>MANTENIMIENTO CORRECTIVO,</b> Evaluar clase de daño	Revisa el tipo de daño	Analista de Soporte a Usuarios	N/A
	Decisión	<b>¿Cuál es la clase de daño?</b> <b>Software:</b> Corrige las fallas del software, pasa a la actividad 4. <b>Hardware:</b> Continúa con la decisión. <b>¿Tiene garantía?</b>	Analista de Soporte a Usuarios	N/A
4	Corregir las fallas del software	Corrige las fallas del software dependiendo de las fallas detectadas. Continúa con la actividad 8	Analista de Soporte a Usuarios	N/A
	Decisión	<b>¿Tiene garantía?</b> <b>SI:</b> Ejecutar trámite de garantía, pasa a la actividad 5 <b>NO:</b> Continúa con la decisión: <b>¿Tiene disponibilidad de repuestos?</b>	Analista de Soporte a Usuarios	N/A
5	Ejecutar trámite de garantía	Ejecuta el trámite de la garantía del equipo de cómputo. Continúa con la actividad 7.	Analista de Soporte a Usuarios	N/A
	Decisión	<b>¿Tiene disponibilidad de repuestos?</b> <b>No:</b> Elaborar informe técnico, pasa a la actividad 7. <b>Si:</b> Elaborar la reparación del equipo informático 6.	Analista de Soporte a Usuarios	N/A
6	Realizar la reparación del equipo informático	Ejecuta la reparación del equipo informático según el análisis realizado. Continúa con la actividad 7.	Analista de Soporte a Usuarios	N/A
7	Elaborar informe técnico	Elabora el informe técnico de acuerdo a la acciones realizadas en los equipos de computo	Analista de Soporte a Usuarios	Informe técnico

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

8	Cerrar el requerimiento	Cierra el requerimiento	Analista de Soporte a Usuarios	N/A
9	<b>SOPORTE A USUARIOS</b> Ejecutar la gestión según requerimiento	Ejecuta la gestión según el requerimiento recibido	Analista de Soporte a Usuarios	N/A
10	Realizar notificación	Realiza la notificación del soporte al usuario realizado mediante correo electrónico	Analista de Soporte a Usuarios	N/A
11	Actualizar el estado de la solicitud	Actualiza el estado del ticket indicando la solución y se lo cierra	Analista de Soporte a Usuarios	N/A
12	Realizar el informe de atención de tickets	Realiza un informe trimestral del número de tickets realizados trimestralmente.	Responsable de Soporte a usuarios	Informe de atención a usuarios

#### 6.3.5. INDICADORES DEL SUBPROCESO DE SOPORTE TÉCNICO

N°	Indicador	Fórmula de Cálculo	Unidad de Medida	Responsable de Medición	Fuente de Medición	Frecuencia de Medición
1	Porcentaje de requerimientos tecnológicos atendidos	$(\text{Número de requerimientos atendidos} / \text{Número de requerimientos solicitados}) * 100$	Porcentaje	Jefe de Soporte a Usuarios	Reporte de requerimientos GLPI	Trimestral

#### 6.3.6. FORMATOS DEL SUBPROCESO DE SOPORTE TÉCNICO

Nombre del Registro de Calidad	Código de Formato
Informe técnico	DITIC-SU-SP3-FOR-01
Informe de atención a usuarios	DITIC-SU-SP3-FOR-02

#### 6.3.7. ANEXOS DEL SUBPROCESO DE SOPORTE TÉCNICO

“No hay anexos.”

Elaborado por: PC	Revisado por: DIPLA - DITIC	Aprobado /Autorizado por: DIREJ	Registrado por: DIPLA, PC
----------------------	--------------------------------	------------------------------------	------------------------------

## 6.4. SUBPROCESO DE INVENTARIO TECNOLÓGICO

### 6.4.1. FICHA TÉCNICA DEL SUBPROCESO DE INVENTARIO TECNOLÓGICO

Proceso:	GESTIÓN DE SOPORTE A USUARIOS		
Nombre del Subproceso:	INVENTARIO TECNOLÓGICO		
Código del Subproceso:	DITIC-SU-SP4		
Descripción:	<p><b>PROPÓSITO:</b> Conocer y mantener actualizado, cuantitativamente y cualitativamente el estado y ubicación de los equipos informáticos asignados a cada funcionario de la institución, de manera consistente y detallada que a futuro sirva de precedente para poder tomar decisiones de forma oportuna, clara y eficiente.</p> <p><b>ALCANCE:</b> El proceso inicia desde la consolidación y registro de las fichas de control de equipos tecnológicos hasta la generación del informe de ejecución del inventario de equipos tecnológicos.</p> <p><b>DISPARADOR:</b></p> <ul style="list-style-type: none"><li>• Norma de control Interno Control Interno, EGSI, Norma de la Contraloría General del Estado</li></ul> <p><b>PROVEEDORES:</b></p> <ul style="list-style-type: none"><li>• Subproceso de Soporte a Usuarios</li><li>• Subproceso de Mantenimiento de Equipos Tecnológicos</li><li>• Dirección Administrativa.</li></ul> <p><b>INSUMOS:</b></p> <ul style="list-style-type: none"><li>• Estado operativo de los equipos</li><li>• Actualización o cambio de partes en los equipos</li><li>• Listado de bienes tecnológicos</li></ul>		
Clientes:	<ul style="list-style-type: none"><li>• Dirección Ejecutiva</li></ul>		
Salidas:	<ul style="list-style-type: none"><li>• Inventario Tecnológico para conciliar</li></ul>		
Tipo de Proceso:	Adjetivo de asesoría.		
Responsable del Proceso:	Responsable de Gestión de Soporte a Usuarios		
Recursos:	<p><b>MATERIALES:</b></p> <ul style="list-style-type: none"><li>• Muebles de Oficina</li><li>• Insumos de Oficina</li><li>• Equipo de Oficina</li></ul> <p><b>HUMANOS:</b></p> <ul style="list-style-type: none"><li>• 1 Servidor Público 1</li><li>• 1 Servidor Público 5</li></ul>		
Elaborado por:	Revisado por:	Aprobado /Autorizado por:	Registrado por:
PC	DIPLA - DITIC	DIREJ	DIPLA, PC

	<b>TECNOLÓGICOS:</b> <ul style="list-style-type: none"> <li>• Hardware: Computador, impresora</li> <li>• Software: GLPI, Office</li> <li>• Pistola de código de barras</li> <li>• Sistema de control de inventario OCS</li> </ul>
<b>Controles/Marco Legal:</b>	<ul style="list-style-type: none"> <li>• 410-09 Mantenimiento y control de infraestructura tecnológica NCI Contraloría</li> <li>• Capítulo 3 Gestión de Activos, de Hardware, Software y Redes- EGSi</li> </ul>

#### 6.4.2. CONTROLES DEL SUBPROCESO DE INVENTARIO TECNOLÓGICO

##### Anexo 1 del Acuerdo No. 166 del 19 de septiembre de 2013 (EGSI)

##### 3.1. Gestión de activos.

Inventariar los activos de soporte de Hardware (\*):

j) Equipos móviles: teléfono inteligente (smartphone), teléfono celular, tableta, computador portátil, asistente digital personal (PDA), etc.

k) Equipos fijos: servidor de torre, servidor de cuchilla, servidor de rack, computador de escritorio, computadoras portátiles, etc.

l) Periféricos de entrada: teclado, ratón, micrófono, escáner plano, escáner de mano, cámara digital, cámara web, lápiz óptico, pantalla de toque, etc.

m) Periféricos de salida: monitor, proyector, audífonos, parlantes, impresora láser, impresora de inyección de tinta, impresora matricial, impresora térmica, plotter, máquina de fax, etc.

n) Periféricos y dispositivos de almacenamiento: sistema de almacenamiento (NAS, SAN), librería de cintas, cintas magnéticas, disco duro portátil, disco flexible, grabador de discos (CD, DVD, Blu-ray), CD, DVD, Blu-ray, memoria USB, etc.

o) Periféricos de comunicaciones: tarjeta USB para redes inalámbricas (Wi-Fi, Bluetooth, GPRS, HSDPA), tarjeta PCMCIA para redes inalámbricas (Wi-Fi, Bluetooth, GPRS, HSDPA), tarjeta USB para redes alámbricas/inalámbricas de datos y de telefonía, etc.

p) Tableros: de transferencia (bypass) de la unidad interrumpible de energía (UPS), de salidas de energía eléctrica, de transferencia automática de energía, etc.

r) Sistemas operativos.

t) Paquetes de software o software base de: suite de ofimática, navegador de Internet, cliente de correo electrónico, mensajería instantánea, edición de imágenes, video conferencia, servidor (proxy, de archivos, de correo electrónico, de impresiones, de mensajería instantánea, de aplicaciones, de base de datos), etc.

u) Aplicativos informáticos del negocio.

##### 5.12. Seguridad en la reutilización o eliminación de los equipos.

b) Evaluar los dispositivos deteriorados que contengan información sensible antes de enviar a reparación, borrar la información o determinar si se debería eliminar físicamente el dispositivo.

<b>Elaborado por:</b>	<b>Revisado por:</b>	<b>Aprobado /Autorizado por:</b>	<b>Registrado por:</b>
PC	DIPLA - DITIC	DIREJ	DIPLA, PC



#### **Normas de Control Interno de la Contraloría General del Estado**

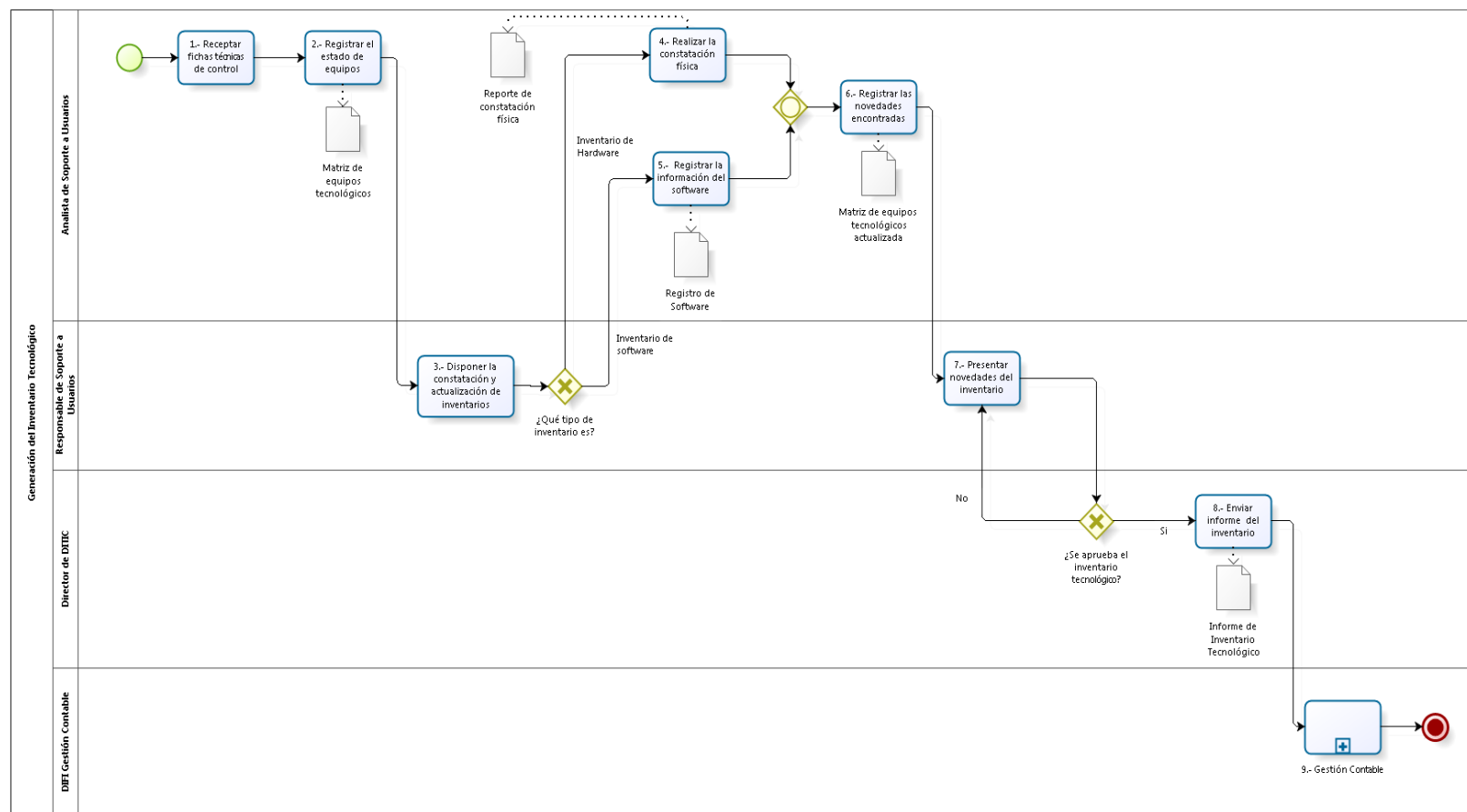
#### **4. SEGURIDAD DE LOS RECURSOS HUMANOS.**

