MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL

OFICINA DE TELEMÁTICA

Bogotá D.C; 12 de octubre de 2017

Análisis GAP con base en las buenas prácticas emitidas por el Sistema de Gestión de Seguridad de la Información a FORPO

De acuerdo al CONPES 3458 Política de Seguridad Digital, el gobierno nacional definió unas misiones particulares, entre ellas la Policía Nacional, encargándola particularmente de la prevención y atención a delitos e incidentes informáticos; por tal motivo el CSIRT-PONAL tiene como misión salvaguardar los activos críticos de la Policía Nacional en relación a su disponibilidad, confidencialidad e integridad, por otra parte brindar servicios proactivos que coadyuven a mitigar las brechas existentes en seguridad de la información del Estado Colombiano.

Es por esto que el CSIRT-PONAL provee servicios de análisis de vulnerabilidades, análisis de brechas de seguridad con respecto a la ISO 27001, alertas tempranas, análisis de malware y jornadas de capacitación a las entidades que así lo soliciten.

De acuerdo a lo anterior el siguiente informe pretende describir el análisis GAP del estándar ISO 27001:2013 que se realizó al Fondo Rotatorio de la Policía (FORPO), el cual permitió determinar el grado de cumplimiento que tiene la entidad con respecto a los lineamientos especificados por la Norma Técnica, la cual contempla diversos aspectos que se deben tener en cuenta como buenas prácticas para la Seguridad de la Información.

Los niveles de madures del sistema se miden en 6 estados, los cuales están descritos en la siguiente tabla.

Nivel de Implementación	% de Cumplimiento	Descripción
Gestionado	**100%**	Los procesos han sido llevados al nivel de mejores prácticas, con base en los resultados de la mejora continua.
		Es posible hacer seguimiento y medir el cumplimiento de los procedimientos, así como tomar acciones correctivas o preventivas cuando se detectan fallas y hacer seguimiento dichas acciones.
Medible	**80%**	Es posible hacer seguimiento y medir el cumplimiento de los procedimientos, aunque no es constante que se tomen acciones correctivas o preventivas.
Definido	**60%**	Los procesos se encuentran totalmente documentados pero la responsabilidad del cumplimiento recae en cada individuo y es poco probable que se detecten desviaciones a los estándares establecidos.

Repetible	**40%**	Los procesos se han desarrollado hasta un punto en el cual procedimientos similares son utilizados por personas diferentes para llevar a cabo la misma tarea, aun cuando estos no se encuentran totalmente documentados.
Inicial	**20%**	Se ha identificado una situación que debe ser tratada y se han implementado acciones aun cuando no hay directivas o procesos documentados relacionados con dichas acciones.
Inexistente	**0%**	Carencia total de procesos relacionados con el SGSI.
		La organización no ha identificado una situación que debe ser tratada.

La verificación tenía como objetivo evidenciar el nivel de madurez de los dominios del anexo A de la Norma ISO 27001, encontrando lo siguiente:

El nivel de cumplimiento de los requisitos esta por el orden de un **28%,** El requisito mínimo de madurez de una entidad para lograr una gestión medible en seguridad de la información debe ser igual o superior al 70%.

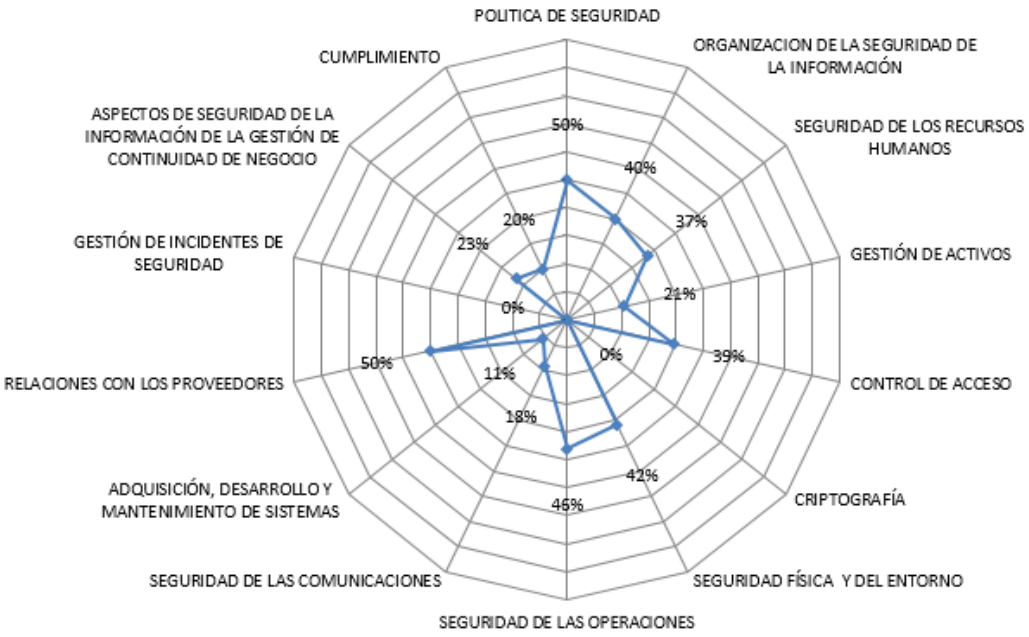
La calificación obtenida de acuerdo a cada dominio, nos permite evidenciar lo siguiente:

Item	Dominios	Cumplimiento
5	**POLITICA DE SEGURIDAD**	50%
6	**ORGANIZACION DE LA SEGURIDAD DE LA INFORMACIÓN**	40%
7	**SEGURIDAD DE LOS RECURSOS HUMANOS**	37%
8	**GESTIÓN DE ACTIVOS**	21%
9	**CONTROL DE ACCESO**	39%
10	**CRIPTOGRAFÍA**	0%
11	**SEGURIDAD FÍSICA Y DEL ENTORNO**	42%
12	**SEGURIDAD DE LAS OPERACIONES**	46%
13	**SEGURIDAD DE LAS COMUNICACIONES**	18%
14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**	11%
15	**RELACIONES CON LOS PROVEEDORES**	50%
16	**GESTIÓN DE INCIDENTES DE SEGURIDAD**	0%
17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO**	23%
18	**CUMPLIMIENTO**	20%
TOTAL		28%

