IMPLEMENTACIÓN DE LA GESTIÓN DE LA MOVILIDAD EMPRESARIAL (ENTERPRISE MOBILITY MANAGEMENT - EMM) PARA LA GESTION DEL CORREO CORPORATIVO EN EL DEPARTAMENTO PARA LA PROSPERIDAD SOCIAL – DPS

OSVALD CAMACHO HERNANDEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA
2015

IMPLEMENTACIÓN DE LA GESTIÓN DE LA MOVILIDAD EMPRESARIAL (ENTERPRISE MOBILITY MANAGEMENT - EMM) PARA LA GESTION DEL CORREO CORPORATIVO EN EL DEPARTAMENTO PARA LA PROSPERIDAD SOCIAL – DPS

OSVALD CAMACHO HERNANDEZ

Informe de trabajo de grado para optar al título de especialista en Seguridad Informática

Director:
Anivar Chaves Torres
Ingeniero de sistemas

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA
2015

Nota de aceptación

_____

_____

_____

_____

_____

_____
Jurado

_____
Jurado

_____
Jurado

Bogotá D.C, Octubre 2015

A toda mi familia, mis padres
Norberto y Celmira, mis
hermanos, mi esposa Stella,
mi hija Paula Milena,
con todo mi amor.

AGRADECIMIENTOS

El desarrollo de este proyecto ha requerido de un gran esfuerzo y mucha dedicación por parte del autor y su director.

Primeramente quiero agradecer a Dios por bendecirme y permitir que logre culminar este proceso de formación. A todas las personas que de una u otra forma contribuyeron en la realización del desarrollo de este proyecto.

Al ingeniero Anívar Chaves quien me proporcionó consejos y sugerencias en el proceso y desarrollo del presente proyecto, realizando un constante acompañamiento al realizar las revisiones de cada una de las etapas del desarrollo del proyecto.

Al ingeniero Jaime Valderrama Oficial de la Seguridad de Información del Departamento Para la Prosperidad Social – DPS, por apoyarme en el desarrollo de este proyecto proporcionándome la información relacionada con el mapa de riesgos y las políticas de seguridad de la información.

Al ingeniero Jaime Paiba Tibaduiza administrador del servicio de correo electrónico corporativo del Departamento para la Prosperidad Social – DPS, por atender gentilmente la entrevista realizada y por suministrarme la información requerida.

Osvald Camacho Hernández

CONTENIDO

Pág.

LISTA DE CUADROS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

INTRODUCCIÓN

El presente proyecto se desarrolla dentro del proceso de modernización del estado y del gobierno de TI, en el Departamento para la Prosperidad Social – DPS, el cual se encuentra implementado un Sistema de Gestión de Seguridad de la Información (SGSI) siguiendo los lineamientos de la norma internacional NTC-ISO/IEC 27001:2013 con la finalidad de garantizar la disponibilidad, integridad y disponibilidad de la información.

Este proyecto es desarrollado con la finalidad de realizar la implementación de la movilidad empresarial en el Departamento para la Prosperidad Social - DPS, analizar las vulnerabilidades, amenazas y riesgos existentes en la seguridad de la información, que se derivan de la utilización del servicio de correo electrónico corporativo en los dispositivos móviles.

El proyecto se ha organizado en cinco capítulos a saber: los capítulos denominados “el problema de investigación”, “marco de referencia”, “metodología”, “Resultados” y “conclusiones”, los cuales permiten desarrollar el problema planteado en el capítulo uno. El objetivo general se estable a cómo mejorar la seguridad en la prestación del servicio de correo electrónico corporativo en dispositivos móviles, mediante la definición de políticas y herramientas para gestionar dichos dispositivos.

Para el efecto, se desarrolla el proyecto según sus objetivos específicos que establecen la necesidad de identificar las amenazas y vulnerabilidades relacionadas con el servicio de correo electrónico corporativo y la definición de controles necesarios para realizar la gestión de este servicio a través de dispositivos móviles. Adicionalmente, se definen las políticas que se proponen para la gestión de los dispositivos móviles en los que se tiene acceso el servicio de correo electrónico corporativo y la correspondiente estrategia de capacitación de usuarios del servicio de correo electrónico corporativo en dispositivos móviles de propiedad de los usuarios o de la Entidad.

El análisis anterior es derivado del levantamiento de información relacionado con la aplicación de encuestas a funcionarios del Departamento para la Prosperidad Social – DPS, de las entrevistas realizadas a funcionarios que desarrollan los roles de Administrador del servicio de correo electrónico corporativo y del Oficial de

seguridad quienes se convierten en información de primera mano.

En el capítulo cuatro se presentan los requisitos del sistema y se listan las vulnerabilidades encontradas. En este mismo capítulo, se plantean las políticas para la gestión de dispositivos móviles en los que se utilizará el servicio de correo electrónico corporativo en el DPS, por último en este mismo capítulo se plantean el plan de sociabilización y de capacitación de usuarios y la implementación de la solución, la cual es una herramienta que hace parte de la suite de los producto de *Mcafee* que la Entidad ha adquirido.

Para terminar, es importante tener en cuenta las conclusiones a las que se ha llegado después de realizar el desarrollo de este proyecto. En este apartado se concluye por ejemplo que la movilidad empresarial está cobrando vida en todas las empresas dada su importancia que representa ofertar y hacer uso de aplicaciones a través de los dispositivos móviles. La utilización de estos dispositivos en el consumo de servicios o aplicaciones de la Entidad originan una serie de vulnerabilidades de la información, que deben ser controlados con la ayuda de herramientas tecnológicas y que para el caso del DPS corresponde a la herramienta *EMM* de *Mcafee*, por satisfacer los requerimientos identificados de la solución de este proyecto.

1. EL PROBLEMA DE INVESTIGACIÓN

1.1 DESCRIPCIÓN

Actualmente en las empresas se han incrementado la cantidad de dispositivos móviles. Cada vez más empleados realizan sus actividades usando tabletas y teléfonos inteligentes. La época del trabajo de oficina frente a una computadora de escritorio está quedando rápidamente atrás. La movilidad que antes era un privilegio de los directivos, ahora se ha extendido a muchos otros empleados en las organizaciones.

Por otra parte, en grandes ciudades, donde los problemas del tráfico pueden complicar una apretada agenda de reuniones fuera de la oficina, el uso de los dispositivos móviles resulta un aliado para desarrollar dichas actividades como consultar la agenda, conexión a *Internet, chat* y demás aplicaciones que posibilitan el contacto con personas de la organización ya sean funcionarios o clientes a los que se les debe brindar un servicio por parte de la Entidad.

Según encuestas aplicadas por la compañía TechTarget[1] , desde el 2013 los resultados de la encuesta anual de prioridades de TI para América Latina, dejaban ver su importancia en un 34 por ciento de las respuestas relacionadas con las iniciativas de la movilidad para las organizaciones latinoamericanas. Lo cual es la segunda prioridad de TI para las empresas de la región en 2015.

Según la encuesta en 2014, los encuestados indicaron que el principal objetivo al permitir el uso de dispositivos móviles en la empresa es responder a la demanda de los usuarios finales para tener soluciones personalizadas. La

[1] PÉREZ ARBESÚ, Lizzette, Empresas latinoamericanas apuestan fuerte por la movilidad en 2015: Los dispositivos móviles se han filtrado fuertemente en las empresas. Es tiempo de sustentar esta tendencia con aplicaciones y servicios a la medida. Consultado el 5 de mayo 2015. Disponible en: http://searchdatacenter.techtarget.com/es/cronica/Empresas-latinoamericanas-apuestan-fuerte-por-la-movilidad-en-2015

encuesta sostiene que la seguridad no ha sido un aspecto relevante en los proyectos de movilidad, pues sólo el 16% contempla aspectos relacionados con la seguridad de dispositivos móviles. Se espera, que los nuevos proyectos involucren la protección de los dispositivos móviles y de la información. La prevención de pérdida de datos, gestión de vulnerabilidades, gestión de accesos e identidades, cifrado, seguridad en la nube y seguridad de punto final.

La solución administrativa de movilidad empresarial, debe incorporar la mejor tecnología que se requiere para mejorar la productividad y proteger la información en dispositivos y aplicaciones, para ello es necesario contar con una solución que ofrezca a las empresas la seguridad de las herramientas móviles de su fuerza de trabajo.

En este proyecto se estudia la seguridad de la movilidad empresarial en el Departamento para la Prosperidad Social – DPS. El DPS es una entidad gubernamental creada mediante decreto 4155 de noviembre de 2011 cuyo objetivo es: formular, adoptar, dirigir, coordinar y ejecutar las políticas, planes generales, programas y proyectos para la superación de la pobreza, la inclusión social, la reconciliación, la recuperación de territorios, la atención y reparación a víctimas de la violencia, la atención a grupos vulnerables, población discapacitada y la reintegración social y económica y la atención y reparación a víctimas de la violencia a las que se refiere el artículo 3° de la Ley 1448 de 2011[2]; actividades que serán desarrolladas directamente o a través de sus entidades adscritas o vinculadas, en coordinación con las demás entidades u organismos competentes. El DPS está conformado en la actualidad por 35 direcciones regionales, que actúan como enlace entre el territorio y el nivel Nacional.

[2] DEPARTAMENTO ADMINISTRATIVO PARA LA PROSPERIDAD SOCIAL – DPS Consultado el 5 de mayo 2015. en disponible en internet: http://www.dps.gov.co/contenido/contenido.aspx?catID=3&conID=544&pagID=18024

Dentro del proceso de modernización del estado y del gobierno de TI, el Departamento para la Prosperidad Social – DPS se encuentra implementado un Sistema de Gestión de Seguridad de la Información (SGSI) siguiendo los lineamientos de la norma internacional NTC-ISO/IEC 27001:2013 con la finalidad de garantizar la integridad y disponibilidad de la información.

Así mismo, ha tomado como referencia el Manual de Gobierno en Línea 3.1, especialmente lo referente a la actividad de Implementación del Sistema de Gestión de Seguridad de la Información (SGSI) perteneciente al componente de elementos transversales, la cual está definida mediante el decreto 2693 de 2012. Este proceso de implementación requiere de recursos tanto tecnológicos como de personal idóneo para adelantar las actividades que garanticen una adecuada implementación de dicho sistema de gestión.

La administración de dispositivos móviles es una tarea crítica en la Entidad que debe reforzarse y que debe ser atendida de manera integral en un contexto más amplio, dentro de la cual la gestión del correo electrónico institucional almacenado en los dispositivos móviles juega un papel importante unido a la caracterización de una estrategia de movilidad de la Entidad.

En los últimos años el DPS ha permitido el uso de clientes de correo electrónico en los dispositivos móviles de los funcionarios, bien sea que estos sean propios o de la entidad, lo cual ha permitido el acceso de forma ubicua a la información y de esta forma ha facilitado el desarrollo de las funciones encomendadas a cada funcionario.

Sin embargo, esta situación ha derivado en la existencia de vulnerabilidades de seguridad de la información debido a que no existe un mecanismo de control de acceso a la información corporativa que es almacenada en el dispositivo o de un

mecanismo de almacenamiento seguro que prevenga un posterior acceso no autorizado a la información.