##### **410-01 Organización informática**

Las entidades y organismos del sector público deben estar acopladas en un marco de trabajo para procesos de tecnología de información que aseguren la transparencia y el control, así como el involucramiento de la alta dirección, por lo que las actividades y procesos de tecnología de información de la organización deben estar bajo la responsabilidad de una unidad que se encargue de regular y estandarizar los temas tecnológicos a nivel institucional.

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

### 6.4.3. DIAGRAMA DE FLUJO DEL SUBPROCESO DE INVENTARIO TECNOLÓGICO



**Elaborado por:**  
PC

**Revisado por:**  
DIPLA - DITIC

**Aprobado /Autorizado por:**  
DIREJ

**Registrado por:**  
DIPLA, PC



#### 6.4.4. PROCEDIMIENTO DEL SUBPROCESO DE INVENTARIO TECNOLÓGICO

Nº	Actividad	Detalle de la actividad	Responsable	Documento Generado
1	Receptar fichas técnicas de control	Recepta las fichas técnicas de control de revisión y mantenimiento de equipos tecnológicos incluye Hardware y Software.	Analista de Soporte a Usuarios	N/A
2	Registrar el estado de equipos	Registra y actualiza en la matriz de estado de equipos tecnológicos.	Analista de Soporte a Usuarios	Matriz de equipos tecnológicos
3	Disponer la constatación y actualización de inventarios	Dispone al analista la constatación y actualización de inventarios	Responsable de Soporte a Usuarios	N/A
	Decisión	<b>¿Qué tipo de inventario es?</b> <b>INVENTARIO DE HARDWARE</b> - Pasa a la actividad 4 <b>INVENTARIO DE SOFTWARE</b> - Pasa a la actividad 5	Responsable de Soporte a Usuarios	N/A
4	Realizar la constatación física	<b>INVENTARIO DE HARDWARE</b> Realiza la constatación física, la misma que consiste en verificar los datos de la matriz vs las características de los equipos y detalla las novedades encontradas. Continúa con la actividad 6	Analista de Soporte a Usuarios	Reporte de constatación física
5	Registrar la información de software	<b>INVENTARIO DE SOFTWARE</b> Registra la información de softwares mediante el OCS, cuando son software varias, para el caso de las aplicaciones INEC se registra el LINK, el contacto de soporte en planta central y el objetivo de la aplicación	Analista de Soporte a Usuarios	Registro de Software
6	Registrar las novedades encontradas	Registra y actualiza la matriz con las novedades encontradas en la constatación física y en registro de software	Analista de Soporte a Usuarios	Matriz de equipos tecnológicos actualizada
7	Presentar novedades del inventario	Presenta al director de DITIC las novedades identificadas en el inventario tecnológico preliminar	Analista de Soporte a Usuarios	N/A
	Decisión	<b>¿Se aprueba el inventario tecnológico?</b> <b>SI:</b> Pasa a la actividad 8. Disponer las acciones pertinentes. <b>No:</b> Regresa a la actividad 6. Registrar las novedades encontradas.	Director de DITIC	N/A
8	Enviar informe del inventario	Envía el informe del inventario a DIFI Gestión Contable para su conciliación	Director de DITIC	Informe de Inventario Tecnológico
9	Gestión Contable	SUBPROCESO PREDEFINIDO: Análisis y registro para la conciliación de bienes de larga duración y bienes de control	DIFI Gestión Contable	N/A

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

#### 6.4.5. INDICADORES DEL SUBPROCESO DE INVENTARIO TECNOLÓGICO

N°	Indicador	Fórmula de Cálculo	Unidad de Medida	Responsable de Medición	Fuente de Medición	Frecuencia de Medición
1	Número de equipos operativos disponibles	Número de equipos operativos disponibles	Número	Jefe de Soporte Técnico	Informe de inventario tecnológico	Anual

#### 6.4.6. FORMATOS DEL SUBPROCESO DE INVENTARIO TECNOLÓGICO

Nombre del Registro de Calidad	Código de Formato
Inventario de Equipos tecnológicos	DITIC-SU-SP4-FOR-01

#### 6.4.7. ANEXOS DEL SUBPROCESO DE INVENTARIO TECNOLÓGICO

“No hay anexos.”

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

## 6.5. SUBPROCESO DE GESTIÓN DEL PARQUE INFORMÁTICO

### 6.5.1. FICHA TÉCNICA DEL SUBPROCESO DE GESTIÓN DEL PARQUE INFORMÁTICO

<b>Proceso:</b>	GESTIÓN DE SOPORTE A USUARIOS
<b>Nombre del Subproceso:</b>	GESTIÓN DEL PARQUE INFORMÁTICO
<b>Código del Subproceso:</b>	DITIC-SU-SP5
<b>Descripción:</b>	<p><b>PROPÓSITO:</b> Gestionar la correcta distribución y/o re-distribución de los equipos informáticos según sea el caso de tal manera que los equipos asignados a los usuarios se ajusten a las necesidades de cada uno de ellos con el propósito de obtener el máximo rendimiento de los equipos y el mejor desarrollo del trabajo de los funcionarios de la Institución.</p> <p><b>ALCANCE:</b> Desde Elaborar requerimiento del equipo informático, hasta recibir y archivar informe técnico</p> <p><b>DISPARADOR:</b></p> <ul style="list-style-type: none"> <li>• Norma de control Interno Control Interno,</li> <li>• EGSi</li> </ul> <p><b>PROVEEDORES:</b></p> <ul style="list-style-type: none"> <li>• Coordinación Administrativa Financiera</li> </ul> <p><b>INSUMOS:</b></p> <ul style="list-style-type: none"> <li>• Parque informático</li> </ul>
<b>Clientes:</b>	<ul style="list-style-type: none"> <li>• Procesos sustantivos y adjetivos del INEC</li> </ul>
<b>Salidas:</b>	<ul style="list-style-type: none"> <li>• Parque informático Gestionado</li> </ul>
<b>Tipo de Proceso:</b>	Adjetivo de asesoría.
<b>Responsable del Proceso:</b>	Responsable de Gestión de Soporte a Usuarios
<b>Recursos:</b>	<p><b>MATERIALES:</b></p> <ul style="list-style-type: none"> <li>• Muebles de Oficina</li> <li>• Insumos de Oficina</li> <li>• Equipo de Oficina</li> </ul> <p><b>HUMANOS:</b></p> <ul style="list-style-type: none"> <li>• 1 Servidor Público 5 (SP5)</li> <li>• 2 Servidores Públicos 3 (SP3)</li> <li>• 2 Servidor Público 1 (SP1)</li> <li>• 1 Servidor Público 2 (SP2)</li> </ul> <p><b>TECNOLÓGICOS:</b></p>

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

	<ul style="list-style-type: none"> <li>• Hardware: Computador, impresora</li> <li>• Software: GLPI.</li> <li>• Software de Ofimática</li> </ul>
<b>Controles/Marco Legal:</b>	<ul style="list-style-type: none"> <li>• 410-09 Mantenimiento y control de infraestructura tecnológica NCI Contraloría</li> <li>• Capítulo 3 Gestión de Activos, de Hardware, Software y Redes- EGSi</li> </ul>

## 6.5.2. CONTROLES DEL SUBPROCESO DE GESTIÓN DEL PARQUE INFORMÁTICO

### Anexo 1 del Acuerdo No. 166 del 19 de septiembre de 2013 (EGSI)

- **6.2. Gestión del Cambio.**

h) Establecer responsables y procedimientos formales del control de cambios en los equipos y software. Los cambios deben efectuarse únicamente cuando haya razón válida para el negocio, como: cambio de versión, corrección de vulnerabilidades, costos, licenciamiento, nuevo hardware, etc.

- **6.3. Distribución de Funciones**

a) Distribuir las funciones y las áreas de responsabilidad, para reducir oportunidades de modificaciones no autorizadas, no intencionales, o el uso inadecuado de los activos de la institución.

b) Limitar el acceso a modificar o utilizar los activos sin su respectiva autorización.