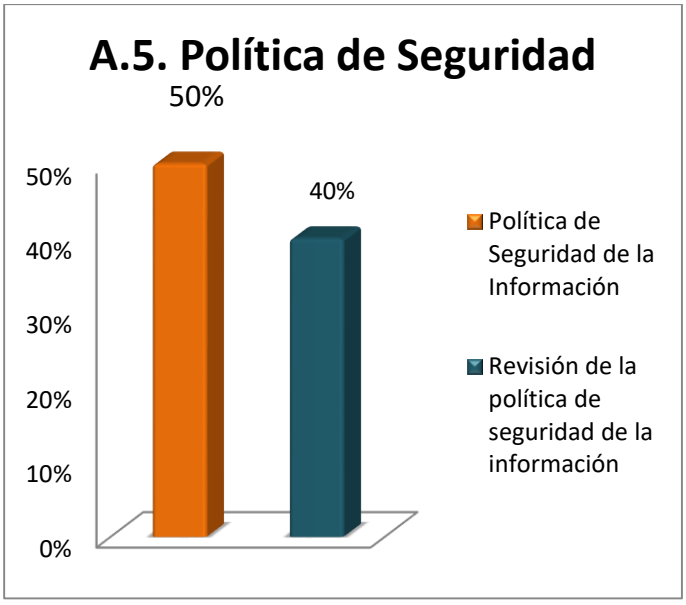
Porcentaje de Implementación de controles

28% Nivel de madurez

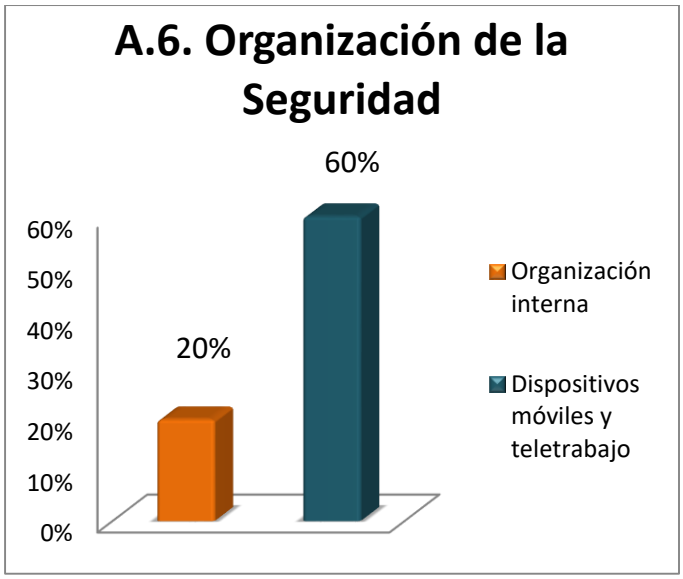
Un valor con el cual una entidad puede tener procesos seguros es del **70%.**



<u>Niveles de madurez por cada uno de los dominios y sus recomendaciones</u>

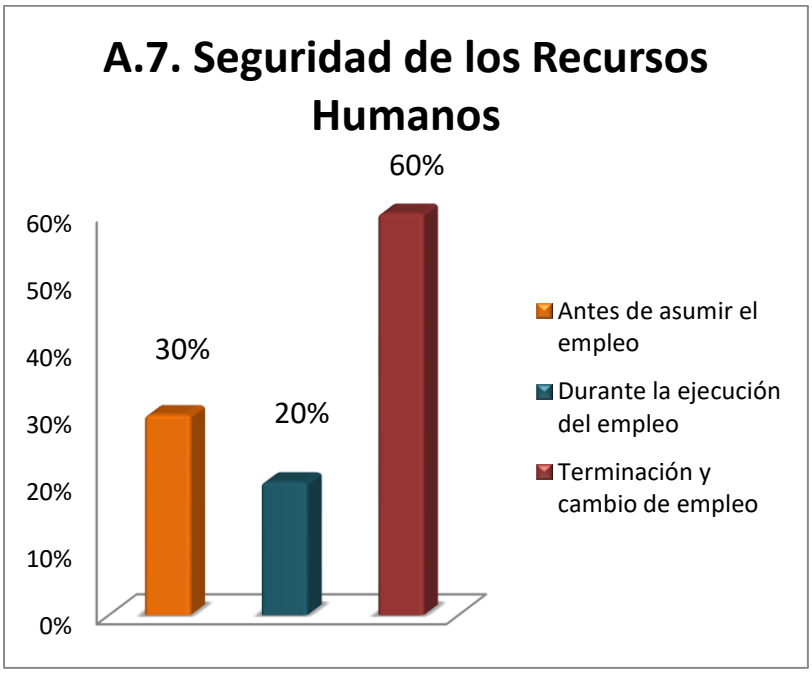


5	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	RECOMENDACIÓN
5.1	Orientación de la dirección para la gestión de la seguridad de la información	
5.1.1	Políticas para la seguridad de la información	Aunque existe una Política de Seguridad revisada y aprobada por la dirección de FORPO esta no ha sido socializada he implementada. Recomendación: Diseñar una política aplicable a el FORPO, que minimice los riesgos evidenciados en el análisis de riesgos, esta debe ser socializa y cumplida por toda la entidad
5.1.2	Revisión de las políticas para seguridad de la información	Solo existe una versión de la Política, a medida que la madurez del sistema va creciendo se deben realizar ajustes a la política, con el fin de atacar problemáticas que no se contemplaron en versiones anteriores.