Esta situación puede provocar perdida de la confidencialidad de los datos corporativos, modificación no autorizada, suplantación de identidad y fuga de información, que afectarán el funcionamiento de la organización, su reputación y podrían tener implicaciones legales.

Esta situación expuesta, se presenta porque actualmente el DPS no cuenta con una administración de los dispositivos móviles y especialmente del servicio de correo electrónico corporativo almacenado en dichos dispositivos, el cual es utilizado por funcionarios a lo largo y ancho del territorio nacional sin un control y seguimiento de este servicio.

Se evidencia una carencia de un conjunto de políticas y directivas corporativas definidas para el uso de dispositivos móviles, las cuales deben tener como objetivo la gestión del uso del servicio de correo electrónico en los dispositivos móviles que son propiedad de la entidad o de terceros, de una forma segura. Actualmente, el servicio de correo electrónico se gestiona mediante la utilización de un servidor *exchange*, el cual cumple con los lineamientos institucionales y políticas de utilización.

Adicionalmente, con el avance de la tecnología alrededor del 70 por ciento de los funcionarios de la Entidad cuentan con dispositivos móviles de su propiedad o que la Entidad les otorga para el cumplimiento de sus funciones y como se menciona anteriormente no existen mecanismos de control sobre estos dispositivos, que de alguna manera minimicen riegos de seguridad de la información asociados al uso del correo corporativo en dichos dispositivos.

La entidad se halla expuesta a vulnerabilidades de seguridad de la información, al utilizar dichos dispositivos sin ninguna política de seguridad que restrinja y gestione elementos de correo corporativo en los dispositivos móviles utilizados por los funcionarios.

Lo anterior evidencia la necesidad de mejorar la gestión de la movilidad empresarial (*Enterprise Mobility Management - EMM*), donde la Administración de Dispositivos Móviles (*Mobile Device Management - MDM*) y la Administración de Aplicaciones Móviles (*Mobile Application Management - MAM*) son dos componentes indispensables.

1.2 FORMULACIÓN

¿Cómo mejorar la seguridad en la prestación del servicio de correo electrónico corporativo en dispositivos móviles en el Departamento para la Prosperidad Social – DPS?

1.3 SUBPREGUNTAS

- ¿Cuáles son los requisitos funcionales y no funcionales relacionados con el uso del correo electrónico corporativo en dispositivos móviles en el DPS, considerando el contexto organizacional y tecnológico, y la alineación con los controles de la norma NTC-ISO/IEC 27001:2013?

- ¿Qué políticas permitirían el uso del servicio de correo electrónico corporativo en el Departamento de la Prosperidad Social – DPS, de una forma segura?

- ¿Cómo implementar la arquitectura de la solución *EMM* para gestionar el servicio de correo electrónico corporativo en los dispositivos móviles en el

DPS?

1.4 OBJETIVOS

1.4.1 General

Mejorar la seguridad en la prestación del servicio de correo electrónico corporativo en dispositivos móviles en el DPS mediante políticas y herramientas de gestión de la movilidad empresarial.

1.4.2 Específicos

- Realizar un levantamiento y análisis de requerimientos relacionados con el uso del correo electrónico corporativo en dispositivos móviles en el DPS, considerando el contexto organizacional y tecnológico, y la alineación con los controles de la norma NTC-ISO/IEC 27001:2013 y las necesidades de la Entidad.

- Diseñar e implementar las políticas de seguridad informática que permitan el uso del servicio de correo electrónico corporativo en el Departamento de la Prosperidad Social – DPS, de una forma segura y funcional utilizando dispositivos móviles.

- Proponer la Implementación de la arquitectura *EMM* para gestionar el servicio de correo electrónico corporativo en los dispositivos móviles en DPS.

- Diseñar un programa de capacitación para los usuarios que utilizarían el servicio, lo cual hace parte y está vinculado con el plan de sensibilización en seguridad de la información del DPS.

1.5 JUSTIFICACIÓN

La Seguridad Informática es relevante en áreas tecnológicas del entorno nacional e internacional, en consecuencia, se requiere no solo conocer y saber aplicar adecuadamente elementos tecnológicos sino también herramientas gerenciales de planeación de continuidad, manejo de incidentes y recursos humanos, auditoria, seguridad física e incluso la adecuada comprensión de los aspectos legales de estos temas.

En el DPS no se cuenta con mecanismos de control del correo corporativo en los dispositivos móviles, que utilizan los funcionarios para cumplir sus actividades y existe ausencia de políticas relacionadas con el uso del correo corporativo en dispositivos móviles. Lo que hace necesario el diseño de políticas y la puesta en marcha de herramientas tendientes a minimizar los riesgos de seguridad de la información asociados al uso del correo electrónico corporativo en los dispositivos móviles que utilizan los funcionarios.

Para ello es necesario diseñar políticas de seguridad de la información que determinen y controlen el uso del servicio de correo electrónico en dispositivos móviles, en función del análisis de riesgos que se obtenga del levantamiento de la información. Adicionalmente, se requiere implementar una herramienta que gestione de manera automática los criterios definidos en la política de seguridad de la información, esto permitiría cumplir con el objetivo general de proyecto.

De otro lado también, se justifica el desarrollo de este proyecto dado que se puede ver como un aporte al cumplimiento del decreto 2693 de 2012, que define la estrategia de gobierno en línea y en el cual se indica que las entidades públicas del orden nacional deben lograr un porcentaje de avance igual al 95%

en el componente de elementos transversales, del cual un 25% corresponde a la implementación de un SGSI.

2. MARCO DE REFERENCIA

2.1 ANTECEDENTES

Como antecedentes de este proyecto se pueden mencionar los siguientes proyectos:

En el año 2013, Colombia Digital, desarrollo el proyecto denominado Estrategia de TI en el Estado colombiano[3], el cual se encargó de formular y diseñar la política pública, lineamientos y estándares de la Gestión de TI en el Estado; así como desarrollar las capacidades para la gestión efectiva de TI en el país.

Otro caso referenciado como antecedente de la presente investigación en Colombia es el de la Pontificia Universidad Javeriana[4] ubicada en la ciudad de Cali, la cual desarrollo en el año 2012 un proyecto relacionado con la utilización de máquinas virtualizadas con la finalidad de que estudiantes y profesores pudieran compartir recursos en el desarrollo de sus proyectos. Los beneficios obtenidos a partir de la implementación del proyecto, cabe mencionar la reducción del costo de licenciamiento, de rotaciones de equipos, de gastos de energía, de mantenimiento y un aumento en productividad de los equipos, además de una disminución a cero de los equipos en reparación.

Otro caso de implementación de la movilidad empresarial es el realizado por la empresa DEPRISA[5] para optimizar los procesos de envío y el seguimiento de los

---

[3] CORPORACIÓN COLOMBIA DIGITAL, Estrategia de TI en el Estado colombiano. Consultado el 5 de mayo 2015. Disponible en: http://www.colombiadigital.net/quienes-somos/item/8022-estrategia-de-ti-en-el-estado-colombiano.html

[4] VEGA Salvador. Estrategias de movilidad y éxito empresarial. Consultado el 26 de julio 2015. Disponible en: http://www.larepublica.co/estrategias-de-movilidad-y-%C3%A9xito-empresarial_245116

[5] DINERO. Deprisa fortalece su negocio con tecnología. Citado en 23 de Septiembre de 2014. Disponible en: http://www.dinero.com/empresas/articulo/tecnologia-usada-deprisa/201300

paquetes en tiempo real. El proyecto incluye la incorporación de 210 computadoras móviles robustas MC65 de *Motorola Solutions* y alrededor de 700 impresoras *Zebra* modelos GT800 y ZM400, así como una gama de soluciones móviles de tecnología de punta, lo que permitirá imprimir mayor eficiencia a la distribución y obtener un mayor control de los envíos.

En el ámbito internacional se ha identificado la investigación de Panrico, compañía líder en el mercado español y portugués de bollería y pan de molde. Esta organización implementó una solución de gestión de movilidad empresarial que permitiera la sustitución de terminales industriales por tabletas con sistema operativo *Android*, con el fin de utilizarlos como terminales de puntos de venta, según lo plantea el articulo denominado Panrico incrementa productividad de sus empleados con el uso de las soluciones de AirWatch[6].

En Perú, la empresa Credinka[7], una institución financiera, implementó una plataforma de servidores Citrix completa con la aplicación *XenServer*, *XenApp* para la entrega de aplicaciones y *XenDesktop* para la virtualización de escritorios, montados sobre equipos Blade de IBM basados en *Windows Server* 2008. Este proyecto tuvo como finalidad contar con centros de datos confiables para ampliar su negocio en el territorio Nacional. Con la implementación de Citrix, Credinka redujo sus gastos en conexiones de banda ancha, uso de energía eléctrica, tiempo de aprovisionamiento y reducción significativa en costos de licenciamiento. Adicionalmente se encripta la información que viaja por

---

[6] AIRWATCH Panrico incrementa productividad de sus empleados con el uso de las soluciones de AirWatch. Consultado el 16 de julio 2015.Disponible en: http://www.air-watch.com/uploads/global-media/es-airwatch-panrico.pdf

[7] MARTÍNEZ Marcelo. La compañía financiera dedicada al microcrédito amplía su cobertura en las zonas urbanas y rurales de Perú a través de la tecnología Citrix que le permite distribuir sus aplicaciones de negocios en todo el país. Consultado el 16 de julio 2015. Disponible en: https://lac.citrix.com/customers/caso-credinka-peru-es.html

las redes y toda la operación del negocio se sostiene sobre la plataforma *Citrix Xen App*

Otro caso citado como antecedente corresponde a la utilización de la aplicación *Dell EMM*[8], en esta aplicación los clientes pueden aprovechar una solución de movilidad integrada para la gestión segura de dispositivos y espacios de trabajo. Adicionalmente, *Dell EMM* incluye aplicaciones de espacio de trabajo basadas en contenedores para facilitar la administración y la adopción segura de "trae tu propio dispositivo" *(BYOD)*.

Para los Smartphone y las tabletas de los empleados, *Dell Mobile Workspace* ofrece a los usuarios un acceso seguro a los datos corporativos y herramientas de productividad, incluyendo correo electrónico, calendario, contactos, navegador móvil y explorador de archivos.

2.2 MARCO TEÓRICO CONCEPTUAL

2.2.1 Gestión de la movilidad empresarial. La gestión de la movilidad empresarial es el conjunto de personas, procesos y tecnologías enfocadas en gestionar la creciente variedad de dispositivos móviles, redes inalámbricas, y servicios relacionados, para permitir el correcto uso de los dispositivos móviles en un contexto de negocios, según lo afirma la empresa TNX9 empresa de sistemas de gestión de telecomunicaciones y consultoría en su artículo llamado La movilidad empresarial.

---

[8] GUILARTE María . Dell muestra durante Dell World su apuesta por la innovación en software ante las nuevas tendencias IT. Consultado el 26 de julio 2015. Disponible en: http://www.muycomputerpro.com/2013/12/12/dell-enterprise-mobility-management.