### Normas de Control Interno de la Contraloría General del Estado

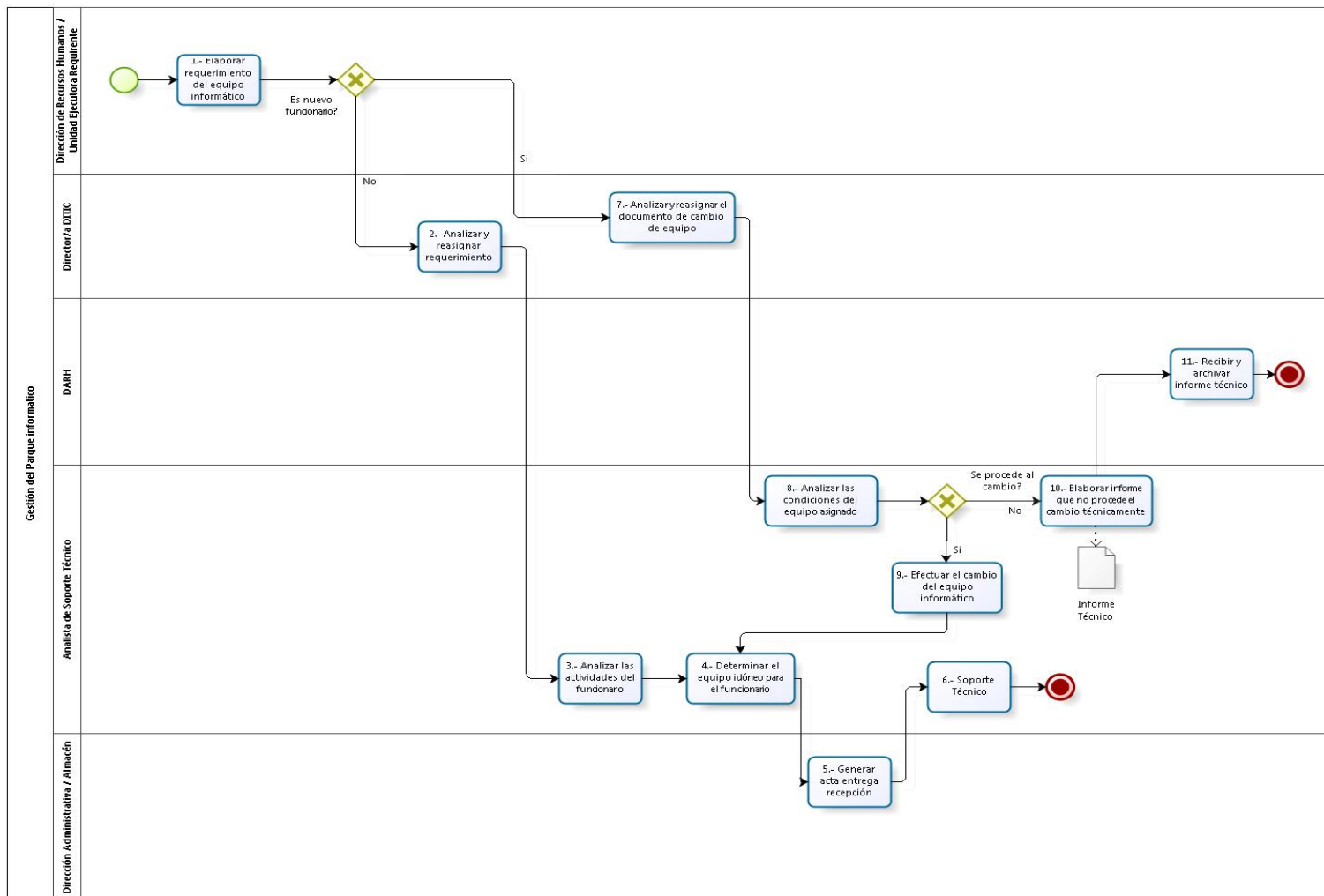
- **4. SEGURIDAD DE LOS RECURSOS HUMANOS.**

- **410-02 Segregación de funciones**

Las funciones y responsabilidades del personal de tecnología de información y de los usuarios de los sistemas de información serán claramente definidas y formalmente comunicadas para permitir que los roles y responsabilidades asignados se ejerzan con suficiente autoridad y respaldo.

Elaborado por: PC	Revisado por: DIPLA - DITIC	Aprobado /Autorizado por: DIREJ	Registrado por: DIPLA, PC
----------------------	--------------------------------	------------------------------------	------------------------------

### 6.5.3. DIAGRAMA DE FLUJO DEL SUBPROCESO DE GESTIÓN DEL PARQUE INFORMÁTICO



Elaborado por:	Revisado por:	Aprobado /Autorizado por:	Registrado por:
PC	DIPLA - DITIC	DIREJ	DIPLA, PC

#### 6.5.4. PROCEDIMIENTO DEL SUBPROCESO DE GESTIÓN DEL PARQUE INFORMÁTICO

Nº	Actividad	Detalle de la actividad	Responsable	Documento Generado
1	Elaborar requerimiento del equipo informático	Realiza el requerimiento del equipo informático según necesidad de la unidad ejecutora	Dirección de Recursos Humanos / Unidad Ejecutora Requirente	N/A
	Decisión	<b>¿Es nuevo funcionario?</b> <b>SI:</b> Pasa a la actividad <b>2</b> . Analiza y reasigna requerimiento. <b>NO:</b> Pasa a la actividad <b>7</b> . Analiza y reasigna el documento de cambio de equipo.	Dirección de Recursos Humanos / Unidad Ejecutora Requirente	N/A
2	Analizar y reasignar requerimiento	Realiza el análisis del requerimiento y reasignarlo para su gestión	Director de DITIC	N/A
3	Analizar las actividades del funcionario	Analiza las actividades del funcionario para entender que equipo tecnológico necesita	Analista de Soporte Técnico	N/A
4	Determinar el equipo idóneo para el funcionario	Determina el equipo idóneo para el funcionario	Analista de Soporte Técnico	N/A
5	Generar acta entrega recepción	Genera el acta de entrega recepción para detallar lo entregado	Dirección Administrativa / Almacén	Acta
6	Soporte Técnico, fin	Detalle de actividades en el subproceso Soporte técnico. Fin.	Dirección Administrativa / Almacén	N/A
7	Analizar y reasignar el documento de cambio de equipo	Analiza y reasigna el documento de cambio de equipo según su estado	Director de DITIC	N/A
8	Analizar las condiciones del equipo asignado	Analiza las condiciones del equipo que se va a asignar al servidor público	Analista de Soporte Técnico	N/A
	Decisión	<b>¿Se procede al cambio?</b> <b>SI,</b> Efectúa el cambio del equipo informático, pasa a la actividad <b>9</b> <b>NO,</b> Elabora informe que no procede el cambio técnicamente, pasa a la actividad <b>10</b>	Analista de Soporte Técnico	N/A

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

9	Efectuar el cambio del equipo informático	Efectúa el cambio del equipo informático en función de su estado. Regresa a la actividad 4.	Analista de Soporte Técnico	N/A
10	Elaborar informe que no procede el cambio técnicamente	Elabora el informe que no procede en el cambio que técnicamente es difícil de ejecución	Analista de Soporte Técnico	Informe técnico
11	Recibir y archivar informe técnico	Recibe y archiva el informe técnico con el fin de mantener registrada la información	Dirección de Recursos Humanos / Unidad Ejecutora Requiriente	N/A

#### 6.5.5. INDICADORES DEL SUBPROCESO DE GESTIÓN DEL PARQUE INFORMÁTICO

N°	Indicador	Fórmula de Cálculo	Unidad de Medida	Responsable de Medición	Fuente de Medición	Frecuencia de Medición
1	Porcentaje de equipos asignados	$(\text{Número de equipos asignados} / \text{Número de equipos requeridos}) * 100$	Porcentaje	Jefe de Soporte a Usuarios	Inventario de Equipos tecnológicos	Trimestral

#### 6.5.6. FORMATOS DEL SUBPROCESO DE GESTIÓN DEL PARQUE INFORMÁTICO

Nombre del Registro de Calidad	Código de Formato
DITIC-SU-SP4-FOR-01	Informe Técnico

#### 6.5.7. ANEXOS DEL SUBPROCESO DE GESTIÓN DEL PARQUE INFORMÁTICO

“No hay anexos.”

Elaborado por: PC	Revisado por: DIPLA - DITIC	Aprobado /Autorizado por: DIREJ	Registrado por: DIPLA, PC
----------------------	--------------------------------	------------------------------------	------------------------------

## 7. DESCRIPCIÓN DE PROCESOS DE GESTIÓN DE SEGURIDAD INFORMÁTICA, INTEROPERABILIDAD Y RIESGOS

### 7.1. SUBPROCESO DE DESARROLLO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

#### 7.1.1. FICHA TÉCNICA DEL SUBPROCESO DE DESARROLLO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

<b>Proceso:</b>	GESTIÓN DE SEGURIDAD INFORMÁTICA, INTEROPERABILIDAD Y RIESGOS
<b>Nombre del Subproceso:</b>	DESARROLLO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA
<b>Código del Subproceso:</b>	DITIC-SI-SP1
<b>Descripción:</b>	<p><b>PROPÓSITO:</b>            Contar con políticas de seguridad informática internas que ayuden a garantizar la seguridad, confidencialidad y disponibilidad de la información, y a su vez puedan ser entendidas y ejecutadas por todos los funcionarios a las que van dirigidos.</p> <p><b>ALCANCE:</b>            Diferenciar el tipo de solicitud, hasta socializar la política aprobada</p> <p><b>DISPARADOR:</b></p> <ul style="list-style-type: none"> <li>• Memorando</li> <li>• Correo electrónico.</li> </ul> <p><b>PROVEEDORES:</b></p> <ul style="list-style-type: none"> <li>• Dirección DITIC</li> <li>• Oficial de Seguridad</li> </ul> <p><b>INSUMOS:</b></p> <ul style="list-style-type: none"> <li>• Parámetros</li> <li>• Directrices</li> </ul>
<b>Clientes:</b>	<ul style="list-style-type: none"> <li>• Procesos sustantivos y adjetivos del INEC</li> </ul>
<b>Salidas:</b>	<ul style="list-style-type: none"> <li>• Políticas de seguridad informática</li> <li>• Procedimientos de seguridad informática</li> </ul>
<b>Tipo de Proceso:</b>	Adjetivo de asesoría.
<b>Responsable del Proceso:</b>	Responsable de la Unidad de Seguridad Informática, Interoperabilidad y Riesgos
<b>Recursos:</b>	<p><b>MATERIALES:</b></p> <ul style="list-style-type: none"> <li>• Muebles de Oficina</li> <li>• Insumos de Oficina</li> <li>• Equipo de Oficina</li> </ul> <p><b>HUMANOS:</b></p> <ul style="list-style-type: none"> <li>• 1 Servidor Público 7</li> </ul>

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------



	<ul style="list-style-type: none"> <li>1 Servidor Público 3</li> </ul> <p><b>TECNOLÓGICOS:</b></p> <ul style="list-style-type: none"> <li>Hardware (Computadores, impresoras)</li> <li>Software</li> <li>Software de ofimática</li> </ul>
<b>Controles/Marco Legal:</b>	<ul style="list-style-type: none"> <li>Registro Oficial N° 88 – Acuerdo 166 – art.1 art.2 art.3 art.4 art.5 art.6 art.7</li> <li>Norma de Control Interno de la Contraloría General del Estado – 410-04 Políticas y procedimientos</li> <li>Norma de Control Interno de la Contraloría General del Estado – 410-14 Sitio web, servicios de internet e intranet</li> <li>Norma de Control Interno de la Contraloría General del Estado – 410-17 Firmas electrónicas</li> <li>Resolución N° 30 DIREJ-DIJU-NI-2012</li> </ul>

## 7.1.2. CONTROLES DEL SUBPROCESO DE DESARROLLO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

### . Registro Oficial N° 88 – Acuerdo 166

#### 1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

##### 1.1. Documento de la Política de la Seguridad de la Información

**a)** La máxima autoridad de la institución dispondrá la implementación de este Esquema Gubernamental de Seguridad de la Información (EGSI) en su entidad (\*).

**b)** Se difundirá la siguiente política de seguridad de la información como referencia (\*):

“Las entidades de la Administración Pública Central, Dependiente e Institucional que generan, utilizan, procesan, comparten y almacenan información en medio electrónico o escrito, clasificada como pública, confidencial, reservada y no reservada, deberán aplicar el Esquema Gubernamental de Seguridad de la Información para definir los procesos, procedimientos y tecnologías a fin de garantizar la confidencialidad, integridad y disponibilidad de esa información, en los medios y el tiempo que su legitimidad lo requiera”.

Las entidades públicas podrán especificar una política de seguridad más amplia o específica en armonía con la Constitución, leyes y demás normativa legal propia o relacionada así como su misión y competencias.

#### 4.8. Devolución de activos

a) Formalizar el proceso de terminación del contrato laboral, para incluir la devolución de software, documentos corporativos y los equipos. También es necesaria la devolución de otros activos de la institución tales como los dispositivos de cómputo móviles, tarjetas de crédito, las tarjetas de acceso, tokens USB con certificados de electrónicos, certificados electrónicos en archivo, memorias flash, teléfonos celulares, cámaras, manuales, información almacenada en medios electrónicos y otros estipulados en las políticas internas de cada entidad.