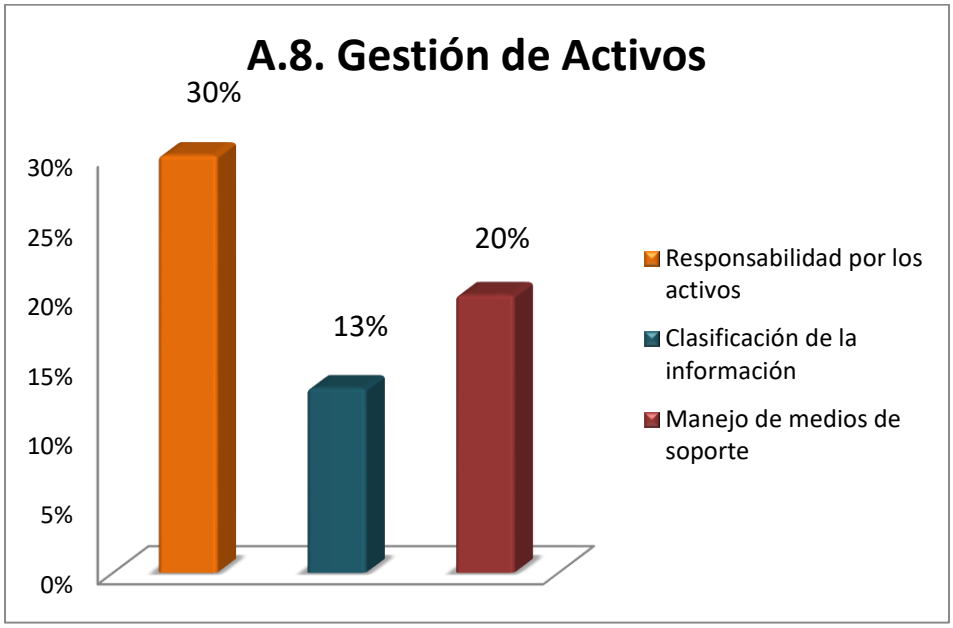
6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	RECOMENDACIÓN
6.1	Organización interna	6.1
6.1.1	Asignación de responsabilidades para la seguridad de la información	Dado que el FORPO cuenta con funcionarios en diferentes modalidades contractuales, a cada uno de ellos se le debe informar la responsabilidad con la
6.1.2	Distribución (segregación) de funciones	

		seguridad de la información, informando el cumplimiento de la Política. Por otra parte, al personal de telemática se le deben asignar responsabilidades específicas en cuanto a control y monitoreo de controles que dependan de Tecnología y asignar el cargo de Analista de Seguridad de la Información a un funcionario que se encargue de la implementación del SGSI.
6.1.3	Contacto con las autoridades	Se debe definir mediante documento "Plan de Emergencias" la lista de contactos definidos y conocidos por el personal de tecnología, seguridad el cual debe contener: número de personal de mantenimiento y dirección para UPS, aire acondicionado, bases de datos, empresa Condensa, proveedor de internet etc. estos se deben encontrar en un lugar de visible ante una falla.
6.1.4	Contacto con grupos de interés especial	Se recomienda suscribirse al sitio https://cc-csirt.policia.gov.co con el fin enterarse sobre boletines informativos, análisis de malware en archivos y URLs
6.1.5	Seguridad de la información en gestión de proyectos	Se recomienda realizar los estudios de seguridad de los ingenieros que implementan proyectos de contratos realizados por FORPO, se recomienda incluir en los estudios previos, una especificaciones realiza con confidencialidad de la información
6.2	Dispositivos móviles y teletrabajo	6.2
6.2.1	Política para dispositivos móviles	Continuar con la política de restricción de equipos móviles.
6.2.2	Teletrabajo	Verificar si es necesaria la implementación de un concentrador de VPN para soporte y trabajo de los administradores en caso de falla.



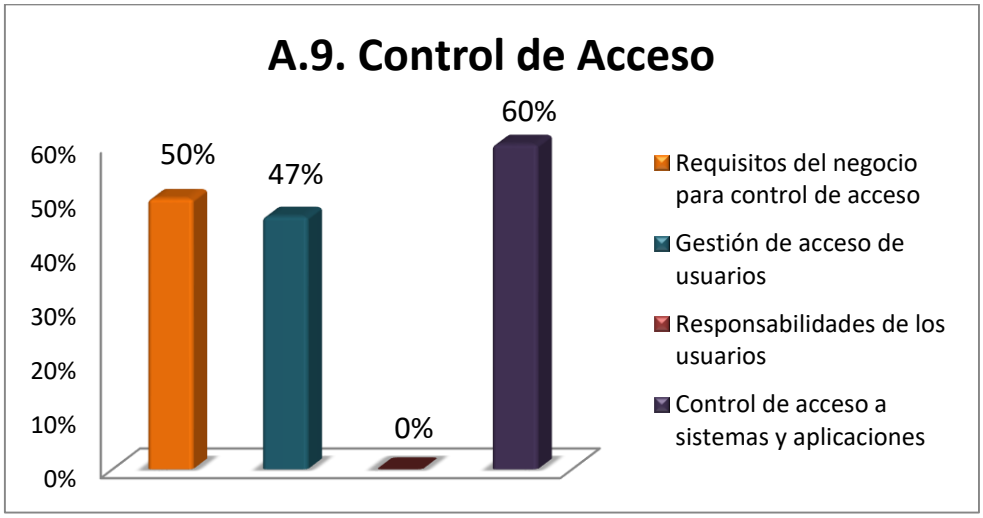
7	SEGURIDAD DE LOS RECURSOS HUMANOS	RECOMENDACIÓN
7.1	Antes de asumir el empleo	7.1
7.1.1	Selección	Se deben implementar procedimientos formales de incorporación para el personal que no hace parte de la Policía Nacional o el Ministerio de Defensa.
7.1.2	Términos condiciones del empleo	Con respecto a seguridad de la información todos los funcionarios deben conocer la política y saber de su obligatorio cumplimiento, esto debe estar en el contrato de trabajo.
7.2	Durante la ejecución del empleo	7.2
7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	Se deben realizar actas de instrucción y socialización de seguridad de la información de forma periódica, adicionalmente se debe realizar un cronograma de capacitación del SGSI y se deben evaluar evidencias y nuevas formas de sensibilización y coordinar con CSIRT-PONAL la realización de conferencias.
7.2.3	Proceso disciplinario	En la política debe estar definido el alcance disciplinario que conllevaría el incumplimiento o violación de las políticas de seguridad emitidas por la FORPO en materia de Seguridad de la información.
7.3	Terminación y cambio de empleo	7.3