[9] TNX. La movilidad empresarial. Consultado el 26 de julio 2015. Disponible en: http://tnxcorp.com/service/la-movilidad-empresarial/

El mismo artículo afirma que se trata de una disciplina creciente dentro de la empresa, que se ha vuelto cada vez más importante en los últimos años, ya que cada vez más los trabajadores adquieren *Smartphone* y *tablet* para el uso laboral y particular. Además están en la búsqueda de servicios de apoyo para poder usar sus dispositivos en el lugar de trabajo. Una estrategia de movilidad empresarial adecuada en una organización debe relacionar la disponibilidad del móvil para el trabajo a realizar, para de esta manera determinar cómo debe ser el proceso de alineamiento del negocio con el móvil y para apoyar a los trabajadores cuando estén usando los dispositivos en el lugar de trabajo.

Tal como lo afirma gerente general de Nubison[10] en su artículo gestión de la movilidad empresarial, según el cual, la incorporación de *smartphones* en las empresas ha ocurrido sin contar con un plan detallado, inicialmente bajo la presión de dotar a la plana ejecutiva de acceso al correo electrónico en dichos dispositivos. La aplicación de correo electrónico móvil genera la masiva adopción de *smartphones* en las empresas, desde grandes corporaciones hasta pequeñas empresas. Adicionalmente afirma que es indispensable administrar la operación para asegurar la disponibilidad, calidad y seguridad de los nuevos servicios que aportan la tecnología móvil, con lo cual se hace necesario adoptar sistemas de administración de los dispositivos móviles (*MDM - Mobile Device Management*).

En este mismo sentido, Carlos Teixidó[11] afirma **"**esta área en la que muchas compañías aún no atienden adecuadamente y cuya complejidad ha aumentado debido a la adopción de múltiples tecnologías (*BlackBerry, iOS, Android* y *Windows Phone*) y la aceptación del uso de dispositivos de los empleados

[10] TEIXIDÓ Carlos. Gestión de la movilidad empresarial. Consultado el 26 de julio 2015. Disponible en: http://www.emb.cl/gerencia/articulo.mvc?xid=3357

(*BYOD*) para acceder al correo electrónico corporativo y otros sistemas".

Según estudio de la Movilidad en las Empresas realizado por Nubison[11]. en Chile, un 60% de las compañías está dispuesto a aceptar parcial o totalmente el *BYOD*, sin embargo un 70% de las empresas reconoce que su nivel de preparación para administrar el contexto *BYOD* es regular o inferior.

2.2.2 La seguridad en la movilidad empresarial. La movilidad debe ofrecer seguridad para evitar la fuga indeseada de información y mantener por ende un alto nivel de competitividad. Este es posiblemente el mayor reto actual, pues se trata de conservar la mejor experiencia de usuario que sea posible, y de garantizar al mismo tiempo la seguridad de los datos, sin que haya lugar a restricciones de acceso a la información necesaria para trabajar. Esto exige para las empresas un desarrollo de políticas de protección de datos y de regulación que no rompan el equilibrio entre seguridad y libertad, según lo afirma el artículo titulado Cómo será la movilidad empresarial en el 2015: 3 tendencias[12].

Según lo expresa Hugo Werner, director general de Citrix México los riesgos de la movilidad al tener una política de movilidad deficiente, afecta la información interna de las empresas y la pérdida y rotación de talentos[13], son los siguientes:

1. Seguridad. Antes los ataques se limitaban en los *websites* o las bases de

[11] TEIXIDÓ Carlos. Gestión de la movilidad empresarial. Consultado el 26 de julio 2015. Disponible en: http://www.emb.cl/gerencia/articulo.mvc?xid=3357

[12] GUTIÉRREZ Tatiana. 5 prácticas para controlar la movilidad en tu empresa. Consultado el 26 de julio 2015. Disponible en: http://www.altonivel.com.mx/44006-5-practicas-para-controlar-la-movilidad-en-tu-empresa.html.

[13] GUTIÉRREZ Tatiana. 5 prácticas para controlar la movilidad en tu empresa. Consultado el 26 de julio 2015. Disponible en: http://www.altonivel.com.mx/44006-5-practicas-para-controlar-la-movilidad-en-tu-empresa.html.

datos. Un ataque tecnológico lo hacía un *hacker*, hoy, lo puedes hacer desde un dispositivo móvil y desde el interior de una empresa. Por lo que se recomienda voltear a ver las políticas de movilidad definidas en la empresa y asegurarse quien tiene acceso y a qué tipo de información.

2. Pérdida de talentos. Las nuevas generaciones buscan personalizar sus espacios, tanto personales como laborales, y la movilidad se los permite en un solo paso. Una gran parte de los talentos en las empresas ponen en tela de juicio su entrada o estancia según las políticas de movilidad que las empresas les brindan.

3. Eficiencia. La movilidad es una gran ventaja competitiva para las organizaciones, la movilidad ha permitido que los espacios de oficia sean virtuales. La flexibilidades una de las grandes ventajas, los colaboradores pueden trabajar de donde sea y cuando sea.

Según lo expresa Tatiana Gutiérrez, “las políticas de seguridad pueden perder valor con el tiempo si los usuarios no creen que violarlas tiene consecuencias, o peor aún, si creen que pasar por encima de ellas mejora su productividad. Las políticas deben mantenerse y estar alineadas con el negocio de la compañía en todo momento.” [14]

2.2.3 Funcionamiento del correo electrónico. El correo electrónico es un servicio de red que permite a los usuarios enviar y recibir mensajes. Mediante estos mensajes de correo electrónico se puede enviar, texto y todo tipo de documentos digitales.

2.2.3.1 Cómo funciona el correo electrónico?. Para identificar el funcionamiento del servicio de correo electrónico se hace necesario identificar los siguientes actores:

- Usuario Remitente
- Usuario Destinatario
- Cuenta o dirección de correo electrónico
- Cliente de correo Electrónico – *MUA(*del inglés *Mail User Agent)* o interfaz *web*

Una dirección de correo electrónico es un conjunto de palabras que identifican un usuario, el cual puede enviar y recibir correo. Cada dirección es única.

Un ejemplo de dirección de correo electrónico es : ocamacho@gmail.com.

Los clientes de correo electrónico son programas para gestionar los mensajes recibidos y poder escribir nuevos.

El proveedor del servicio de correo electrónico debe manifestar detalladamente cómo se debe configurar el programa de correo. Entre los datos necesarios están: tipo de conexión (*POP* o *IMAP*), dirección del servidor de correo, nombre de usuario y contraseña.

Tal como lo establece el artículo denominado “Cómo funciona el correo electrónico (MTA, MDA, MUA) ”14 el cual manifiesta que “Cuando se envía un correo electrónico, el mensaje se enruta de servidor a servidor hasta llegar al servidor de correo electrónico del receptor”.

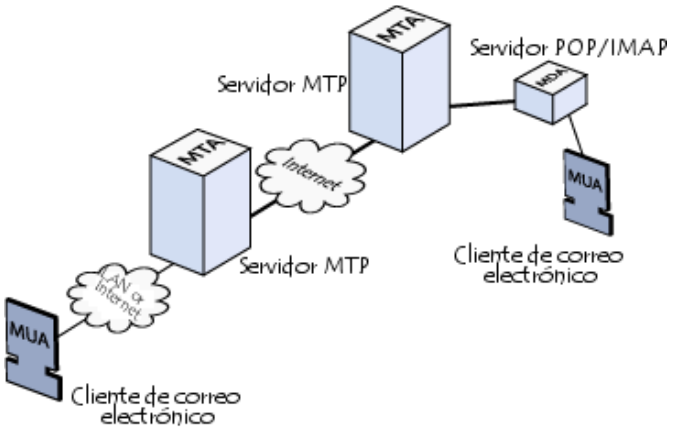
En el mismo artículo habla de la existencia de dos protocolos encargados de gestionar el correo electrónico a saber:

- POP3 (*Post Office Protocol* [Protocolo de Oficina de Correo]), se utiliza para recuperar el correo electrónico.

[14] CCM BENCHMARK. Cómo funciona el correo electrónico (MTA, MDA, MUA). Consultado el 26 de julio 2015.Disponible en: http://es.ccm.net/contents/115-como-funciona-el-correo-electronico-mta-mda-mua

- IMAP (*Internet Message Access Protocol*) Se usa para coordinar el estado de los correos electrónicos (leído, eliminado, movido) a través de múltiples clientes de correo electrónico. En la figura No 1 se muestra la arquitectura de un sistema de correo electrónico.

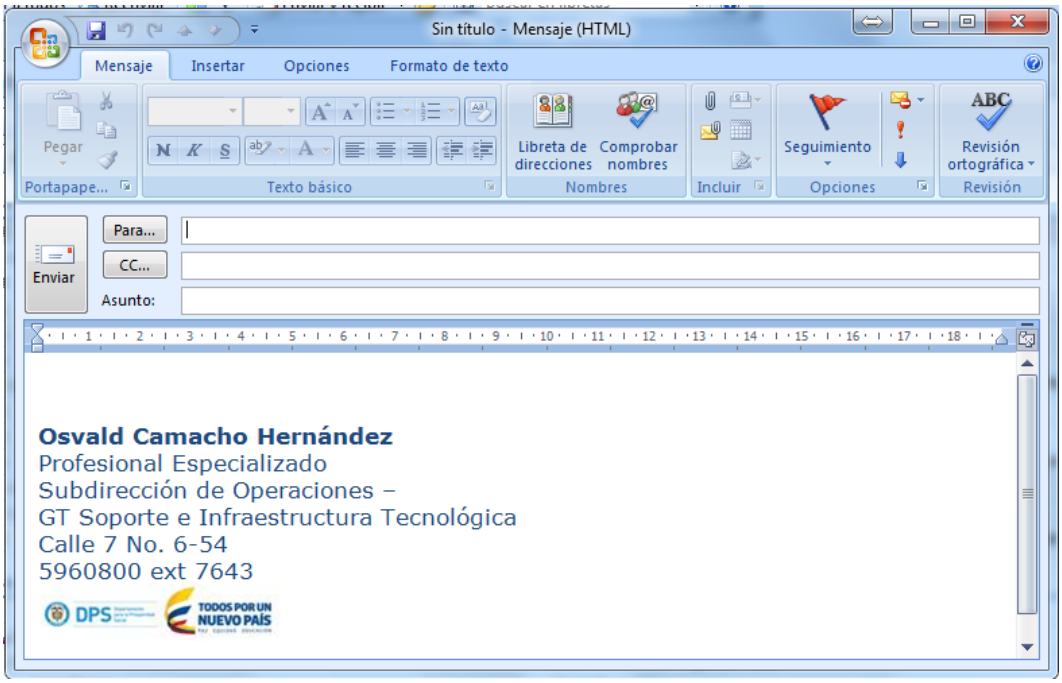
Figura No 1. Servicio de correo electrónico



Fuente: http://es.ccm.net/contents/115-como-funciona-el-correo-electronico-mta-mda-mua

2.2.3.2 Creación y envío de mensajes de correo electrónico. En la figura No 2, se describe cómo diligenciar el formulario de un mensaje de correo electrónico, estos pueden variar dependiendo del programa de correo electrónico:

Figura No 2. Formulario de Mensaje de correo electrónico



1. Cuadro **Para**, se escribe la dirección de correo electrónico del o los destinatarios.

2. Cuadro **CC**, escriba las direcciones de correo electrónico de cualquier destinatario secundario o persona que deba ser notificada del correo electrónico.