#### 6.19. Políticas y procedimientos para el intercambio de información.

a) Establecer procedimientos para proteger la información intercambiada contra la interpretación, copiado, modificación, enrutamiento y destrucción.

b) Definir procedimientos para detección y protección contra programas maliciosos, cuando se utilizan comunicaciones electrónicas.

c) Proteger la información sensible que se encuentra en forma de adjunto.

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

- d) Establecer directrices para el uso de los servicios de comunicación electrónica.
- e) Definir procedimientos para el uso de las redes inalámbricas en base a los riesgos involucrados.
- f) Establecer responsabilidades de empleados, contratistas y cualquier otro usuario de no comprometer a la institución con un mal uso de la información.
- g) Establecer controles por medio de técnicas criptográficas.
- h) Definir directrices de retención y eliminación de la correspondencia incluyendo mensajes, según la normativa legal local.
- i) No dejar información sensible en copiadoras, impresoras, fax, contestadores, etc.
- j) No revelar información sensible al momento de tener una conversación telefónica o mantener conversaciones sin tomar los controles necesarios.
- k) No dejar datos demográficos al alcance de cualquier persona, como los correos electrónicos, ya que se puede hacer uso de ingeniería social para obtener más información.

## 7. CONTROL DE ACCESO

### 7.1. Política de control de acceso

- a) Gestionar los accesos de los usuarios a los sistemas de información, asegurando el acceso de usuarios autorizados y previniendo los accesos no autorizados.
- b) Definir responsabilidades para identificar, gestionar y mantener perfiles de los custodios de información.
- c) Definir claramente los autorizadores de los permisos de acceso a la información.

### 7.8. Política de puesto de trabajo despejado y pantalla limpia

- a) El Oficial de Seguridad de la Información deberá gestionar actividades periódicas (una vez cada mes como mínimo) para la revisión al contenido de las pantallas de los equipos, con el fin de que no se encuentren iconos y accesos innecesarios, y carpetas y archivos que deben ubicarse en la carpeta de documentos del usuario.
- b) Mantener bajo llave la información sensible (cajas fuertes o gabinetes), en especial cuando no estén en uso y no se encuentre personal en la oficina.
- c) Desconectar de la red, servicio o sistema, las computadoras personales, terminales, impresoras asignadas a funciones críticas, cuando se encuentren desatendidas. Por ejemplo, haciendo uso de protectores de pantalla con clave.

### 7.9. Política de uso de los servicios de red

- a) Levantar un registro de los servicios de red la institución.
- b) Identificar por cada servicio los grupos de usuarios que deben acceder.
- c) Definir los perfiles y roles para cada grupo de usuarios que tenga acceso a la red y sus servicios.
- d) Definir mecanismos de bloqueos para que sea restringido el acceso de equipos a la red.

### 7.16. Procedimiento de registro de inicio seguro

- c) Llevar un proceso de monitoreo y registro de los intentos exitosos y fallidos de autenticación del sistema, registros de alarmas cuando se violan las políticas de seguridad del sistema.

### 7.18. Sistema de gestión de contraseñas

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

a) Evidenciar en la política de accesos, la responsabilidad del buen uso de la contraseña y que debe ser secreta e intransferible.

**7.22. Control de acceso a las aplicaciones y a la información**

a) Controlar el acceso de usuarios a la información y a las funciones del sistema de aplicación, de acuerdo con una política definida de control de acceso;

**7.25. Computación y comunicaciones móviles**

c) En la política para uso de equipos portátiles y comunicaciones móviles de la institución, deberá definir rangos de tiempo máximo que el equipo puede permanecer sin conexión a la red de la institución, a fin de que este actualice el antivirus y las políticas aplicadas por la institución.

**10.4. Estructura para la planificación de la continuidad del negocio**

j) Distribuir la política, estrategias, procesos y planes generados.

**11.4. Protección de los datos y privacidad de la información personal**

e) Definir la política para autorización de uso de los servicios de procesamiento de información aprobados, misma que debe ser suscrita por cada funcionario en relación de trabajo permanente o temporal, así como contratistas, asesores, proveedores y representantes de terceras partes.

**11.7. Cumplimiento con las políticas y las normas de la seguridad**

c) Revisar con regularidad en su área de responsabilidad, el cumplimiento del Procesamiento de información de acuerdo con la política de la seguridad, las normas y cualquier otro requisito de seguridad. Si se determina algún incumplimiento o no conformidad como resultado de la revisión, la dirección deberá:

- Determinar la causa del incumplimiento
- Evaluar la necesidad de acciones para garantizar que no se repitan estos incumplimientos
- Determinar e implementar la acción correctiva apropiada
- Revisar la acción correctiva que se ejecutó

**11.10. Protección de las herramientas de auditoría de los sistemas de información**

d) Mantener un estricto control de respaldos y tiempo de retención de los archivos de seguridad y auditoría de acuerdo al tipo de información y la política que se defina.

**Norma de Control Interno de la Contraloría General del Estado – 410-04 Políticas y procedimientos**

La máxima autoridad de la entidad aprobará las políticas y procedimientos que permitan organizar apropiadamente el área de tecnología de información y asignar el talento humano calificado e infraestructura tecnológica necesaria.

**Norma de Control Interno de la Contraloría General del Estado – 410-14 Sitio web, servicios de internet e intranet**

Es responsabilidad de la unidad de tecnología de información elaborar las normas, procedimientos e instructivos de instalación, configuración y utilización de los servicios de internet, intranet, correo electrónico y sitio WEB de la entidad, a base de las disposiciones legales y normativas y los requerimientos de los usuarios externos e internos.

**Norma de Control Interno de la Contraloría General del Estado – 410-17 Firmas electrónicas**

Las entidades, organismos y dependencias del sector público, así como las personas jurídicas que actúen en virtud de una potestad estatal, ajustarán sus procedimientos y operaciones e incorporarán los medios técnicos

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

**INSTITUTO NACIONAL DE ESTADÍSTICA Y CENSOS****MANUAL DE PROCESOS Y PROCEDIMIENTOS DE  
LA DIRECCIÓN DE TECNOLOGÍAS DE LA  
INFORMACIÓN Y COMUNICACIÓN**

Versión: 2.0

DITIC-MPP-001

Página 152-171

necesarios, para permitir el uso de la firma electrónica de conformidad con la Ley de Comercio Electrónico, Firmas y Mensajes de Datos y su Reglamento.

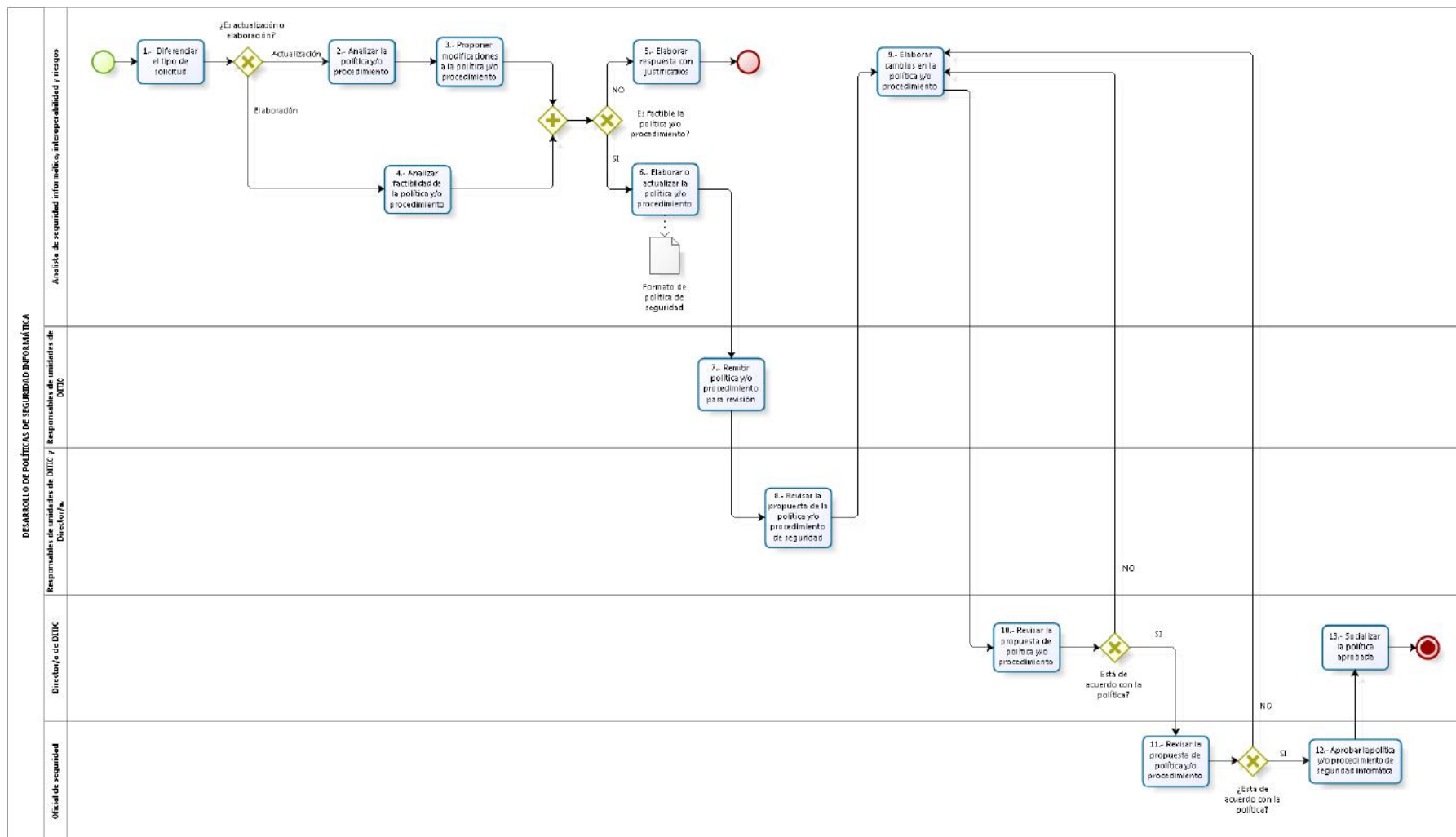
Conservación de archivos electrónicos los archivos electrónicos o mensajes de datos firmados electrónicamente se conservarán en su estado original en medios electrónicos seguros, bajo la responsabilidad del usuario y de la entidad que los generó. Para ello se establecerán políticas internas de manejo y archivo de información digital.

Resolución N° 30 DIREJ-DIJU-NI-2012

Artículo 16.- Implementación de Normas TJC's.- Las Normas TIC's que establezca la Dirección de Tecnologías de la Información y Comunicación a futuro para el mejoramiento de los sistemas y aplicaciones informáticos Institucional formarán parte del presente Reglamento, y serán regulados por el mismo.