7.3.1	Terminación o cambio de responsabilidades de empleo	Aunque se cuenta con un procedimiento y un documento de paz y salvo, este no se constata, adicionalmente se deben contar un una plataforma de usuarios centralizados en la cual se validen el estado laborar de los funcionarios y así proactivamente realizar bloqueos por inhabilidades laborales



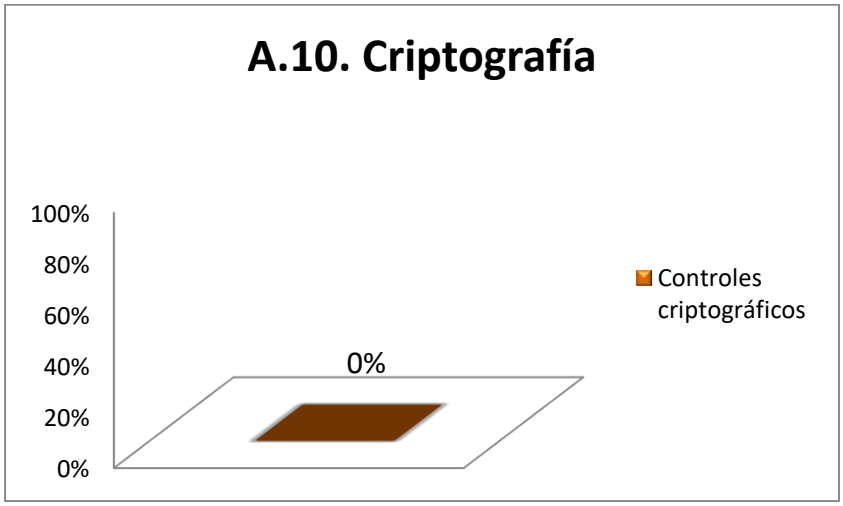
8	GESTIÓN DE ACTIVOS	RECOMENDACIONES
8.1	Responsabilidad por los activos	8.1
8.1.1	Inventario de activos	Se debe implementar un software que le permita contar a FORPO con un mapeo de sus activos, riesgos, planes de mitigación y controles implementados. Se debe realizar un análisis de riesgos y base en los resultados, se deben realizar un inventario de activos categorizándolos en (infraestructura, hardware, software, información y personas)
8.1.2	Propiedad de los activos	En el software o sistema utilizado se debe asignar a cada activo un propietario y custodio
8.1.3	Uso aceptable de los activos	Se deben realizar campañas, recalcando el uso correcto de las aplicaciones. Todos los usuarios que realicen uso de las aplicaciones de

		FORPO deben tener soporte de sus usuarios.
8.1.4	Devolución de activos	Existe un control de entrega de equipos, pero este no tiene trazabilidad por el jefe directo se sugiere cargar los inventarios al jefe de grupo o área y este asignar a los funcionarios para mejorar la trazabilidad y responsables de los equipos
8.2	Clasificación de la información	8.2
8.2.1	Clasificación de la información	Se debe definir una clasificación de la información, publica, privada, reservada y/o secreta según su impacto en el estado.
8.2.2	Etiquetado de la información	Una vez implementada una clasificación de la información se deben herramientas tipo DLP (Data Loss Prevention) para validar como se transfiere o comparte este tipo de información
8.2.3	Manejo de activos	Incluir en la Política, el manejo de activos asignados
8.3	Manejo de medios de soporte	8.3
8.3.1	Gestión de medios de soporte removibles	Se deben implementar herramientas que verifiquen y controlen los periféricos de los equipos de cómputo, herramientas tipo DLP (Data Loss Prevention)
8.3.2	Disposición de los medios de soporte	Realizar borrado seguro no solo a los equipos de baja sino a los de reasignación
8.3.3	Transferencia de medios de soporte físicos	Diseñar procedimientos y formatos para la entrega de información física o digital, esto debe ir alineado con la clasificación de la información