3. Cuadro **Asunto**, escriba una breve descripción para el mensaje.

4. En el área en blanco grande, escriba el mensaje.

Para adjuntar un archivo al mensaje, haga clic en el botón **Adjuntar archivo al mensaje** de la barra de herramientas.

2.3 MARCO CONTEXTUAL

El Departamento para la Prosperidad Social (DPS) es la Entidad del gobierno de Colombia que encabeza el sector de inclusión social y reconciliación, al cual se

encuentran adscritos el Instituto Colombiano de Bienestar Familiar, la Agencia Nacional para la Superación de la Pobreza Extrema-ANSPE, la Unidad de Atención y Reparación Integral a las Víctimas, la Unidad Administrativa Especial para la Consolidación Territorial y el Centro de Memoria Histórica.

El DPS se propone como misión "Formular y dirigir políticas para el Sector de Inclusión Social y Reconciliación e implementar acciones para la estabilización socioeconómica de la población vulnerable"[15] y como visión pretende a 2018 ser "el eje dinamizador de la movilidad social del sistema de protección social y el principal promotor de los procesos de reconciliación de la población colombiana "[16]

Entre los objetivos del DPS[17] se mencionan:

1. Dirigir las acciones sectoriales que contribuyan a la creación de condiciones para la reconciliación.
2. Generar condiciones en la población y territorios que permitan la reconciliación y la no repetición.
3. Contribuir a la superación de la pobreza con una oferta efectiva.
4. Lograr la atención a las poblaciones y territorios de manera eficiente.
5. Mejorar la gestión del DPS.

El Departamento para la Prosperidad Social DPS es el organismo del Gobierno Nacional que busca fijar políticas, planes generales, programas y proyectos para

[15] DEPARTAMENTO ADMINISTRATIVO PARA LA PROSPERIDAD SOCIAL – DPS Misión Consultado el 26 de julio 2015 disponible en internet: http://www.dps.gov.co/ent/gen/SitePages/Misi%C3%B3n%20y%20visi%C3%B3n.aspx

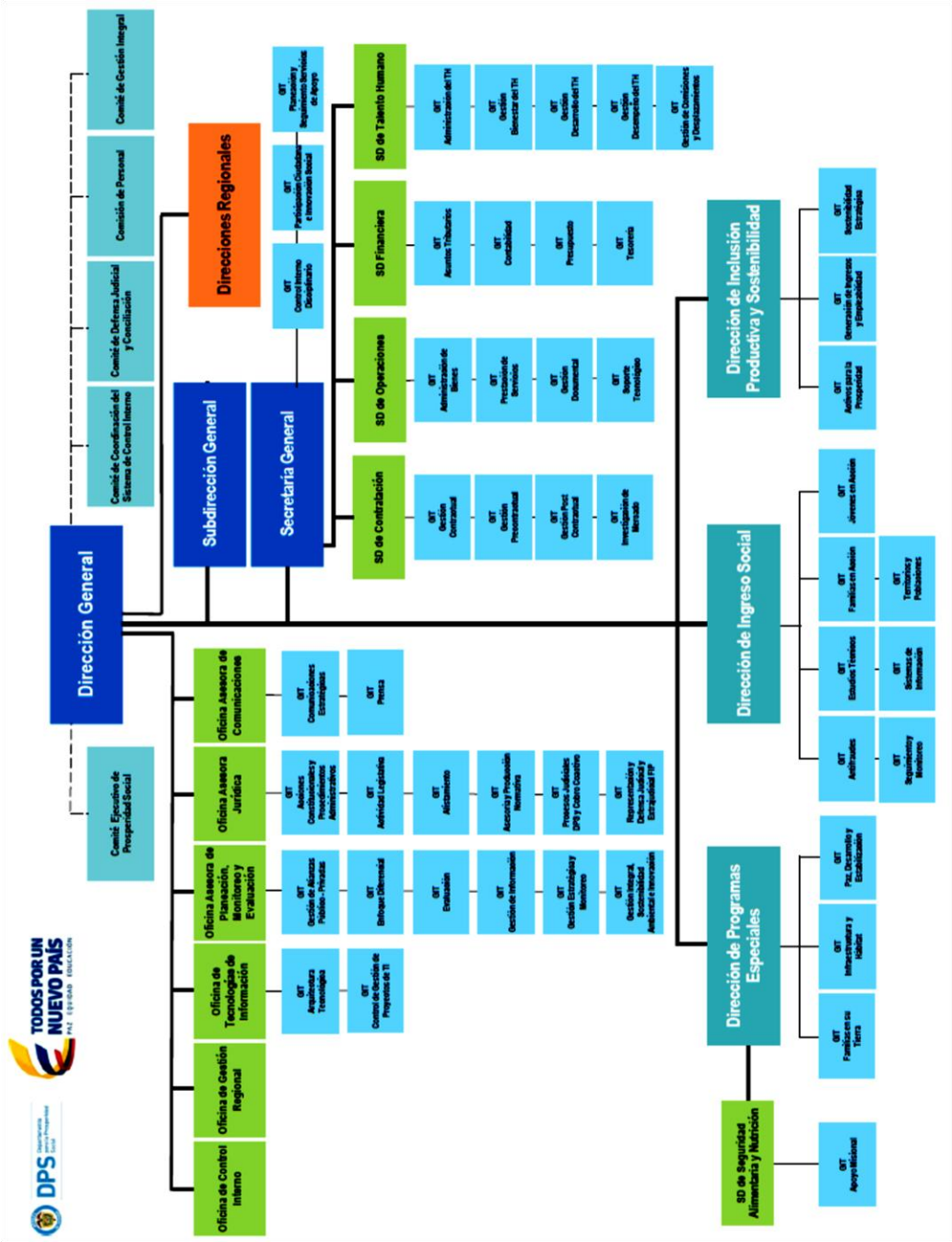
[16] DEPARTAMENTO ADMINISTRATIVO PARA LA PROSPERIDAD SOCIAL – DPS Visión Consultado el 26 de julio 2015 disponible en internet: http://www.dps.gov.co/ent/gen/SitePages/Misi%C3%B3n%20y%20visi%C3%B3n.aspx

[17] DEPARTAMENTO ADMINISTRATIVO PARA LA PROSPERIDAD SOCIAL – DPS Funciones Consultado el 26 de julio 2015 disponible en internet: http://www.dps.gov.co/ent/gen/SitePages/Misi%C3%B3n%20y%20visi%C3%B3n.aspx

la asistencia, atención y reparación a las víctimas de la violencia, la inclusión social, la atención a grupos vulnerables y su reintegración social y económica.

Para alcanzar este propósito, el Departamento trabaja integralmente en la formulación y ejecución de políticas sociales, además de realizar la coordinación de la Unidad de Atención y Reparación Integral a las Víctimas, el Instituto Colombiano de Bienestar Familiar, la Agencia Nacional para la Superación de la Pobreza Extrema, el Centro de Memoria Histórica y la Unidad Administrativa Especial para la Consolidación Territorial. El DPS está estructurado como se muestra en la figura 3.

Figura No 3. Organigrama del DPS



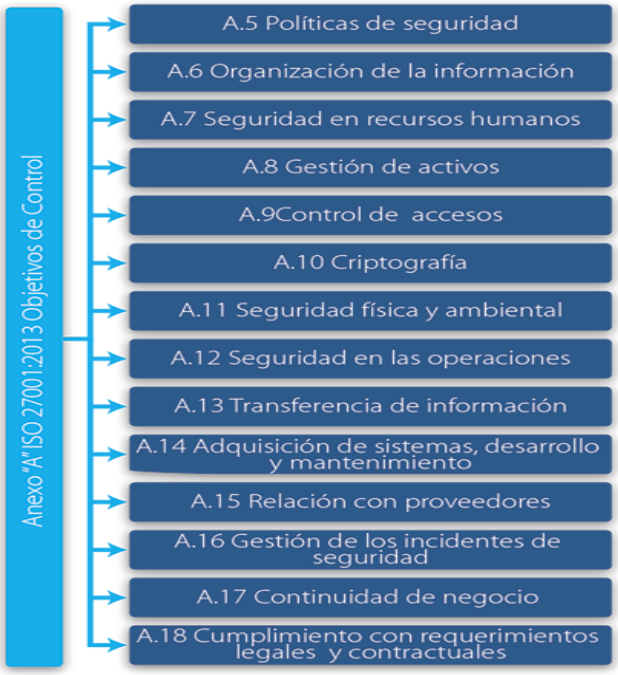
Fuente: http://www.dps.gov.co/ent/gen/SitePages/Organigrama.aspx

Como ya se describió en la formulación del problema, el DPS está adelantando dentro del proceso de modernización del estado la implementación de un SGSI, para controlar y gestionar los sistemas y las herramientas tecnologías de la Entidad. Por lo tanto, no podría quedarse marginado sin la utilización de dispositivos móviles por parte de los usuarios y funcionarios en el cumplimiento de sus funciones, para lo cual demanda la construcción de políticas y utilización de herramientas que permitan gestionar la utilización de dispositivos móviles al interior de la entidad, que como sucede en la mayoría de la empresas dichos dispositivos son de propiedad del funcionario, con lo cual la información queda expuesta a riesgos de seguridad de la información.

2.4 MARCO LEGAL

Esta propuesta se enmarca dentro del tema de controles de seguridad de la información del Anexo A de la norma NTC-ISO/IEC 27001:2013. En la figura 4 se observa la estructura general del anexo A y sus correspondientes dominios.