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

### 7.1.3. DIAGRAMA DE FLUJO DEL SUBPROCESO DE DESARROLLO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA



Elaborado por:

PC

Revisado por:

DIPLA - DITIC

Aprobado /Autorizado por:

DIREJ

Registrado por:

DIPLA, PC

#### 7.1.4. PROCEDIMIENTO DEL SUBPROCESO DE DESARROLLO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

Nº	Actividad	Detalle de la actividad	Responsable	Documento Generado
1	Diferenciar el tipo de solicitud	Analiza el tipo de solicitud o requerimiento	Analista de seguridad informática, interoperabilidad y riesgos	N/A
	Decisión	<b>¿Es actualización o elaboración?</b> <b>Actualización:</b> Pasar a la actividad 2. Analizar la política y/o procedimiento. <b>Elaboración:</b> Pasar a la actividad 4. Analizar factibilidad de la política y/o procedimiento.	Analista de seguridad informática, interoperabilidad y riesgos	N/A
2	<b>ACTUALIZACIÓN,</b> Analizar la política y/o procedimiento	Realiza el análisis de la política y/o procedimiento para una actualización en el documento	Analista de seguridad informática, interoperabilidad y riesgos	N/A
3	Proponer modificaciones a la política y/o procedimiento	Propone las modificaciones a la política y/o procedimiento en función de las observaciones encontradas.	Analista de seguridad informática, interoperabilidad y riesgos	N/A
4	<b>ELABORACIÓN,</b> Analizar factibilidad de la política y/o procedimiento	Realiza el análisis de factibilidad de elaboración de la política y/o procedimiento.	Analista de seguridad informática, interoperabilidad y riesgos	N/A
	Decisión	<b>¿Es factible la política y/o procedimiento?</b> <b>SI:</b> Elaborar la política y/o procedimiento, pasa a la actividad 5. <b>NO:</b> Elaborar respuesta con justificativos, <b>Fin del proceso.</b>	Analista de seguridad informática, interoperabilidad y riesgos	N/A
5	Elaborar respuesta con justificativos, fin	Elabora la respuesta con los justificativos encontrados en el documento.	Analista de seguridad informática, interoperabilidad y riesgos	N/A
6	Elaborar o actualizar la política y/o procedimiento	Elabora o actualiza la política y/o procedimiento.	Analista de seguridad informática, interoperabilidad y riesgos	Política de Seguridad Informática
7	Remitir política y/o procedimiento para revisión	Remite el documento modificado o elaborado para revisión de los responsables de Unidad de la Dirección de Tecnologías.	Responsables de Unidades de DITIC	N/A
8	Revisar la propuesta de la política y/o procedimiento de seguridad informática	Realiza la propuesta de la política de seguridad informática en función de las modificaciones realizadas.	Responsables de unidades de DITIC y Director/a	N/A

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

9	Elaborar cambios en la política y/o procedimiento	Elabora las modificaciones de la política y/o procedimiento presentada en función de las observaciones entregadas	Analista de seguridad informática, interoperabilidad y riesgos	N/A
10	Revisar la propuesta de política y/o procedimiento	Realiza la revisión de la propuesta de la política y/o procedimiento en función de las observaciones emitidas	Director/a de DITIC	N/A
	Decisión	<b>¿Está de acuerdo con la política?</b> <b>SI:</b> Revisar la propuesta de política, pasa a la actividad <b>11</b> . <b>NO:</b> Elaborar cambios en la política, pasa a la actividad <b>10</b> .	Director/a de DITIC	N/A
11	Revisar la propuesta de política y/o procedimiento	Revisa la propuesta de la política y/o procedimiento elaborado o modificado en función de las necesidades de la institución y la normativa legal.	Oficial de seguridad	N/A
	Decisión	<b>¿Está de acuerdo con la política?</b> <b>NO:</b> Elaborar cambios en la política, pasa a la actividad <b>10</b> . <b>SI:</b> Aprobar la política de seguridad informática, pasa a la actividad <b>12</b> .	Oficial de seguridad	N/A
12	Aprobar la política y/o procedimiento de seguridad informática	Aprueba la política y/o procedimiento de seguridad informática dejando constancia mediante la firma de los involucrados para su posterior socialización y aplicación.	Oficial de seguridad	N/A
13	Socializar la política aprobada	Realiza la socialización de la política y/o procedimiento de seguridad informática a través de la Intranet Institucional.	Director/a de DITIC	N/A

#### 7.1.5. INDICADORES DEL SUBPROCESO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

N°	Indicador	Fórmula de Cálculo	Unidad de Medida	Responsable de Medición	Fuente de Medición	Frecuencia de Medición
1	Número de políticas, procedimientos y/o instructivos elaborados, revisados y/o actualizados en el periodo	Número de políticas, procedimientos y/o instructivos elaborados, revisados y/o actualizados en el periodo	Número	Responsable de Seguridad Informática	Reporte de políticas y/o procedimientos desarrollados	Anual

#### 7.1.6. FORMATOS DEL SUBPROCESO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

Nombre del Registro de Calidad	Código de Formato
Formato de políticas	DITIC-SI-SP1-FOR-01

#### 7.1.7. ANEXOS DEL SUBPROCESO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

“No hay anexos.”

Elaborado por: PC	Revisado por: DIPLA - DITIC	Aprobado /Autorizado por: DIREJ	Registrado por: DIPLA, PC
----------------------	--------------------------------	------------------------------------	------------------------------

	<b>INSTITUTO NACIONAL DE ESTADÍSTICA Y CENSOS</b>	
	<b>MANUAL DE PROCESOS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN</b>	Versión: 2.0
		DITIC-MPP-001
		Página 156-171

## 7.2. FICHA TÉCNICA DEL SUBPROCESO DE PLAN DE CONCIENCIACIÓN DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA A USUARIOS

### 7.2.1. FICHA TÉCNICA DEL SUBPROCESO DE PLAN DE CONCIENCIACIÓN DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA A USUARIOS

<b>Proceso:</b>	GESTIÓN DE SEGURIDAD INFORMÁTICA, INTEROPERABILIDAD Y RIESGOS
<b>Nombre del Subproceso:</b>	PLAN DE CONCIENCIACIÓN DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA A USUARIOS
<b>Código del Subproceso:</b>	DITIC-SI-SP2
<b>Descripción:</b>	<p><b>PROPÓSITO:</b> Concienciar a todos los funcionarios de la Institución acerca las buenas prácticas con respecto a la seguridad informática acorde a las políticas y/o procedimientos elaborados e implementadas en la Institución.</p> <p><b>ALCANCE:</b> Desde analizar que políticas se deben socializar, hasta elaborar informe de las socializaciones realizadas.</p> <p><b>DISPARADOR:</b></p> <ul style="list-style-type: none"> <li>Políticas aprobadas y socializadas</li> </ul> <p><b>PROVEEDORES:</b></p> <ul style="list-style-type: none"> <li>Dirección DITIC</li> <li>Oficial de Seguridad</li> </ul> <p><b>INSUMOS:</b></p> <ul style="list-style-type: none"> <li>Políticas aprobadas y socializadas</li> <li>Procedimientos aprobados y socializadas.</li> <li>Archivos de texto.</li> <li>Directrices dadas por el Oficial de Seguridad de la Información.</li> </ul>
<b>Clientes:</b>	<ul style="list-style-type: none"> <li>Procesos sustantivos y adjetivos del INEC</li> </ul>
<b>Salidas:</b>	<ul style="list-style-type: none"> <li>Correos electrónicos</li> <li>Presentaciones</li> </ul>
<b>Tipo de Proceso:</b>	Adjetivo de asesoría.
<b>Responsable del Proceso:</b>	Responsable de la Unidad de Seguridad Informática, Interoperabilidad y Riesgos
<b>Recursos:</b>	<p><b>MATERIALES:</b></p> <ul style="list-style-type: none"> <li>Muebles de Oficina</li> <li>Insumos de Oficina</li> <li>Equipo de Oficina</li> </ul> <p><b>HUMANOS:</b></p> <ul style="list-style-type: none"> <li>1 Servidor Público 7</li> <li>1 Servidor Público 3</li> </ul>

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------



	<b>INSTITUTO NACIONAL DE ESTADÍSTICA Y CENSOS</b>	
	<b>MANUAL DE PROCESOS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN</b>	Versión: 2.0
		DITIC-MPP-001
		Página 157-171

	<b>TECNOLÓGICOS:</b> <ul style="list-style-type: none"> <li>• Hardware (Computadores, impresoras)</li> <li>• Software</li> <li>• Software de ofimática</li> </ul>
<b>Controles/Marco Legal:</b>	<ul style="list-style-type: none"> <li>• Registro Oficial N° 88 – Acuerdo 166</li> <li>• Norma de Control Interno de la Contraloría General del Estado - 410 - 04 Políticas y procedimientos</li> <li>• Políticas y/o procedimientos aprobados.</li> </ul>

## 7.2.2. CONTROLES DEL SUBPROCESO DE PLAN DE CONCIENCIACIÓN DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA A USUARIOS

**Registro Oficial N° 88 – Acuerdo 166**

### 4.5. Educación, formación y sensibilización en seguridad de la información

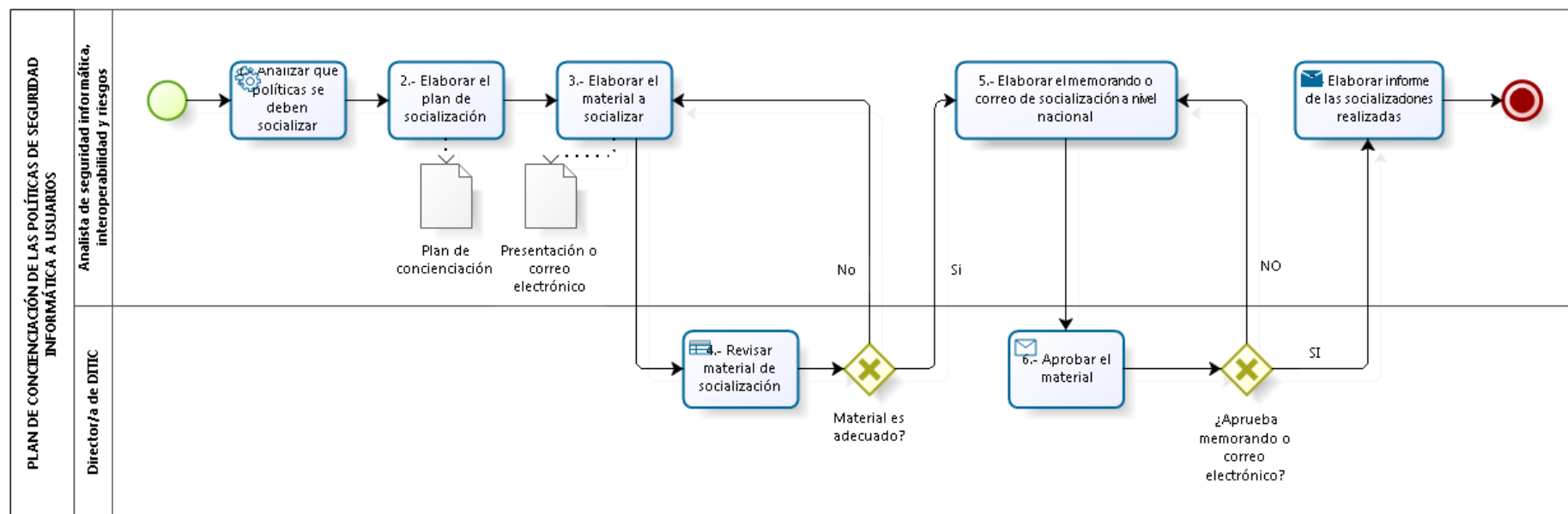
- a) Socializar y capacitar de forma periódica y oportuna sobre las normas y los procedimientos para la seguridad, las responsabilidades legales y los controles de la institución, así como en la capacitación del uso correcto de los servicios de información.