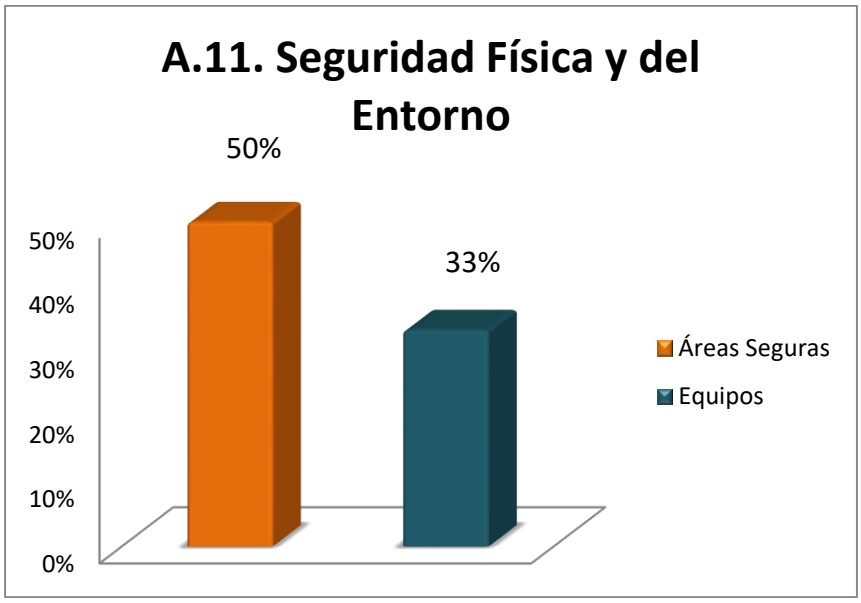


9	CONTROL DE ACCESO	RECOMENDACIONES
9.1	Requisitos del negocio para control de acceso	9.1
9.1.1	Política de control de acceso	Implementar un control de identidades e integrarlo con todas las aplicaciones del FORPO, de esta forma validar estado laborar, etc.
9.1.2	Acceso a redes y a servicios en red	Cuentan con Vlan sin embargo se sugiere implementar un monitoreo por Firewall, IPS del proxy de navegación
9.2	Gestión de acceso de usuarios	9.2
9.2.1	Registro y cancelación del registro de usuarios	Implementar un control de identidades e integrarlo con todas las aplicaciones del FORPO, de esta forma validar estado laborar, etc.
9.2.2	Suministro de acceso de usuarios	
9.2.3	Gestión de derechos de acceso privilegiado	Implementar un procedimiento para entregar roles al aplicativo Linyx
9.2.4	Gestión de información de autenticación secreta de usuarios	Aunque los equipos se encuentran en el dominio se deben implementar la alta disponibilidad de los servicios y por otra parte implementar un manejo de identidades en el sistema de información Linyx
9.2.5	Revisión de los derechos de acceso de usuarios	Implementar un control de identidades e integrarlo con todas las aplicaciones del FORPO, de esta forma validar estado laborar, etc.
9.2.6	Cancelación o ajuste de los derechos de acceso	Implementar un control de identidades e integrarlo con todas las aplicaciones del FORPO, de esta forma validar estado laborar, etc.
9.3	Responsabilidades de los usuarios	9.3
9.3.1	Uso de información de autenticación secreta	De acuerdo a la clasificación de la información y la política, adquirir software para el cifrado de la información que por su confidencialidad lo amerite, sea para almacenamiento o transferencia.
9.4	Control de acceso a sistemas y aplicaciones	9.4
9.4.1	Restricción de acceso a información	Se realiza por dominio, pero se sugiere la implementación de un servidor de archivos que garantice la confidencialidad, integridad y disponibilidad de la información ante falla.
9.4.2	Procedimiento de ingreso seguro	Implementar políticas de acceso seguro a los aplicativos del FORPO, políticas de contraseña, bloqueo por número de intentos.

9.4.3	Sistema de gestión de contraseñas	Existe para dominio pero no para los aplicativos, implementar políticas de contraseñas con un manejo de identidades
9.4.4	Uso de programas utilitarios privilegiados	Para los equipos de cómputo se maneja adecuadamente mediante el dominio.
9.4.5	Control de acceso a códigos fuente de programas	Implementar software de control de aplicaciones y corrupción del código fuente de la aplicaciones, con el fin de evitar copias no autorizadas.

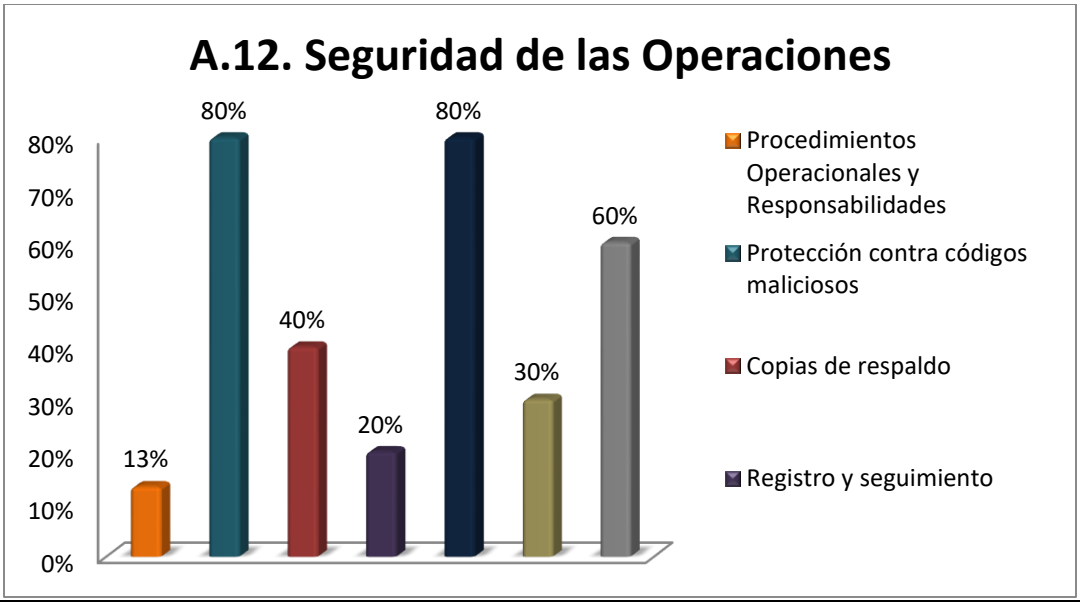


A.10..	**CRIPTOGRAFÍA**	
A.10.1.	**Controles criptográficos**	
10.1.1	Política sobre el uso de controles criptográficos	Crear política de uso de cifrado para almacenamiento de archivos, transferencia de archivos
10.1.2	Gestión de claves	Implementar software de cifrado con base en la clasificación de la información.