Figura No 4. Dominios Anexo “A” de ISO 27001:2013

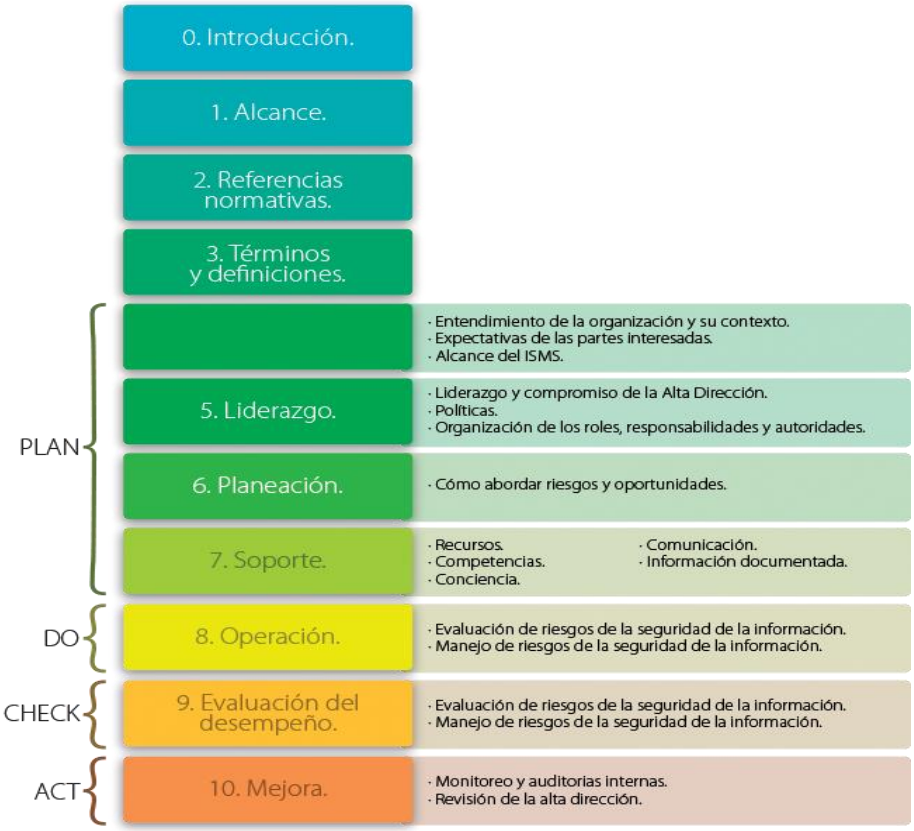


Fuente: http://www.isaca.org/chapters7/Madrid/Events/Documents/Principales%20Novedades%20de%20la%20ISO27001ISO%2027002%20-%20Paloma%20Garcia.pdf

La estructura de la norma ISO 27001:2013 lo establece el autor del artículo llamado “ISO-27001:2013 ¿Qué hay de nuevo?” cuando afirma que las principales modificaciones se ven reflejadas en la estructura y el contenido de los controles que conforman el Anexo “A”, donde el número total de dominios era de 11 y ahora son 14 y se reduce el número de controles de 133 a 113, todo como resultado de un proceso de fusión, exclusión e incorporación de nuevos controles de seguridad[18] como se muestra en la figura 5.

[18] MAGAZCITUM. ISO-27001:2013 ¿Qué hay de nuevo? Consultado el 26 de julio 2015. Disponible en: http://www.magazcitum.com.mx/?p=2397#.VbgYfMB_Oko

Figura No 5. Estructura del estándar ISO/IEC 27001:2013



Fuente: http://www.magazcitum.com.mx/?p=2397#.VbgYfMB_Oko

Adicionalmente se requiere considerar el siguiente acervo legal, que enmarca el contenido temático de este proyecto, a continuación las normas:

- Ley 1341 de 2009 define un marco legal propicio para el desarrollo de los contenidos digitales.

- Plan Vive Digital Colombia busca proyectar al país como hub regional y mundial de contenidos digitales y fomentar el desarrollo de contenidos digitales, aplicaciones móviles y web a través de clúster que potencien la industria nacional.

- LEY 527 DE 1999 por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

- LEY 1273 DE 2009 por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

3. METODOLOGIA

La investigación se desarrolla teniendo en cuenta un enfoque cuantitativo, de tal manera que se estudian variables cuantificables y que pueden ser medidas con indicadores objetivos.

3.1 TIPO DE INVESTIGACIÓN

La presente investigación es descriptiva ya que se aborda la seguridad informática y los principales riesgos de seguridad informática asociados con la movilidad del servicio de correo electrónico corporativo en el DPS; también es una investigación aplicada, orientada hacia la gestión de los controles definidos en el anexo A de la norma ISO 27001:2013, de tal manera que fundamentados en el análisis de riesgos se diseñará una política que permita gestionar y controlar el servicio de correo corporativo de la Entidad en los dispositivos móviles de propiedad de los empleados del DPS.

3.2 DISEÑO DE INVESTIGACIÓN

El Diseño de la investigación se refiere a la manera práctica y que de forma precisa el investigador desarrolla para cumplir con los objetivos del estudio propuesto, el diseño de investigación indica los pasos a seguir para alcanzar dichos objetivos.

El diseño empleado en esta investigación es experimental de tipo transeccional, los resultados se fundamentan en la observación y análisis descriptivo de los hallazgos encontrados. En la figura 6 se muestran los momentos de desarrollo de este proyecto.

Figura No 6.Pasos de la metodología

3.3 POBLACIÓN Y MUESTRA

Como población se toman todos los funcionarios del Departamento Administrativo para la Prosperidad Social - DPS que hacen uso del servicio de correo desde sus dispositivos móviles, se toma una muestra intencionada (no probabilística) conformada por personas que por su cargo o por alguna otra razón son más indicadas como fuente de información y que de una u otra manera interactúan a diario con aplicaciones y servicios.

3.4 FUENTES DE INFORMACIÓN

Las fuentes de información que se tienen en cuenta para la realización del proyecto se pueden catalogar en información primaria y secundaria.

- Fuentes de información primaria: Las fuentes primarias están constituidas por la información suministrada por los profesionales que desempeñan roles de administradores de aplicaciones, de servicios y servidores,

adicionalmente se cuenta con la información suministrada por el oficial de seguridad de la información de la Entidad.

- Fuentes de información secundaria: La información secundaria es toda la información documental que orienta al análisis y evaluación de la seguridad informática y que se encuentra consignada en documentos como: normas: NTC- ISO-IEC-27001:2013, y documentos de la Entidad relacionados con el sistema de seguridad de la información del DPS.

3.5 TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

- Entrevista: para obtener información relevante para el proyecto se utilizó la entrevista de modelo conversacional, por ser una técnica eficaz para obtener datos relevantes y significativos, utilizando una entrevista no estructurada con el fin de obtener una opinión personalizada de los Profesionales especializados quienes son los encargados de la administración de las aplicaciones, servicios, servidores y el oficial de seguridad de la información.

- Encuestas: para identificar vulnerabilidades, conductas, controles de seguridad de la información y conocimiento que tenían los usuarios de las políticas de seguridad de la información, se aplicó una encuesta que fue contestada por 51 personas.

- Observación: por otra parte en la realización del proyecto se utilizó la observación para registrar patrones de conducta de los usuarios y de la interacción del usuario con el servicio de correo corporativo.

- Revisión documental: para ello se revisó los documentos existentes que brindan soporte a la seguridad informática y el control de los mismos como

son: normas NTC-ISO-IEC- 27001:2013 documentación del DPS que soportan el sistema de gestión de la seguridad de la información, la política de seguridad de información relacionada con el servicio de correo corporativo y el mapa de riesgos asociados al correo electrónico en el Departamento para la Prosperidad Social - DPS.

4. RESULTADOS

4.1 REQUISITOS PARA EL USO DEL SERVICIO DE CORREO ELECTRÓNICO CORPORATIVO EN DISPOSITIVOS MOVILES

Con la finalidad de conocer las amenazas y vulnerabilidades del sistema, y obtener requisitos del sistema propuesto se aplicó una encuesta a un grupo de usuarios representativos de algunas áreas y programas del Departamento para la Prosperidad Social DPS que corresponde al 20% de los usuarios de la Entidad, y que gentilmente contribuyeron al diligenciamiento del cuestionario. El cuestionario se puede consultar en el anexo 1 y los resultados detallados en el anexo 2.

Realizando una análisis de la información suministrada por los usuarios a través de la encuesta y de las entrevistas realizadas al oficial de seguridad de la información y al administrador del servicio de correo electrónico, se evidencia la existencia de vulnerabilidades que podrían ser explotadas y poner en peligro la información que es gestionada a través del servicio de correo electrónico corporativo en los dispositivos móviles.

Teniendo en cuenta que el Departamento para la Prosperidad Social – DPS tiene implementado un sistema de seguridad de la información SGSI y que dentro de este existe un documento relacionado con el análisis de riesgos y particularmente existen dicha matriz como se evidencia en el anexo 4 de este documento, se propone realizar una modificación a dicho documento, en el sentido de incluir las vulnerabilidades evidenciadas con el servicio de correo electrónico corporativo en los dispositivos móviles, teniendo en cuenta la información detallada continuación:

Entre las vulnerabilidades y amenazas identificadas se tienen:

1. Debilidad en sistema de Autenticación

   Esta vulnerabilidad está asociada con la verificación de la identidad del usuario, generalmente cuando entra en el sistema o la red, o accede a una base de datos.

   La autenticación utilizando contraseñas resulta ser el mejor o peor de los métodos, dependiendo de las características de la contraseña. En la medida que la contraseña sea más grande y compleja para ser adivinada, más difícil será burlar esta técnica.

2. Ausencia de control de datos y servicio de correo corporativo

   Esta vulnerabilidad está asociada con la ausencia de control de dispositivos, esto es el registro de cada uno de ellos desde su configuración e información básica relacionada con la información requerida para efectuar el registro del dispositivo móvil, en el cual se accederá al servicio de correo electrónico corporativo.

3. Violación o incumplimiento de las políticas de seguridad en dispositivos móviles

   Esta amenaza está conformada por las acciones que realizan los usuarios de los dispositivos móviles, quienes ignoran controles de políticas asociadas con los dispositivos móviles en los cuales será utilizado el servicio de correo electrónico de la Entidad y con lo cual se pone en riesgo la información que contiene cada uno de los correos electrónicos.

4. Carencia del Inventario de dispositivos móviles

   Hoy por hoy la utilización de los dispositivos móviles para acceder al servicio de correo electrónico corporativo no existe un inventario bien

definido y estructurado, que garantice la identificación de cada dispositivo móvil y que se emplea para utilizar el servicio de correo electrónico en la Entidad.

5. Soporte inadecuado a usuarios

   Estás relacionado con la ausencia de formación de los usuarios en relación con el uso de dispositivos móviles para acceder al correo electrónico corporativo. En este aspecto es fundamental que el usuario tome conciencia de la importancia de utilizar los dispositivos móviles para acceder al servicio de correo electrónico de la Entidad, unido a la conciencia de la responsabilidad que representa hacer un uso adecuado del servicio acatando las políticas para la prestación del servicio.

6. Pérdida o robo de dispositivos

   Está relacionada con la amenaza inminente de que un dispositivo móvil con el cual se acede al servicio de correo electrónico se robado o se extravié, este aspecto representa una vulnerabilidad de la información contenida en los mensajes del dispositivo extraviado.

7. Fuga de datos o la divulgación inadvertida de la información confidencial

   Es la ausencia de políticas de intercambio y envío de correo para proteger la información, la Entidad debe asegurar que los datos corporativos sensibles se mantengan detrás de un *Firewall,* de esta manera se evita que los dispositivos no administrados no tengan acceso al servidor de correo electrónico corporativo.

8. Inadecuada estrategia de protección contra las amenazas o ataques

   Estás asociada con controles de seguridad de la información para garantizar el acceso al servicio de correo electrónico en dispositivos móviles contra los ataques externos, las aplicaciones fraudulentas, la navegación no

segura, el robo de información, robo de identidad entre otras formas de ataque de seguridad de la información.

A continuación en el cuadro 15, se presentan para algunas vulnerabilidades o amenazas, el control y el objetivo para cada una de ellas.