#### **Norma de Control Interno de la Contraloría General del Estado – 410-04 Políticas y procedimientos**

La máxima autoridad de la entidad aprobará las políticas y procedimientos que permitan organizar apropiadamente el área de tecnología de información y asignar el talento humano calificado e infraestructura tecnológica necesaria. La unidad de tecnología de información definirá, documentará y difundirá las políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y comunicaciones en la organización, estos se actualizarán permanentemente e incluirán las tareas, los responsables de su ejecución, los procesos de excepción, el enfoque de cumplimiento y el control de los procesos que están normando, así como, las sanciones administrativas a que hubiere lugar si no se cumplieran.

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

### 7.2.3. DIAGRAMA DE FLUJO DEL SUBPROCESO DE PLAN DE CONCIENCIACIÓN DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA A USUARIOS



Elaborado por:

PC

Revisado por:

DIPLA - DITIC

Aprobado /Autorizado por:

DIREJ

Registrado por:

DIPLA, PC

#### 7.2.4. PROCEDIMIENTO DEL SUBPROCESO DE PLAN DE CONCIENCIACIÓN DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA A USUARIOS

Nº	Actividad	Detalle de la actividad	Responsable	Documento Generado
1	Analizar que políticas se deben socializar	Realiza el análisis de las políticas que deben ser difundidas a los servidores públicos	Analista de seguridad informática, interoperabilidad y riesgos	N/A
2	Elaborar el plan de socialización	Elabora el plan de socialización para ser difundida según la programación	Analista de seguridad informática, interoperabilidad y riesgos	Plan de concienciación
3	Elaborar el material a socializar	Elabora el material para la respectiva socialización según el cronograma de trabajo	Analista de seguridad informática, interoperabilidad y riesgos	Presentación o correo electrónico
4	Revisar material de socialización	Ejecuta la revisión del material de la socialización para emisión de observaciones en pos de mejora del material	Director/a de DITIC	N/A
	Decisión	<b>¿Material es adecuado?</b> <b>SI:</b> Realiza la actividad 6. Aprobar el material. <b>NO:</b> Pasa a la actividad 3. Elaborar el material a socializar.	Director/a de DITIC	N/A
5	Elaborar el memorando o correo de socialización a nivel nacional	Elaborar el memorando o correo de socialización a nivel nacional.	Analista de seguridad informática, interoperabilidad y riesgos	N/A
6	Aprobar el material	Realizar la aprobación del material para poner en acción lo planificado en el cronograma	Director/a de DITIC	N/A
	Decisión	<b>¿Aprueba memorando o correo electrónico?</b> <b>NO:</b> Pasa a la actividad 5. Elaborar el memorando o correo electrónico de socialización a nivel nacional. <b>SI:</b> Realiza la actividad 7. Elaborar informe de las socializaciones.	Analista de seguridad informática, interoperabilidad y riesgos	N/A
7	Elaborar informe de las socializaciones realizadas	Realiza la elaboración del informe de las socializaciones realizadas	Analista de seguridad informática, interoperabilidad y riesgos	N/A

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

### 7.2.5. INDICADORES DEL SUBPROCESO DE PLAN DE CONCIENCIACIÓN DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA A USUARIOS

N°	Indicador	Fórmula de Cálculo	Unidad de Medida	Responsable de Medición	Fuente de Medición	Frecuencia de Medición
1	Número de informes presentados en relación a las socializaciones del programa de concientización realizadas en el periodo	Número de informes presentados en relación a las socializaciones del programa de concientización realizadas en el periodo	Número	Responsable de Seguridad Informática	Informes presentados en relación a las socializaciones del programa de concientización realizadas en el periodo	Trimestral

### 7.2.6. FORMATOS DEL SUBPROCESO DE PLAN DE CONCIENCIACIÓN DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA A USUARIOS

Nombre del Registro de Calidad	Código de Formato
Informe socialización de políticas	DITIC-SI-SP2-FOR-01

### 7.2.7. ANEXOS DEL SUBPROCESO DE PLAN DE CONCIENCIACIÓN DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA A USUARIOS

“No hay anexos.”

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

### 7.3. SUBPROCESO DE MONITOREO Y CUMPLIMIENTO DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN RELACIONADO A LA SEGURIDAD INFORMÁTICA

#### 7.3.1. FICHA TÉCNICA DEL SUBPROCESO DE MONITOREO Y CUMPLIMIENTO DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN RELACIONADO A LA SEGURIDAD INFORMÁTICA

<b>Proceso:</b>	GESTIÓN DE SEGURIDAD INFORMÁTICA, INTEROPERABILIDAD Y RIESGOS
<b>Nombre del Subproceso:</b>	MONITOREO Y CUMPLIMIENTO DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN RELACIONADO A LA SEGURIDAD INFORMÁTICA
<b>Código del Subproceso:</b>	DITIC-SI-SP3
<b>Descripción:</b>	<p><b>PROPÓSITO:</b> Realizar seguimiento a la implementación de controles de seguridad Informática en la Dirección de Tecnologías de la Información y Comunicación.</p> <p><b>ALCANCE:</b> Desde enviar matriz con los hitos que deben ser cumplidos, hasta entregar y archivar el informe.</p> <p><b>DISPARADOR:</b></p> <ul style="list-style-type: none"> <li>• Memorandos o correos electrónicos</li> </ul> <p><b>PROVEEDORES:</b></p> <ul style="list-style-type: none"> <li>• Oficial de Seguridad de la Información</li> </ul> <p><b>INSUMOS:</b></p> <ul style="list-style-type: none"> <li>• Matrices con los hitos que deben ser cumplidos</li> </ul>
<b>Clientes:</b>	<ul style="list-style-type: none"> <li>• DITIC</li> </ul>
<b>Salidas:</b>	<ul style="list-style-type: none"> <li>• Informes de cumplimiento de los hitos</li> </ul>
<b>Tipo de Proceso:</b>	Adjetivo de asesoría.
<b>Responsable del Proceso:</b>	Responsable de la Unidad de Seguridad Informática, Interoperabilidad y Riesgos
<b>Recursos:</b>	<p><b>MATERIALES:</b></p> <ul style="list-style-type: none"> <li>• Muebles de Oficina</li> <li>• Insumos de Oficina</li> <li>• Equipo de Oficina</li> </ul> <p><b>HUMANOS:</b></p> <ul style="list-style-type: none"> <li>• 1 Servidor Público 7</li> </ul> <p><b>TECNOLÓGICOS:</b></p> <ul style="list-style-type: none"> <li>• Hardware (Computadores, impresoras)</li> <li>• Software</li> </ul>

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

	<ul style="list-style-type: none"> <li>Software de ofimática</li> </ul>
<b>Controles/Marco Legal:</b>	<ul style="list-style-type: none"> <li>Registro Oficial N° 88 – Acuerdo 166</li> <li>Norma de Control Interno de la Contraloría General del Estado - 410 - 13 Monitoreo y evaluación de los procesos y servicios</li> </ul>

### 7.3.2. CONTROLES DEL SUBPROCESO DE MONITOREO Y CUMPLIMIENTO DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN RELACIONADO A LA SEGURIDAD INFORMÁTICA

#### Registro Oficial N° 88 – Acuerdo 166

#### 6.6. Monitoreo y revisión de los servicios, por terceros.

- a) Identificar los sistemas sensibles o críticos que convenga tener dentro o fuera de la institución.
- b) Monitorear los niveles de desempeño de los servicios para verificar el cumplimiento de los acuerdos (\*).
- c) Analizar los reportes de servicios, reportes de incidentes elaborados por terceros y acordar reuniones periódicas según los acuerdos (\*).
- d) Revisar y verificar los registros y pruebas de auditoría de terceros, con respecto a eventos de seguridad, problemas de operación, fallas relacionados con el servicio prestado (\*).

#### 6.8. Gestión de la capacidad

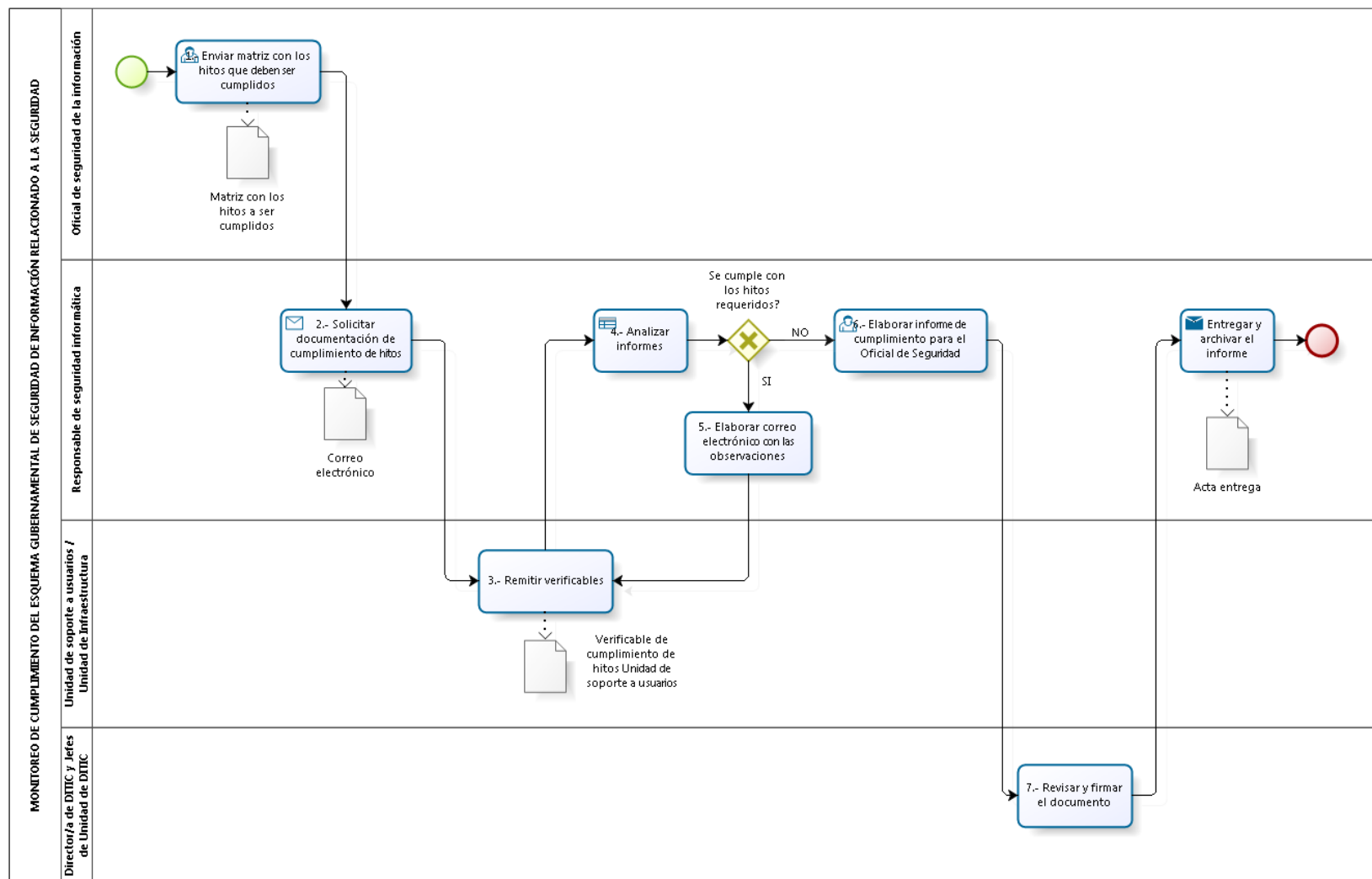
- a) Realizar proyecciones de los requerimientos de capacidad futura de recursos para asegurar el desempeño de los servicios y sistemas informáticos (\*).
- b) Monitorear los recursos asignados para garantizar la capacidad y rendimiento de los servicios y sistemas informáticos.
- c) Utilizar la información del monitoreo para la adquisición, asignación de recursos y evitar cuellos de botella.