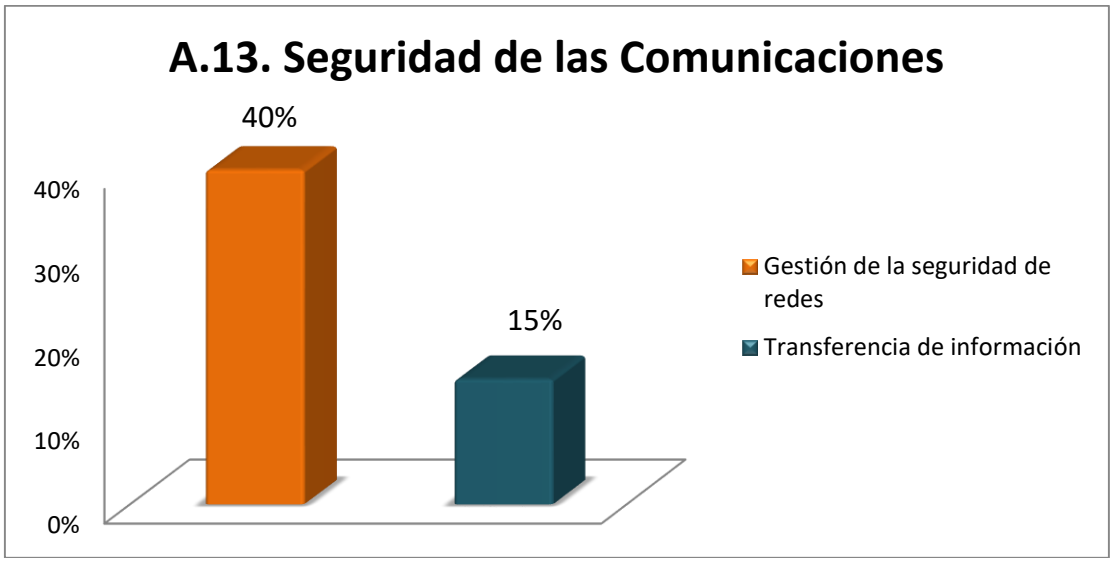
11	SEGURIDAD FÍSICA Y AMBIENTAL	RECOMENDACIONES
11.1	Áreas seguras	11.1
11.1.4	Perímetro de seguridad física	Definir política de almacenamiento de los CCTV
11.1.2	Controles de acceso físico	Se encuentra en óptimas condiciones
11.1.3	Seguridad de oficinas, recintos e instalaciones	Se encuentra en óptimas condiciones
11.1.4	Protección contra amenazas externas y ambientales	Se tiene plan de evacuación y se cuenta con botiquines y camillas en los pisos del edificio. Se cuenta con un sistema de control de incendios y extintores
11.1.5	Trabajo en áreas seguras	Se encuentra en óptimas condiciones
11.2	Equipos	11.2
11.2.1	Ubicación y protección de los equipos	Definir campañas de sensibilización de Escritorio y pantallas limpias.
11.2.2	Servicios públicos de soporte.	Se cuenta con una ups, una planta eléctrica.
11.2.3	Seguridad del cableado	Se debe contar con cableado estructurado en todo el edificio
11.2.4	Mantenimiento de equipos.	Se debe contar con un plan de mantenimientos
11.2.5	Retiro de activos	Se debe realizar un procedimiento para el retiro de equipos de las instalaciones
11.2.6	Seguridad de equipos y activos fuera del predio	Se debe crear una política de acceso directo por dominio, cifrado de discos, usuario y contraseña.
11.2.7	Disposición segura o reutilización de equipos	Se realiza el procedimiento de borrado seguro solo a los discos duros de equipo a dar de bajar, se

		debe incluir los equipos que se van a reasignar.
11.2.8	Equipos de usuario desatendido	La Política se aplica en la actualidad
11.2.9	Política de escritorio limpio y pantalla limpia	Se evidencia falta de cultura de los funcionarios quienes guardan en el escritorio documentos. Socializar y reforzar la cultura a través de brigadas y comparendos.

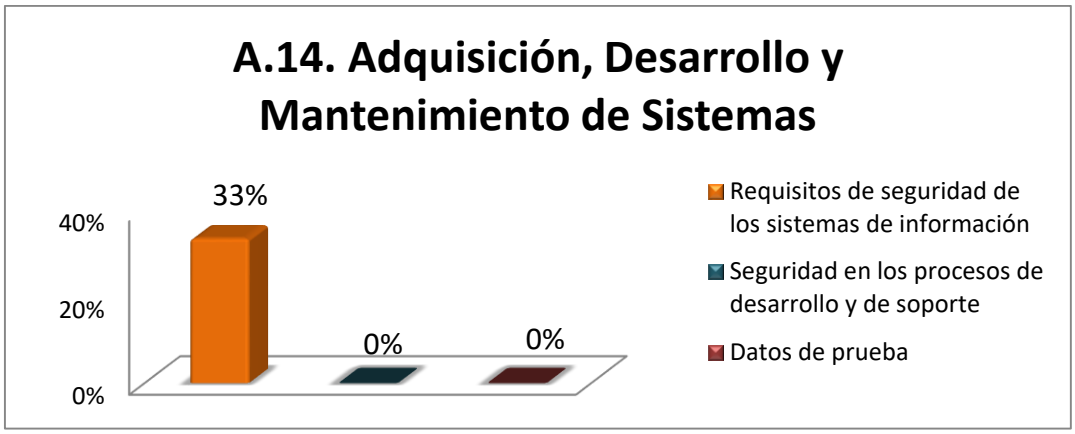


A.12..	**SEGURIDAD DE LAS OPERACIONES**	
A.12.1.	**Procedimientos Operacionales y Responsabilidades**	**RECOMENDACIONES**
A.12.1.1	Documentación de los procedimientos de operación	Se debe hacer un manual o instructivo por cada sistema operado en FORPO
A.12.1.2	Gestión del cambios	Se debe crear un comité de cambios tecnológicos
A.12.1.3	Gestión de la capacidad	Se debe generar un formato para la validación de capacidad de los sistemas de información en hw y sw
A.12.1.4	Separación de las instalaciones de desarrollo, pruebas y operación	No aplica
A.12.2.	**Protección contra códigos maliciosos**	
A.12.2.1	Controles contra códigos maliciosos	Se cuenta con software de antivirus
A.12.3.	**Copias de respaldo**	