Cuadro No 15 Vulnerabilidades

Ítem	Vulnerabilidad/Amenaza	Objetivo de Control	Control
1	Debilidad en sistema de Autentificación	Proteger control el acceso no autorizado	Implantar Política de Password
2	Ausencia de control de datos y servicio de correo corporativo	Prevenir fuga de datos sensibles	Configuración adecuada del correo electrónico en el dispositivo
			Instalación de aplicaciones remotas
3	Violación o incumplimiento de las políticas de seguridad en Dispositivos móviles	Prevenir violaciones a las políticas de seguridad	Monitoreo, control y verificación del cumplimiento de las Políticas de seguridad
4	Ausencia del Inventario de Dispositivos móviles	Registrar las Características básicas de los dispositivos	Mantener un Inventario actualizado
5	Soporte inadecuado a Usuarios	Apoyar el uso del correo electrónico corporativo en dispositivos móviles	Capacitar y generar conciencia del buen uso del servicio
			Garantizar disponibilidad mediante ANS

Teniendo en cuenta las vulnerabilidades y amenazas de igual manera que la información obtenida mediante las encuestas y entrevistas se considera que la utilización del correo electrónico corporativo en dispositivos móviles debe atender los siguientes requisitos:

1. El sistema de gestión del correo electrónico debe garantizar que se mantiene la política de contraseñas seguras. Esta investigación ha mostrado que la mayoría de usuarios utilizan contraseñas en las que incluyen caracteres de todo tipo (52%) o combinaciones de números y letras (37%) y la mayoría de usuarios utilizan más de siete caracteres. Esta información ha sido confirmada por el administrador del directorio activo quien manifestó que el sistema no admite contraseñas blandas.

   Lo anteriormente expuesto evidencia que se requiere adoptar controles similares en el registro de usuarios que utilizarían el servicio de correo corporativo en los dispositivos móviles del DPS.

2. El análisis planteado en el anexo 2 da cuenta que existen problemas de discontinuidad del servicio, pérdida de conexión, virus y otras cosas que exigen controles de seguridad, relacionados con el uso del servicio de correo en los dispositivos móviles de la Entidad, en los cuales se deben mitigar los riesgos que se viene presentando con la indisponibilidad de los servicios y aplicaciones, presencia de virus, perdida de información.

3. También en el análisis planteado en el anexo 2 se determina que la mayoría de los usuarios no utilizan el servicio de correo electrónico corporativo en los dispositivos móviles mientras que un 7,8% siempre está utilizando éste servicio, también se afirma que no deben registrar alguna forma de control al utilizar el servicio de correo electrónico en dispositivos móviles

Este planteamiento evidencia que se debe implementar una herramienta que permita gestionar el uso del servicio de correo electrónico corporativo en dispositivos móviles de la Entidad.

4. También se evidencia la necesidad de establecer un mecanismo de capacitación de los usuarios en uso del servicio de correo electrónico corporativo en dispositivos móviles, que permita concientizar a los usuarios de las responsabilidades y vulnerabilidades a las que se expone el uso de dicho servicio en los dispositivos móviles.

5. De forma similar se establece otro requerimiento, el cual se establece mediante las entrevistas al oficial de seguridad de información y del administrador del servicio de correo electrónico corporativo es la necesidad de establecer políticas que determinen controles para la utilización de dispositivos móviles que utilizarían el servicio de correo electrónico en el DPS.

4.2 POLITICAS PROPUESTAS

A continuación se proponen las siguientes políticas relacionadas con la gestión de los dispositivos móviles en el Departamento para la Prosperidad Social – DPS.

4.2.1 Política de dispositivos móviles.

Objetivo: Proteger la información del DPS que se encuentra almacenada en dispositivos móviles y gestionar sus riesgos asociados

1. El uso de los equipos portátiles de propiedad del DPS fuera de las instalaciones, únicamente se permitirá a usuarios autorizados mediante una

orden de salida, la cual debe tener el visto bueno del delegado de los procesos con firma autorizada para este fin.

2. Los equipos que estén autorizados para salir y que contengan información sensible, se deben proteger mediante el uso de uno o varios de los siguientes controles tecnológicos:

   - Antivirus.
   - Encriptación de datos.
   - Restricción en la ejecución de aplicaciones.
   - Restricción de conexión de dispositivos USB.
   - Protección física mediante la guaya de seguridad.
   - Desactivar accesos inalámbricos cuando se encuentren conectadas a la red LAN

3. Cualquier dispositivo móvil que albergue información del DPS debe poseer un sistema de autenticación, basado al menos en un patrón de movimiento, un código de desbloqueo o una contraseña.

4. Cualquier dispositivo móvil que albergue información del DPS debe tener instalado un software de antivirus.

5. Los dispositivos móviles que son propiedad del DPS pueden estar sometidos a un control sobre el tipo y la versión de aplicaciones instaladas, al igual que pueden estar sometidos a restricciones de conexión hacia ciertos servicios de información que sean considerados maliciosos.

6. Los dispositivos móviles que son propiedad de los funcionarios, pueden tener almacenada información del DPS, como el correo electrónico, siempre y cuando dichos equipos se encuentren registrados e identificados y se

implementen las medidas de aseguramiento definidas por el Grupo de Trabajo (GT) de Infraestructura y Soporte de TI para garantizar la preservación de la confidencialidad e integridad de la información del DPS.

7. En caso de pérdida o robo de un dispositivo móvil que contenga información del DPS, el funcionario a cargo del dispositivo móvil, debe avisar inmediatamente al Grupo de Trabajo (GT) de Infraestructura y Soporte de TI, quien está en libertad para iniciar un proceso de borrado remoto de información.

4.2.2 Política de uso de recursos tecnológicos

Objetivo: Definir las pautas generales para asegurar una adecuada protección de la información del DPS a través de la definición de las condiciones de uso aceptable de los recursos tecnológicos.

El DPS asignará diferentes recursos tecnológicos como herramientas de trabajo para uso exclusivo de sus colaboradores autorizados. El uso adecuado de estos recursos se reglamenta bajo las siguientes directrices:

1. La instalación de cualquier tipo de software en los equipos de cómputo del DPS debe ser realizada por el Grupo de Trabajo de Infraestructura y Soporte de TI y por tanto son los únicos autorizados para realizar esta labor.

2. Los usuarios no deberán realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo. Estos cambios podrán ser realizados únicamente por el Grupo de Trabajo de Infraestructura y Soporte de TI.

3. El Grupo de Trabajo de Infraestructura y Soporte de TI definirá la lista actualizada de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones de trabajo de los usuarios; así mismo, realizará el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.

4. Sólo personal autorizado podrá realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información del DPS; las conexiones establecidas para este fin, utilizarán los esquemas de seguridad definidos.

5. Los colaboradores de la Entidad son responsables de hacer buen uso de los recursos tecnológicos del DPS y en ningún momento podrán ser usados para beneficio propio o para realizar prácticas ilícitas o mal intencionadas que atenten contra otros Colaboradores, terceros, la legislación vigente y las políticas y lineamientos de seguridad de la información del DPS.

6. La información de carácter personal almacenada en dispositivos de cómputo o móviles, medios de almacenamiento o cuentas de correo institucionales debe de ser almacenada en su totalidad en una carpeta especificada para tal fin, la cual debe ser nombrada como “PERSONAL”.

7. Devolución de los Activos: Todo activo de propiedad del DPS, asignado a un Colaborador de la Entidad o a una tercera parte, deberá ser entregado a la finalización del contrato o por cambio de cargo. Esto incluye los documentos corporativos, equipos de cómputo (Hardware y Software), dispositivos móviles, tarjetas de acceso, manuales, tarjetas de identificación y la información que tenga almacenada en dispositivos móviles o removibles.

4.3. PROPUESTA DE IMPLEMENTACIÓN DE LA SOLUCIÓN - *EMM* DE *MCAFEE*

La plataforma *EMM de McAfee* integra dispositivos como son los *smartphones*, *PDAs* y *Tablet* PC, mediante la utilización de directivas de control de acceso a la red de la Entidad.

A continuación se establecen los aspectos representativos que cumple la aplicación *EMM* de *McAfee* para gestionar la movilidad empresarial en el Departamento para la Prosperidad Social – DPS.

- Acceso de usuarios y aplicaciones

  Hace referencia a que el acceso de los usuarios de los dispositivos móviles en los que se accederá el servicio de correo electrónico corporativo debe ser registrado con nombres de usuarios y contraseñas debidamente autorizados para interactuar con el servicio de correo electrónico.

- Protección de aplicaciones y datos

  Se refiere a que la información al ser el activo más importante de la Entidad, debe ser protegida en todo momento. Se deben establecer mecanismos de control y métodos de protección de seguridad de la información para que los datos en todo momento al interactuar con las aplicaciones específicamente con el servicio de correo electrónico corporativo estén protegidos.

- Administración de dispositivos

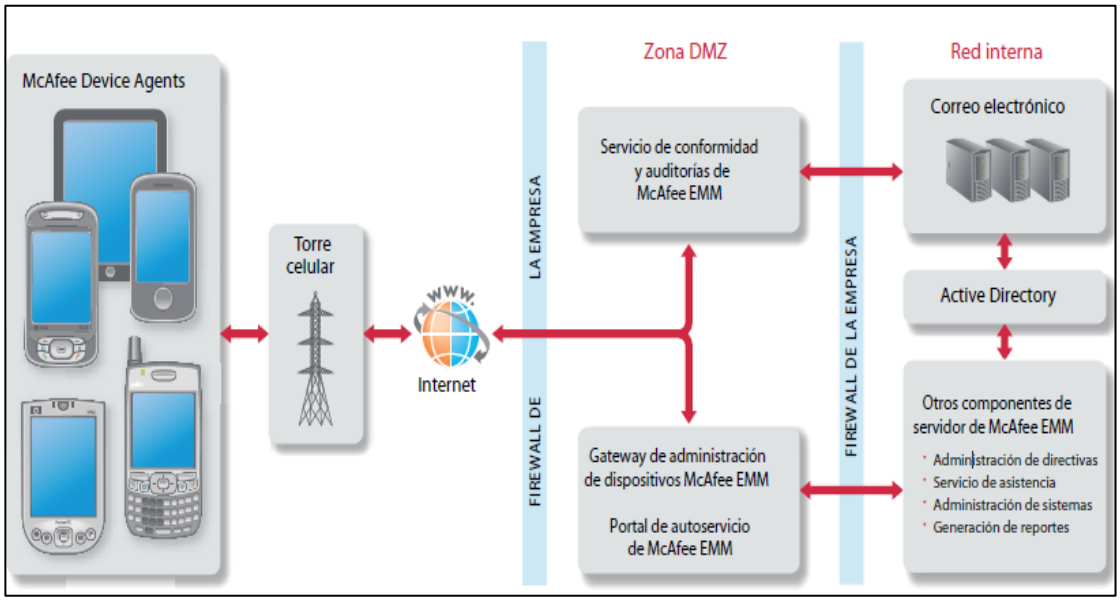
  Todos los dispositivos móviles con los que se acceden a los servicios corporativos deben administrarse y protegerse según las políticas adecuadas para dispositivos móviles.

- Protección contra amenazas

  Se refiere a que cada día la utilización de dispositivos móviles es empleada por más personas incluidas los delincuentes que están al asecho. Cada plataforma tiene diferentes perfiles de riesgo, y es importante identificar vulnerabilidades existentes y tomar las medidas adecuadas para minimizar los riesgos y proteger la información

En la figura No 7 se observa la estructura general de la aplicación EMM de *McAfee*.