#### Norma de Control Interno de la Contraloría General del Estado – 410-13 Monitoreo y evaluación de los procesos y servicios

Es necesario establecer un marco de trabajo de monitoreo y definir el alcance, la metodología y el proceso a seguir para monitorear la contribución y el impacto de tecnología de información en la entidad.

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

### 7.3.3. DIAGRAMA DE FLUJO DEL SUBPROCESO DE MONITOREO Y CUMPLIMIENTO DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN RELACIONADO A LA SEGURIDAD INFORMÁTICA



Elaborado por:

PC

Revisado por:

DIPLA - DITIC

Aprobado /Autorizado por:

DIREJ

Registrado por:

DIPLA, PC

#### 7.3.4. PROCEDIMIENTO DEL SUBPROCESO DE MONITOREO Y CUMPLIMIENTO DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN RELACIONADO A LA SEGURIDAD INFORMÁTICA

Nº	Actividad	Detalle de la actividad	Responsable	Documento Generado
1	Enviar matriz con los hitos que deben ser cumplidos	Remite mediante correo electrónico la matriz con los hitos a ser cumplidos por parte de DITIC	Oficial de seguridad de la información	Matriz con los hitos a ser cumplidos
2	Solicitar documentación de cumplimiento de hitos	Solicita la documentación de cumplimiento de hitos en función de los requerimientos a los jefes de unidad de DITIC	Responsable de seguridad informática	Correo electrónico
3	Remitir verificable	Remite la información que permite verificar el cumplimiento del hito.	Unidad de soporte a usuarios / Unidad de Infraestructura	Verificable de cumplimiento de hitos Unidad de soporte a usuarios
4	Analizar informes	Realiza el análisis de los informes presentados por los responsables de las Unidades de Soporte a Usuarios e Infraestructura de DITIC	Responsable de seguridad informática	N/A
	Decisión	<b>¿Se cumple con los hitos requeridos?</b> <b>SI:</b> Pasa a la actividad <b>6</b> . Elaborar informe de cumplimiento. <b>NO:</b> Pasa a la actividad <b>5</b> . Elaborar correo electrónico con las observaciones.	Responsable de seguridad informática	N/A
5	Elaborar correo electrónico con las observaciones	Genera un correo electrónico según las observaciones encontradas a los jefes de unidad de DITIC. Regresa a la actividad <b>3</b> .	Responsable de seguridad informática	N/A
6	Elaborar informe de cumplimiento para el Oficial de Seguridad	Elabora el informe de cumplimiento en función de las observaciones y previa constatación del cumplimiento de los hitos en base a los formatos establecidos por el Oficial de Seguridad.	Responsable de seguridad informática	N/A
7	Revisar y firmar el documento	Verifica el informe para ratificar su contenido	Director/a de DITIC y Jefes de Unidad de DITIC	N/A
8	Entregar y archivar el informe	Entrega el informe a través de un acta entrega recepción y su posterior archivo para futuros respaldos de gestión	Responsable de seguridad informática	Acta entrega

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------



### 7.3.5. INDICADORES DEL SUBPROCESO DE MONITOREO Y CUMPLIMIENTO DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN RELACIONADO A LA SEGURIDAD INFORMÁTICA

N°	Indicador	Fórmula de Cálculo	Unidad de Medida	Responsable de Medición	Fuente de Medición	Frecuencia de Medición
1	Porcentaje de hosts actualizados con antivirus corporativo	$(\# \text{ de computadores actualizados} / \text{número de computadores en red}) * 100$	Porcentaje	Responsable de Unidad	Reporte de aplicativo McAfee	Trimestral
2	Número de informes elaborados respecto del cumplimiento del EGSi	Número de informes elaborados	Número	Responsable de Unidad	Informes trimestrales	Trimestral

### 7.3.6. FORMATOS DEL SUBPROCESO DE MONITOREO Y CUMPLIMIENTO DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN RELACIONADO A LA SEGURIDAD INFORMÁTICA

Nombre del Registro de Calidad	Código de Formato
Matriz con los hitos a ser cumplidos	DITIC-SI-SP3-FOR-01
Actas de entrega a recepción realizadas al Oficial de Seguridad de la Información	DITIC-SI-SP3-FOR-02

### 7.3.7. ANEXOS DEL SUBPROCESO DE MONITOREO Y CUMPLIMIENTO DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN RELACIONADO A LA SEGURIDAD INFORMÁTICA

“No hay anexos.”

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

	<b>INSTITUTO NACIONAL DE ESTADÍSTICA Y CENSOS</b>	
	<b>MANUAL DE PROCESOS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN</b>	Versión: 2.0
		DITIC-MPP-001
		Página 166-171

## 7.4. SUBPROCESO DE ADMINISTRACIÓN DE SISTEMA GPR

### 7.4.1. FICHA TÉCNICA DEL SUBPROCESO DE ADMINISTRACIÓN DE SISTEMA GPR

<b>Proceso:</b>	GESTIÓN DE SEGURIDAD INFORMÁTICA, INTEROPERABILIDAD Y RIESGOS
<b>Nombre del Subproceso:</b>	ADMINISTRACIÓN DE SISTEMA GPR
<b>Código del Subproceso:</b>	DITIC-SI-SP4
<b>Descripción:</b>	<p><b>PROPÓSITO:</b> Mantener actualizada el listado de servidores que tienen acceso al sistema GPR, con la finalidad de evitar accesos no autorizados.</p> <p><b>ALCANCE:</b> Desde elaborar memorando de creación de usuarios, hasta elaborar comunicado.</p> <p><b>DISPARADOR:</b></p> <ul style="list-style-type: none"> <li>• Memorandos o correos electrónicos</li> </ul> <p><b>PROVEEDORES:</b></p> <ul style="list-style-type: none"> <li>• DIPLA</li> <li>• Procesos sustantivos y adjetivos del INEC</li> </ul> <p><b>INSUMOS:</b></p> <ul style="list-style-type: none"> <li>• Memorandos o correos electrónicos</li> </ul>
<b>Clientes:</b>	<ul style="list-style-type: none"> <li>• Procesos sustantivos y adjetivos del INEC</li> </ul>
<b>Salidas:</b>	<ul style="list-style-type: none"> <li>• Sistema actualizado con los usuarios</li> </ul>
<b>Tipo de Proceso:</b>	Adjetivo de asesoría.
<b>Responsable del Proceso:</b>	Responsable de la Unidad de Seguridad Informática, Interoperabilidad y Riesgos
<b>Recursos:</b>	<p><b>MATERIALES:</b></p> <ul style="list-style-type: none"> <li>• Muebles de Oficina</li> <li>• Insumos de Oficina</li> <li>• Equipo de Oficina</li> </ul> <p><b>HUMANOS:</b></p> <ul style="list-style-type: none"> <li>• 1 Servidor Público 7</li> </ul> <p><b>TECNOLÓGICOS:</b></p> <ul style="list-style-type: none"> <li>• Hardware (Computadores, impresoras)</li> <li>• Software</li> <li>• Software de ofimática</li> </ul>
<b>Controles/Marco Legal:</b>	<ul style="list-style-type: none"> <li>• Norma de implementación y operación de gobiernos por resultados – Acuerdo Ministerial 1002 – art. 30, art. 31, art. 32.</li> </ul>

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

#### 7.4.2. CONTROLES DEL SUBPROCESO DE ADMINISTRACIÓN DE SISTEMA GPR

**Norma de implementación y operación de gobiernos por resultados – Acuerdo Ministerial 1002 – art. 30, art. 31, art. 32.**

Capítulo VIII - de los actores de gobierno por resultados

**Art. 30.-** Equipo Institucional GPR.-

Cada institución conformará un equipo institucional GPR con los siguientes roles y responsabilidades:

##### LIDER METODOLOGICO GPR

- Líderes metodológicos.- Son roles permanentes dentro de la Coordinación General de Gestión Estratégica y en su ausencia de la Coordinación de Planificación, con un mínimo de dos (2) personas por entidad para ser capacitados como expertos en la metodología, con asistencia obligatoria a los eventos de GPR y asignados como custodios internos de la calidad de la información registrada y de la metodología al interior de la misma.

##### ADMINISTRADOR INSTITUCIONAL DE GPR

- Administrador institucional de GPR.- Es un rol permanente dentro de la Unidad de Tecnologías de Información de la entidad, encargado de manejar el acceso de sus usuarios y el mantenimiento 1 de la estructura organizacional registrada en GPR.
- Capacitación del Administrador Institucional de GPR.- Cada Administrador Institucional de GPR será capacitado en el uso del Módulo de Administración GPR y recibirá una copia del Manual de Administración GPR con la información detallada necesaria para ejecutar su rol.

##### LIDER DE LOGISTICA GPR

- Líder de logística GPR.- Es un rol temporal que responde al titular de la entidad, para coordinar y apoyar la logística de eventos y el proceso de invitaciones durante el despliegue de GPR al interior de la misma.

**Art. 31.-** Directrices de administración de usuarios y soporte técnico de la institución.-

La administración de usuarios y soporte técnico de GPR se regirá por las siguientes directrices:

##### CONTROL DE ACCESO A LA HERRAMIENTA GPR

- Gestión de usuarios y claves.- La institución creará sus usuarios por medio del responsable i determinado para el efecto. La solicitud de usuario y clave de un servidor o funcionario debe ser aprobada por el Jefe inmediato superior, deberán únicamente provenir de un correo electrónico institucional comprobado.
- Depuración periódica de usuarios.- El administrador institucional de GPR debe depurar semanalmente los usuarios que hayan salido de la institución o que dejen de ser responsables en cualquiera de los elementos de los planes estratégicos y operativos, así como llevar un control periódico de acceso y roles para salvaguardar la seguridad de la información.

##### PERFILES DE USUARIOS

- Perfiles de usuarios de la herramienta GPR.- Existen cinco (5) perfiles de usuarios en la herramienta GPR. Es responsabilidad del Administrador Institucional de GPR asegurar la aplicación correcta a los usuarios de la institución de acuerdo a los siguientes perfiles:
  - Administrador: Es el responsable de administración de usuarios y claves, estructura de planes y control de cambios de metas cenadas de indicadores. Tiene acceso a todos los elementos de la organización y sub-organizaciones designadas.
  - Ejecutivo: Es el responsable de un plan, estratégico y tiene permiso de actualización de todos sus elementos.
  - Participante: Es el perfil estándar para participantes de talleres y usuarios que requieren acceso a todos los elementos con algunas restricciones.
  - Líder: Es un usuario limitado con permiso de actualización solamente para elementos en donde está registrado como responsable (especialmente proyectos y procesos).
  - Observador: Es un usuario con permiso de lectura solamente.
  - Usuarios de alto nivel.- En casos de usuarios que requieren acceso a más de una institución, la Secretaría Nacional de la Administración Pública determinará y otorgará los permisos necesarios.