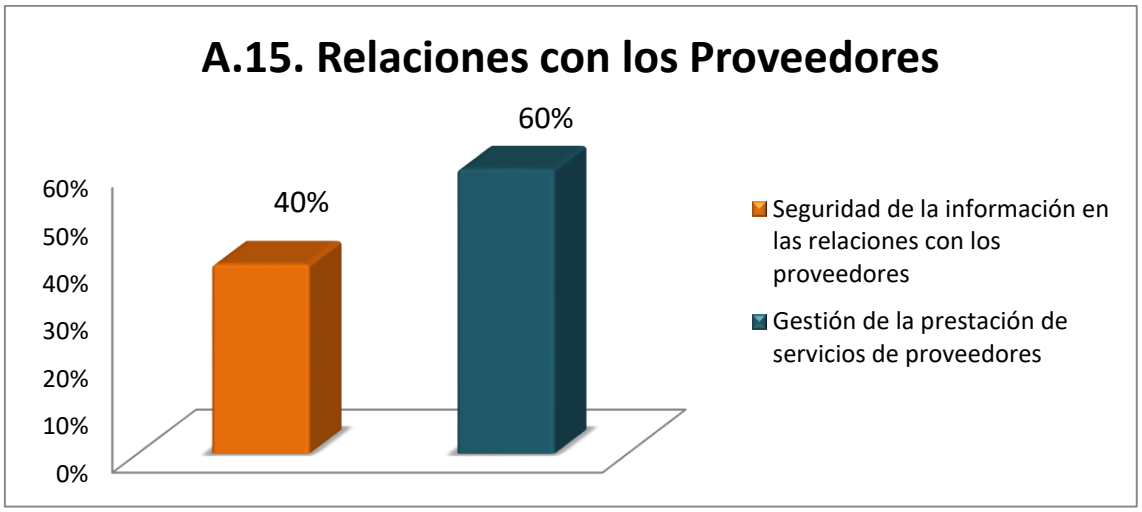
A.12.3.1	Copias de respaldo de la información	Se debe implementar servidor de archivos con el fin de salvaguardar la información de los funcionarios, este debe contar con políticas de backup
A.12.4.	**Registro y seguimiento**	
A.12.4.1	Registro de eventos	Se debe implementar un Correlacionador de eventos .
A.12.4.2	Protección de la información de registro	Se debe implementar un Correlacionador de eventos
A.12.4.3	Registros del administrador y del operador	Se debe implementar un Correlacionador de eventos
A.12.4.4	Sincronización de relojes	Los relojes de las máquinas se encuentran en el dominio se encuentran sincronizados con la hora legal Colombiana
A.12.5.	**Control de software operacional**	
A.12.5.1	Instalación de software en sistemas operativos	Se hace por dominio, pero se debe contar con un software que verifique el software instalado en los equipos
A.12.6.	**Gestión de la vulnerabilidad técnica**	
A.12.6.1	Gestión de las vulnerabilidades técnicas	Se debe implementar un procedimiento y una herramienta para realizar análisis de vulnerabilidades
A.12.6.2	Restricciones sobre la instalación de software.	Se hace por dominio, pero se debe contar con un software que verifique el software instalado en los equipos
A.12.7.	**Consideraciones sobre auditorías de sistemas de información**	
A.12.7.1	Controles de auditorías de sistemas de información.	Se realiza Actualmente, sin embargo se sugiere contar con un Correlacionador de eventos



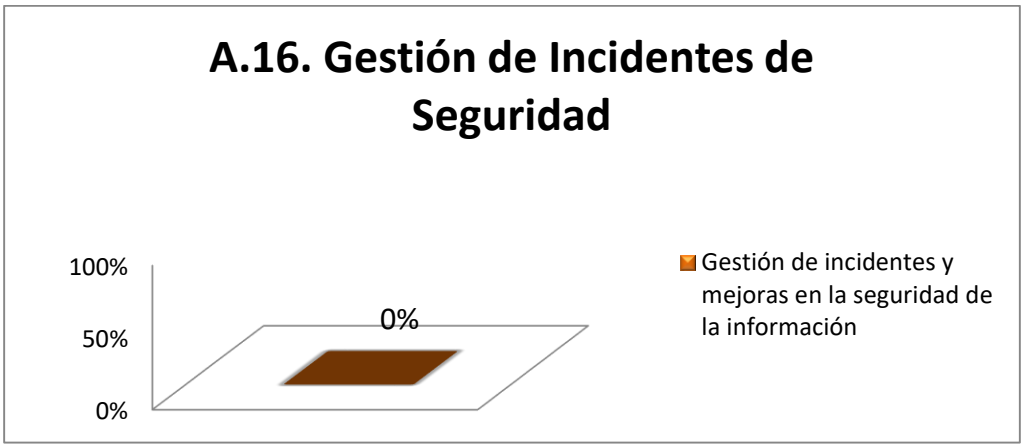
13	SEGURIDAD DE LAS COMUNICACIONES	RECOMENDACIONES
13.1	Gestión de la seguridad de redes	13.1
13.1.1	Controles de redes	Cuenta con firewall
13.1.2	Seguridad de los servicios de red.	Se debe realizar un segmento de invitados y otro para el área de pagos o tesorería
13.1.3	Separación en las redes	Se encuentra segmentado por una Vlan
13.2	Transferencia de información	13.2
13.2.1	Políticas y procedimientos de transferencia de información	Se debe crear una política de transferencia de información
13.2.2	Acuerdos sobre transferencia de información	Se debe crear una política de transferencia de información
13.2.3	Mensajes electrónicos	Se debe crear una política de transferencia de información.
13.2.4	Acuerdos de confidencialidad o de no divulgación	Se debe crear un formato para acuerdos de confidencialidad que aplique a todas las áreas



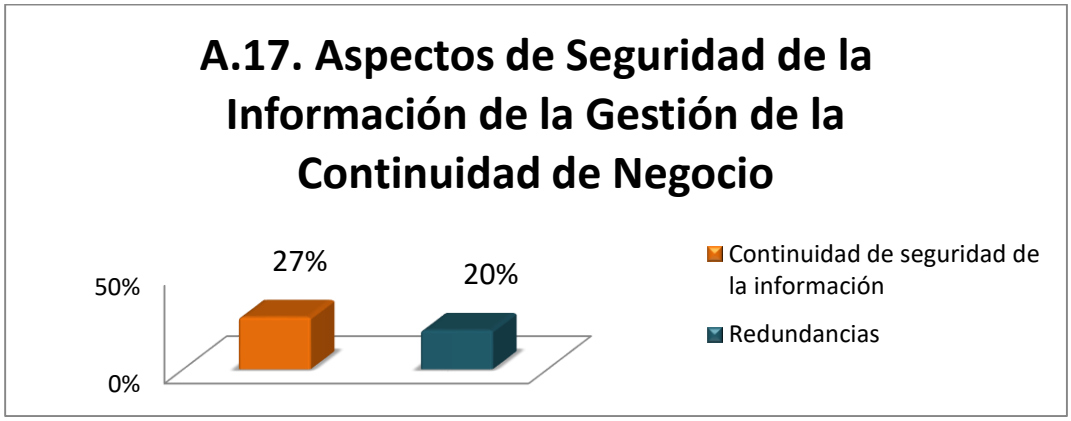
A.14..	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**	
A.14.1.	**Requisitos de seguridad de los sistemas de información**	**RECOMENDACIONES**
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Solicitar acuerdos de confidencialidad en todos los contratos
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	Cuentan con firewall, se sugiere realizar análisis de vulnerabilidades al portal para evitar intrusiones.
A.14.1.3	Protección de transacciones de servicios de aplicaciones	Se sugiere implementar auditvault o similares en las bases de datos
A.14.2.	**Seguridad en los procesos de desarrollo y de soporte**	
A.14.2.1	Política de desarrollo seguro	Aunque los procesos no son desarrollados en el FORPO se sugiere implementar unas probas de aceptación, enfocadas en calidad del desarrollo del software y de vulnerabilidades técnicas del desarrollo y del hardware de la aplicación
A.14.2.2	Procedimientos de control de cambios en sistemas	
A.14.2.3	Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones	
A.14.2.4	Restricciones en los cambios a los paquetes de software	
A.14.2.5	Principios de construcción de los sistemas seguros	
A.14.2.6	Ambiente de desarrollo seguro	
A.14.2.7	Desarrollo contratado externamente	
A.14.2.8	Pruebas de seguridad de sistemas	
A.14.2.9	Prueba de aceptación de sistemas	