Figura No 7. Arquitectura de *McAfee EMM*



Fuente: http://calderoncardona.com/wp-content/uploads/2011/05/McAfee__Secure.pdf

4.3.1 Funcionalidades de la aplicación

- Control de acceso por usuario, datos y dispositivos
- Cumplimiento de los requisitos de conectividad a la red, VPN y WiFi incluidos
- Aplicación de procesos de autenticación y cifrado
- Bloqueo o borrado completo en remoto de dispositivos perdidos o robados
- Software independiente antimalware para proteger dispositivos de códigos malintencionados
- Almacenar datos de forma cifrada y restringir la función de cortar y pegar datos en zonas no seguras

4.3.2 Aspectos de la administración de dispositivos móviles. Los siguientes requerimientos o funcionalidades de la aplicación permiten realizar una administración de dispositivos de manera más fácil.

- Incluir distinciones por usuario, grupo, dispositivo y sistema operativo.
- Paneles, vistas e informes móviles personalizables o estandarizados
- Procesos automatizados y simplificados, incluida una regla de marcado para administrar el inventario y diseñar directivas específicas
- Analizar, alertar, supervisar y generar informes
- Identificar y bloquear dispositivos peligrosos
- Alojar y distribuir aplicaciones empresariales

4.3.3 Requisitos de la solución *EMM* de *McAfee.* Del lado del servidor los siguientes son los requisitos:

Cuadro 17. Requerimientos del lado del servidor

No	Componente	Requisito
1	Software de aplicación	*Epolicy Orchestrator* 4.6.7 - 5.1
2	Hardware	Memoria: 8GB o superior
		Disco: Mínimo 200GB
		Procesador Dual Core o superior
3	Sistema Operativo	*Windows server* 2008 de 64 bits con *service pack* 2
4	Bases de datos	*SQL Server* 2008 64 bits con el último service pack (Enterprie edition)
5	Correo	*exchange* 2007,2010 o 2013
		Dominio 8.5.3 o 9.0
6	Exploradores	Internet explorer, Firefox o Chrome
7	CA *SERVER*	*windows server* 2008 R2 de 64 bits con *service pack* 1

Del lado del cliente basta con tener un dispositivo móvil inteligente, la solución es compatible con diferentes plataformas de sistemas operativos móviles, entre las que se encuentran, *Apple iOS* (desde versión 3.x en adelante), *Androide,* Palm *webOS*, así como Windows *Mobile* .

4.4 DIFUSIÓN Y SENSIBILIZACIÓN DE POLITICAS PARA USO DEL SERVICIO DE CORREO ELECTRONICO CORPORATIVO EN DISPOSITIVOS MOVILES

El objetivo principal de esta actividad de sensibilización está orientado a dar a conocer las amenazas, vulnerabilidades y políticas relacionadas con el uso del correo electrónico en dispositivos móviles del DPS. Unido a la responsabilidad que adquiere el funcionario en ejercicio de sus funciones al utilizar el servicio y exponer la información de la Entidad en los dispositivos móviles.

Esta estrategia de sensibilización es parte indispensable dentro de cualquier organización puesto que involucra a todos los actores en una relación de cumplimiento de normas a la hora de utilizar un servicio. Esta contribuye a minimizar los riesgos a los que se puede exponer la información de la Entidad.

Una vez creadas las políticas relacionadas con los dispositivos móviles y la utilización del correo corporativo en ellos, es importante establecer una estrategia de difusión y sensibilización sobre las mismas. Este plan debe ser abordado como parte del proceso de capacitación de usuarios del Sistema de Seguridad de Información - SGSI del DPS. Adicionalmente el oficial de seguridad de la información de la Entidad debe velar por las actividades derivadas de este proyecto.

Se deben emplear recursos como salas y servicios de diseño del grupo de comunicaciones de la Entidad, con la finalidad de dar cumplimiento a las actividades propuestas en este plan, como se muestra en el cuadro 16.

Es importante resaltar que este plan debe ser aplicado una vez la Entidad tome la decisión de realizar su implementación como parte del sistema de seguridad de la información en un ambiente de producción.

Se diseñarán e imprimirán cartillas que cartillas deben ser entregadas a los usuarios que utilizaran el servicio de correo electrónico corporativo en dispositivos móviles, quienes además deben conocer las políticas establecidas para la utilización de dispositivos móviles.

Cuadro 16. Plan de difusión y sensibilización

No	Actividad	Propósito	Responsables / Destinatarios
1	Crear cronograma de difusión y sensibilización	Mantener el usuario actualizado y concientizado de la aplicación de las políticas	Oficial de Seguridad de la Información.
2	Creación de cartillas didácticas cuyo contenido sean las políticas	Hacer que los funcionarios de la Entidad conozcan de manera didáctica las políticas.	Oficial de Seguridad de la Información y Oficina de comunicaciones
3	Reproducción y distribución de las políticas.	Permitir que los funcionarios de la Entidad conozcan las políticas.	Oficial de Seguridad de la Información y Usuario del GIT – soporte tecnológico
4	Difusión por medio de intranet	Entregar vía correo electrónico el material relacionado con cartillas didácticas. Ver Anexo No 5	Dirigido a todos los usuarios del servicio de correo electrónico
5	De manera presencial divulgar las políticas	Sensibilizar y concientizar a los usuarios de la importancia de aplicar las políticas	Oficial de Seguridad de la Información
			Usuarios del servicio de la Entidad
6	Orientar mediante charlas a todos los usuarios de todos los niveles de la Entidad.	Sensibilizar y concientizar a todos los usuarios de los riesgos por incumplimiento de políticas.	Oficial de Seguridad de la Información
			Usuarios del servicio de la Entidad
7	Elaborar carteleras y publicar los contenidos relacionadas con las cartillas de políticas.	Otra manera de hacer llegar el mensaje de las políticas relacionadas con la utilización del servicio de correo corporativo.	Oficial de Seguridad de la Información y Oficina de comunicaciones

5. CONCLUSIONES

- Con el mejoramiento de la seguridad del servicio de correo electrónico corporativo en dispositivos móviles, la movilidad empresarial en el DPS permitirá que los usuarios utilicen el servicio de correo electrónico de manera transparente y segura en cada dispositivo, puesto que mediante este proyecto se busca alcanzar mejor desempeño y gestión de la movilidad en la Entidad, al implementar políticas y controles de seguridad de la información.

- Al realizar el desarrollo de este proyecto, fue posible identificar los requerimientos relacionados con el uso del correo electrónico corporativo en dispositivos móviles en el DPS, mediante los cuales se identificaron vulnerabilidades y amenazas en la utilización de este servicio en la Entidad.

- Se han identificado dos políticas relacionadas con el uso del servicio de correo electrónico corporativo en el DPS, con las cuales es posible gestionar la movilidad en la entidad mediante la implementación de los controles que las compone. Dichas políticas son:
    1. Política de dispositivos móviles.
    2. Política de uso de recursos tecnológicos

- Haciendo uso de la documentación de la suite de *Mcafee* relacionada con la arquitectura *EMM,* es posible definir los requerimientos a nivel de Hardware y Software necesarios para realizar la instalación y puesta en marcha de la herramienta, en función de los requisitos identificados y las políticas propuestas.

- La movilidad empresarial es un factor determinante en las relaciones del trabajador con las empresas, ya no es necesario que la Entidad le asigne

un dispositivo móvil al trabajador para que este interactúe con aplicaciones como la de correo electrónico corporativo.

- El proyecto también propone un plan de capacitación con el cual será posible concientizar a los usuarios del servicio de correo electrónico corporativo mediante la utilización de dispositivos móviles propios o de la Entidad, relacionada con la responsabilidad que asume cada quien en su utilización.

- La demanda de accesos a redes corporativas se ha incrementado con el uso de dispositivos móviles, los usuarios demandan tener conexión desde cualquier lugar, en cualquier momento y desde cualquier dispositivo. Es decir, apostar por una política de movilidad empresarial trae consigo un atractivo para los recursos humanos más dinámicos y capacitados, además de oportunidad para retenerlos ya que se les está ofreciendo un equilibrio entre buenas condiciones de trabajo y flexibilidad, calidad de vida. La movilidad empresarial representa una ventaja competitiva en términos de recursos humanos unida a la innovación y desarrollo.

- Como resultado del análisis de las encuestas, entrevistas y observación de los documentos de información relacionados con el SGSI del DPS, se encontraron amenazas / vulnerabilidades representativas asociadas al uso del correo corporativo en los dispositivos móviles, como: debilidad en sistema de autenticación, ausencia de control de datos y servicio de correo corporativo, violación o incumplimiento de las políticas de seguridad en dispositivos móviles, ausencia del inventario de dispositivos móviles, soporte inadecuado a usuarios, pérdida o robo de dispositivos, fuga de datos o la divulgación inadvertida de la información confidencial e inadecuada estrategia de protección contra las amenazas o ataques.

BIBLIOGRAFIA

AIRWATCH Panrico incrementa productividad de sus empleados con el uso de las soluciones de AirWatch. Consultado el 16 de julio 2015.Disponible en: http://www.air-watch.com/uploads/global-media/es-airwatch-panrico.pdf.

CCM BENCHMARK. Cómo funciona el correo electrónico (MTA, MDA, MUA). Consultado el 26 de julio 2015.Disponible en: http://es.ccm.net/contents/115-como-funciona-el-correo-electronico-mta-mda-mua.

CORPORACIÓN COLOMBIA DIGITAL, Estrategia de TI en el Estado colombiano. Consultado el 5 de mayo 2015. Disponible en: http://www.colombiadigital.net/quienes-somos/item/8022-estrategia-de-ti-en-el-estado-colombiano.html.

CREDINKA. Consultado el 16 de julio 2015. Disponible en: http:// www.credinka.com.

DEPARTAMENTO ADMINISTRATIVO PARA LA PROSPERIDAD SOCIAL – DPS disponible en internet: http://www.dps.gov.co/ent/gen/SitePages/Misi%C3%B3n%20y%20visi%C3%B3n.aspx.

DEPARTAMENTO ADMINISTRATIVO PARA LA PROSPERIDAD SOCIAL – DPS Funciones Consultado el 26 de julio 2015 disponible en internet: http://www.dps.gov.co/ent/gen/SitePages/Misi%C3%B3n%20y%20visi%C3%B3n.aspx.

DEPARTAMENTO ADMINISTRATIVO PARA LA PROSPERIDAD SOCIAL – DPS Mision Consultado el 26 de julio 2015 disponible en internet: http://www.dps.gov.co/ent/gen/SitePages/Misi%C3%B3n%20y%20visi%C3%B3n.aspx.

DEPARTAMENTO ADMINISTRATIVO PARA LA PROSPERIDAD SOCIAL – DPS Vision Consultado el 26 de julio 2015 disponible en internet: http://www.dps.gov.co/ent/gen/SitePages/Misi%C3%B3n%20y%20visi%C3%B3n.aspx.