##### RESPONSABILIDAD POR MAL USO DE USUARIO Y CLAVE

Elaborado por:	Revisado por:	Aprobado /Autorizado por:	Registrado por:
PC	DIPLA - DITIC	DIREJ	DIPLA, PC



- Responsabilidad de los usuarios.- Los usuarios son responsables por la no divulgación de sus claves de acceso a la herramienta GPR, en caso de que se detecte que su clave ha sido utilizada por otra persona que no tiene autorización se debe notificar a la Secretaría Nacional de la Administración Pública. La omisión de las acciones determinadas generará responsabilidad administrativa.

**Art. 32.- Soporte y administración de nuevos requerimientos.-**

Las actividades de soporte metodológico y administración de nuevos requerimientos a GPR se Regirán por las siguientes directrices:

**NUEVOS USUARIOS O CAMBIO DE AUTORIDADES**

- Nuevos ejecutivos y/o usuarios.- Si existe cambio de autoridad o titular responsable de un plan GPR, el equipo institucional GPR es responsable de capacitarle en la metodología y el uso de la herramienta durante su primer mes de gestión, así como a todo nuevo líder de proyecto o responsables de procesos y a todo nuevo usuario de la herramienta GPR.

**CAMBIOS EN EL EQUIPO INSTITUCIONAL GPR**

- Continuidad de capacidades institucionales en GPR.- En caso de que existan cambios en el equipo institucional GPR capacitado para la implementación y operación de Gobierno Por Resultados, se notificará inmediatamente a la Secretaría Nacional de la Administración Pública con el fin de que inicie las acciones pertinentes de inducción y capacitación para los nuevos miembros.

**NIVELES Y TIPOS DE SOPORTE**

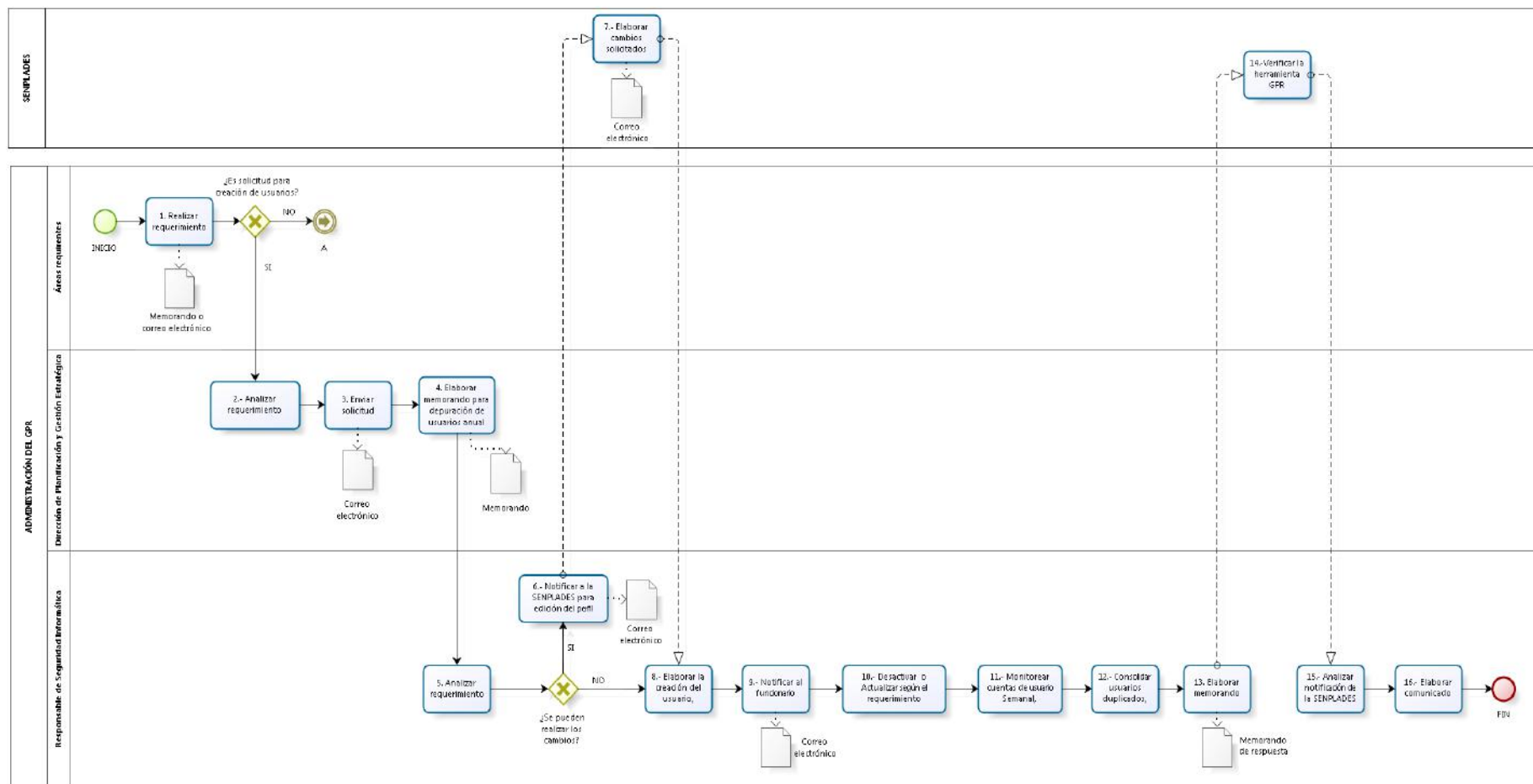
- Primer nivel.- El primer nivel de resolución de requerimiento de mesa de ayuda será el equipo institucional GPR.
- Segundo nivel.- El segundo nivel será el equipo de consultores GPR-SNAP.
- Tercer nivel.- El tercer nivel deberá ser formado con equipos de trabajo y responderá a cambios de estructuras orgánicas y cambios de versiones en la planificación, será tratado por los consultores GPR-SNAP.

**EVOLUCION Y MEJORAS A GPR**

Administración de nuevos requerimientos.- Todos los requerimientos de los usuarios de Gobierno Por Resultados, tales como cambios que requieren autorización, modificaciones a la funcionalidad de la herramienta, consultas metodológicas y de contenido, reportes requeridos, entre otros se receptorán a través de la mesa de ayuda, de conformidad con el procedimiento y requisitos que la Secretaría Nacional de la Administración Pública determine para el efecto.

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

### 7.4.3. DIAGRAMA DE FLUJO DEL SUBPROCESO DE ADMINISTRACIÓN DE SISTEMA GPR



Elaborado por:

PC

Revisado por:

DIPLA - DITIC

Aprobado /Autorizado por:

DIREJ

Registrado por:

DIPLA, PC

#### 7.4.4. PROCEDIMIENTO DEL SUBPROCESO DE ADMINISTRACIÓN DE SISTEMA GPR

Nº	Actividad	Detalle de la actividad	Responsable	Documento Generado
1	Realizar requerimiento	Elabora el memorando para creación de nuevos usuarios o correo electrónico en caso de activación o cambios de clave, todo esto según procedimiento socializado con memorando INEC-DIPLA-2017-0925-M.	Áreas requerientes	Memorando o correo electrónico
	Decisión	<b>¿Es solicitud para creación de usuarios?</b> <b>SI:</b> Pasar a la actividad 2. Realiza memorando solicitando la creación del usuario. <b>NO:</b> Pasar a la actividad 5. Realiza correo electrónico al Administrador GPR DITIC.	Áreas requerientes	N/A
2	Analizar requerimiento	Analiza el requerimiento para verificar el tipo de perfil que se le asignará al usuario que será creado	Dirección de Planificación y Gestión Estratégica	N/A
3	Enviar solicitud	Envía la solicitud a través de correo electrónico para que se proceda con la creación del usuario	Dirección de Planificación y Gestión Estratégica	Correo Electrónico
4	Elaborar memorando para depuración de usuarios anual	Elabora memorando solicitando la depuración de usuarios a nivel Institucional	Dirección de Planificación y Gestión Estratégica	Memorando
5	Analizar requerimiento	Analiza el requerimiento para entender que acciones se deberá tomar	Responsable de Seguridad Informática	N/A
	Decisión	<b>¿Se pueden realizar los cambios?</b> <b>SI:</b> Pasar a la actividad 6. Notifica a SENPLADES. <b>NO:</b> Pasar a la actividad 8. Realiza lo solicitado.	Responsable de Seguridad Informática	N/A
6	Notificar a la SENPLADES para edición del perfil	Elabora la notificación a SENPLADES para poder realizar la edición de los perfiles	Responsable de Seguridad Informática	Correo electrónico
7	Elaborar cambios solicitados	Elabora los cambios solicitados en función de lo requerido. Fin	SENPLADES	N/A
8	Elaborar la creación del usuario	Elabora la creación del usuario y realizar la respectiva notificación para que inicie acciones en el sistema GPR	Responsable de Seguridad Informática	N/A
9	Notificar al funcionario	Notifica al funcionario la creación o actualización del usuario mediante correo electrónico	Responsable de Seguridad Informática	Correo electrónico
10	Desactivar o Actualizar según el requerimiento	Ejecuta la desactivación cuando un usuario se ha retirado de la institución o en función del requerimiento	Responsable de Seguridad Informática	N/A

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------

11	Monitorear cuentas de usuario Semanal,	<b>Semanalmente:</b> Realiza el monitoreo de las cuentas de usuario para controlar la funcionalidad y cuentas que estén sin usarse	Responsable de Seguridad Informática	N/A
12	Consolidar usuarios duplicados,	Consolida a los usuarios que hayan sido creados por varias veces. <b>Fin del proceso.</b>	Responsable de Seguridad Informática	N/A
13	Elaborar Memorando	Elabora el memorando que indica que se realizó la depuración de usuarios de toda la Institución de acuerdo a requerimiento de DIPLA.	Responsable de Seguridad Informática	Memorando de respuesta
14	Verificar la herramienta GPR	Realiza la verificación de la herramienta GPR para medir el status del sistema	SENPLADES	N/A
15	Analizar notificación de la SENPLADES	Realiza la notificación a la Secretaría Nacional de Administración Pública para su ejecución en función del requerimiento	Responsable de Seguridad Informática	N/A
16	Elaborar comunicado	Elabora el comunicado para notificar a los involucrados	Responsable de Seguridad Informática	N/A

#### 7.4.5. INDICADORES DEL SUBPROCESO DE ADMINISTRACIÓN DE SISTEMA GPR

N°	Indicador	Fórmula de Cálculo	Unidad de Medida	Responsable de Medición	Fuente de Medición	Frecuencia de Medición
1	Número de requerimientos atendidos	Número de requerimientos realizados	Número	Responsable de Unidad	Informe de requerimientos atendidos de forma trimestral	Trimestral

#### 7.4.6. FORMATOS DEL SUBPROCESO DE ADMINISTRACIÓN DE SISTEMA GPR

Nombre del Registro de Calidad	Código de Formato
Informe de requerimiento	DITIC-SI-SP4-FOR01

#### 7.4.7. ANEXOS DEL SUBPROCESO DE ADMINISTRACIÓN DE SISTEMA GPR

- Memorando INEC-DIPLA-2017-0925-M

<b>Elaborado por:</b> PC	<b>Revisado por:</b> DIPLA - DITIC	<b>Aprobado /Autorizado por:</b> DIREJ	<b>Registrado por:</b> DIPLA, PC
-----------------------------	---------------------------------------	---	-------------------------------------