A.15.	RELACIONES CON LOS PROVEEDORES	
A.15.1.	**Seguridad de la información en las relaciones con los proveedores**	**RECOMENDACIONES**
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	Se debe incluir en los contratos el cumplimiento de la Política de Seguridad de la Información y la firma de formatos de confidencialidad
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	En la etapa de contratación se deben contemplar los riesgos relacionado con la seguridad de la información, como confidencialidad, integridad y disponibilidad de los bienes y servicios en la cadena de suministro
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	En la etapa de contratación se deben contemplar los riesgos relacionado con la seguridad de la información, como confidencialidad, integridad y disponibilidad de los bienes y servicios en la cadena de suministro
A.15.2.	Gestión de la prestación de servicios	
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	Se realiza de acuerdo a la supervisión
A.15.2.2	Gestión de cambios a los servicios de los proveedores	Se debe hacer cumplir a los proveedores el comité de cambios creado por FORPO

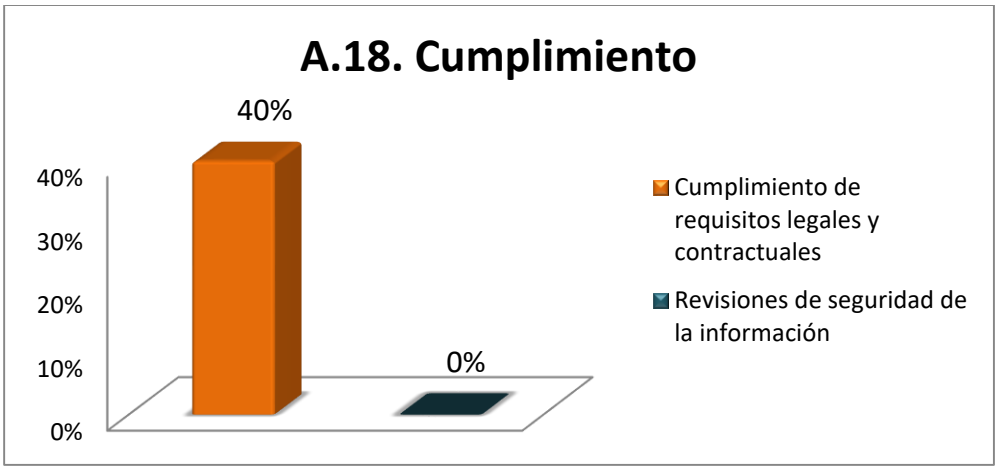


16.1	Gestión de incidentes y mejoras en la seguridad de la información	RECOMENDACIONES
16.1.1	Responsabilidades y procedimientos	Se deben crear procedimientos, guías y formatos para la atención de incidentes informáticos, en la herramienta de tickets de FORPO se debe crear una opción que permita a los funcionarios notificar posibles incidentes de seguridad
16.1.2	Reporte de eventos de seguridad de la información	
16.1.3	Reporte de debilidades de seguridad de la información	
16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos.	
16.1.5	Respuesta a incidentes de seguridad de la información	
16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	



17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO	RECOMENDACIONES
17.1	Continuidad de seguridad de la información	
17.1.1	Planificación de la continuidad de la seguridad de la información	Se debe documentar un BIA (Análisis del Impacto del Negocio) y con base en este

		realizar un BCP (Plan de continuidad del negocio) y un DRP (Plan de recuperación ante desastre).
17.1.2	Implementación de la continuidad de la seguridad de la información	Una vez se cuente con el BIA, BCP y el DRP se deben priorizar los sistemas que deben contar con contingencia, sea activo-activo, activo-pasivo (Backups, Data Standalone, etc).
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Tanto el BIA como el DRP deben contar con un plan de pruebas definido por el FORPO y al igual que una actualización.
17.2	Redundancias	
17.2.1	Disponibilidad de instalaciones de procesamiento de información	Se debe implementar en el BCP y DRP



A.18..	CUMPLIMIENTO	
A.18.1.	**Cumplimiento de requisitos legales y contractuales**	
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Se debe tener en cuenta un asesor jurídico que realice difusión de información sobre legislación legal aplicable en cuanto a seguridad de la información en FORPO.
A.18.1.2	Derechos de propiedad intelectual	No aplica por el momento
A.18.1.3	Protección de registros	Se debe contar con un Correlacionador de eventos y políticas definidas para tiempos de almacenamiento.
A.18.1.4	Privacidad y protección de información de datos personales	Se debe implementar una política
A.18.1.5	Reglamentación de controles criptográficos	Se debe implementar una política y software de cifrado para los casos que lo amerite

A.18.2.	**Revisiones de seguridad de la información**	
A.18.2.1	Revisión independiente de la seguridad de la información	En el área de control interno se debe contar con el talento humano que permita realizar auditorías de revisión del SGSI, tanto documentales como técnicas.
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	
A.18.2.3	Revisión del cumplimiento técnico	