DEPARTAMENTO ADMINISTRATIVO PARA LA PROSPERIDAD SOCIAL – DPS Consultado el 5 de mayo 2015. en disponible en internet: http://www.dps.gov.co/contenido/contenido.aspx?catID=3&conID=544&pagID=18024.

DINERO. DEPRISA fortalece su negocio con tecnología. Citado en 23 de Septiembre de 2014. Disponible en: http://www.dinero.com/empresas/articulo/tecnologia-usada-deprisa/201300.

GUILARTE María . Dell muestra durante Dell World su apuesta por la innovación en software ante las nuevas tendencias IT. Consultado el 26 de julio 2015. Disponible en: http://www.muycomputerpro.com/2013/12/12/dell-enterprise-mobility-management.

GUTIÉRREZ Tatiana. 5 prácticas para controlar la movilidad en tu empresa. Consultado el 26 de julio 2015. Disponible en: http://www.altonivel.com.mx/44006-5-practicas-para-controlar-la-movilidad-en-tu-empresa.html.

.

MAGAZCITUM. ISO-27001:2013 ¿Qué hay de nuevo? Consultado el 26 de julio 2015. Disponible en: http://www.magazcitum.com.mx/?p=2397#.VbgYfMB_Oko.

MARTÍNEZ Marcelo. La compañía financiera dedicada al microcrédito amplía su cobertura en las zonas urbanas y rurales de Perú a través de la tecnología Citrix que le permite distribuir sus aplicaciones de negocios en todo el país. Consultado el 16 de julio 2015. Disponible en: https://lac.citrix.com/customers/caso-credinka-peru-es.html

PÉREZ ARBESÚ, Lizzette, Empresas latinoamericanas apuestan fuerte por la movilidad en 2015. Consultado el 5 de mayo 2015. Disponible en: http://searchdatacenter.techtarget.com/es/cronica/Empresas-latinoamericanas-apuestan-fuerte-por-la-movilidad-en-2015.

TEIXIDÓ Carlos. Gestión de la movilidad empresarial. Consultado el 26 de julio 2015. Disponible en: http://www.emb.cl/gerencia/articulo.mvc?xid=3357.

TNX. La movilidad empresarial. Consultado el 26 de julio 2015. Disponible en: http://tnxcorp.com/service/la-movilidad-empresarial/.

VEGA Salvador. Estrategias de movilidad y éxito empresarial. Consultado el 26 de julio 2015. Disponible en: http://www.larepublica.co/estrategias-de-movilidad-y-%C3%A9xito-empresarial_245116.

Anexos

ANEXOS

Anexo A. Formulario de encuesta a funcionarios del DPS

ENCUESTA PARA FUNCIONARIOS DEL DPS

IMPLEMENTACIÓN DE LA GESTIÓN DE LA MOVILIDAD EMPRESARIAL (ENTERPRISE MOBILITY MANAGEMENT - EMM) PARA LA GESTION DEL CORREO CORPORATIVO EN EL DEPARTAMENTO PARA LA PROSPERIDAD SOCIAL – DPS

*Obligatorio

Dependencia / Programa *

Área, Programa o Dependencia a la cual pertenece

1) ¿Qué tipo de relación laboral desarrolla con la Entidad? *

Selecciones una respuesta

- a) Vinculación Por Planta – Carrera Administrativa
- b) Vinculación Por Planta – Provisional
- c) Contrato de prestación de servicios
- d) Contrato a través de terceros
- e) Vinculación Por Planta – de libre nombramiento y remoción

2) ¿Qué rol desempeña dentro de los sistemas de información del DPS? *

Seleccione una o varias respuestas según corresponda

- ○ a) Administrador
- ○ b) Directivo
- ○ c) Desarrollador o programador
- ○ d) Soporte de aplicativo
- ○ e) Usuario Final Interno
- ○ f) Usuario Final Externo
- ○ g) Programador /desarrollador externo

3) ¿De los siguientes controles de seguridad de la información, cuáles son aplicados en su desempeño laboral? *

Seleccione una o varias respuestas según corresponda

- ☐ a) Control sobre el uso general del computador en el trabajo,
- ☐ b) Control para el uso de dispositivos de almacenamiento externo (memorias o discos USB)
- ☐ c) Control para el manejo de claves de usuario
- ☐ d) Control para el uso de enlaces Inalámbricos
- ☐ e) Control para el uso del internet
- ☐ f) Control para realizar copias de seguridad de la información
- ☐ g) Control en el uso del correo electrónico.
- ☐ h) Control para el cierre de sesión y bloqueo de acceso al equipo ante ausencias temporales
- ☐ i) Control sobre el resguardo y protección de la información
- ☐ j) Control para el mantenimiento del computador
- ☐ k) Control para atención de ayuda a usuarios – help desk

4) ¿Para el manejo de contraseñas de su equipo y/o programas qué tipo de combinación de caracteres utiliza? *

Seleccione una respuesta según corresponda

- ○ a) Solo nombres conocidos
- ○ b) Fechas conocidas
- ○ c) Solo minúsculas
- ○ d) Solo mayúsculas
- ○ e) Combinación de mayúsculas y minúsculas
- ○ f) Combinación de letras y números
- ○ g) Combinación de todo tipo de caracteres

5) ¿Cuantos caracteres o letras utiliza para sus contraseñas? *

Seleccione una respuesta según corresponda

- ○ a) Entre uno y tres
- ○ b) Entre cuatro y seis
- ○ c) Entre siete y nueve
- ○ d) Entre diez y doce
- ○ e) Más de doce caracteres

6) Por labores propias de su desempeño en el trabajo usted? *

Selecciones una o varias respuestas según corresponda

- ☐ a) Procesa información fuera de la Entidad
- ☐ b) Se conecta a través de escritorio remoto al computador de la Entidad
- ☐ c) Recibe asesorías a través de escritorio remoto
- ☐ d) No requiere conectarse remotamente.
- ☐ e) No requiere llevar información a su casa
- ☐ f) Lo trabaja en horario extendido en la Entidad

7) En su desempeño laboral, ha sufrido incidentes como: *

Selecciones una o varias respuestas según corresponda

- [ ] a) Ataque de virus informáticos
- [ ] b) Pérdida de información
- [ ] c) Lentitud en los procesos o aplicaciones
- [ ] d) Pérdida de conexión con algún aplicativo
- [ ] e) Discontinuidad en algunos de los servicios corporativos (internet, aplicaciones, correo electrónico, etc.)
- [ ] f) Daño en su equipo de trabajo
- [ ] g) Ninguno de los anteriores
- [ ] h) Todas las anteriores

8) La frecuencia con que han sucedido los incidentes en su equipo de trabajo es: *

Seleccione una respuesta según corresponda

- ( ) a) A diario
- ( ) b) Cada semana
- ( ) c) Cada mes
- ( ) d) Cada tres meses
- ( ) e) Cada seis meses
- ( ) f) Cada año
- ( ) g) Más de un año
- ( ) h) Nunca

9) ¿Utiliza el servicio de correo electrónico corporativo en su dispositivo móvil? *

Seleccione una respuesta según corresponda

- ( ) a) Siempre
- ( ) b) Algunas veces
- ( ) c) Nunca

10) ¿Para poder utilizar el servicio de correo electrónico corporativo desde su dispositivo móvil usted debe diligenciar alguna forma de registro? *

Seleccione una respuesta según corresponda

- a) Siempre
- b) Algunas veces
- c) Nunca

11) ¿Al utilizar el servicio de correo electrónico corporativo desde su dispositivo móvil usted ha sufrido perdida de información? *

Seleccione una respuesta según corresponda

- a) Siempre
- b) Algunas veces
- c) Nunca

12) Si su respuesta a la pregunta anterior fue afirmativa ¿Cuántas veces ha sufrido perdida de información? *

Seleccione una respuesta según corresponda

- a) de 1 a 5 veces
- b) de 6 a 10 veces
- c) más de 10 veces
- c) Nunca

13) ¿Es consciente de la responsabilidad como funcionario público al utilizar el servicio de correo electrónico corporativo desde su dispositivo móvil? *

Seleccione una respuesta según corresponda

- a) Mucha
- b) Poca
- c) Ninguna

14) ¿La Entidad le ha brindado capacitación como funcionario público para utilizar el servicio de correo electrónico corporativo desde su dispositivo móvil? *

Seleccione una respuesta según corresponda

- a) Suficiente
- b) Escasa
- c) Ninguna

Enviar

100 %: ¡Lo lograste!

Nunca envíes contraseñas a través de Formularios de Google.

Anexo B. Análisis de la Información

Analizando los resultados de la encuesta se identifican diferentes variables tales como la información que se maneja, algunos hábitos de usuarios, vulnerabilidades, políticas de seguridad informática, controles de políticas, riesgos, entre otras. Se obtiene los siguientes resultados:

1. ¿Qué tipo de relación laboral desarrolla con la Entidad?

Resultado:

A continuación en el cuadro No 1 y la Figura No 1 se presenta el tipo de vinculación de los encuestados y su participación por nivel, siendo el más representativo la vinculación de planta como provisional.

Cuadro 1. Tipos de vinculación

Respuesta	Valor
a) Vinculación Por Planta – Carrera Administrativa	**9,8%**
b) Vinculación Por Planta – Provisional	**56,9%**
c) Contrato de prestación de servicios	**3,9%**
d) Contrato a través de terceros	**5,9%**
e) Vinculación Por Planta – de libre nombramiento y remoción	**23,5%**

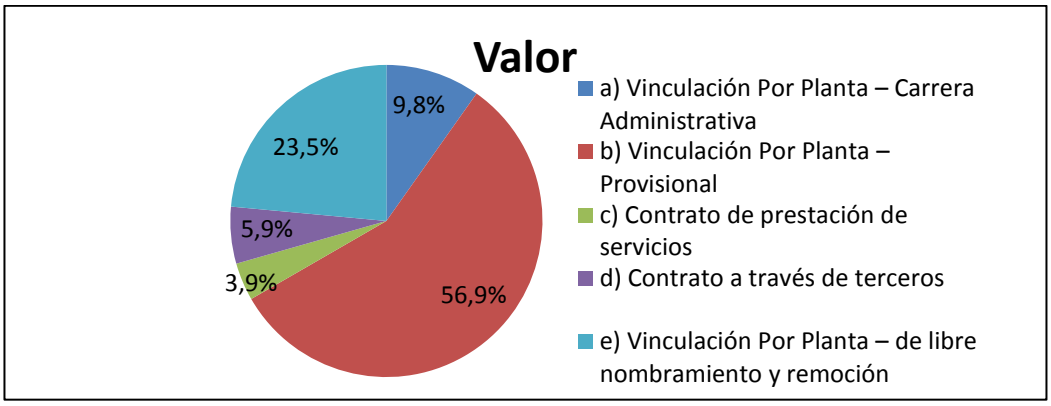


Figura 1. Tipos de vinculación

2. ¿Qué rol desempeña dentro de los sistemas de información del DPS?

Resultado:

En este apartado se presenta el Cuadro No 2 y la gráfica No 2 que permite mostrar el rol que cumple cada usuario en el dinamismo de la Entidad y su relación con los sistemas de información.

Cuadro 2. Roles de los funcionarios del DPS

Respuesta	Valor
a) Administrador	**9,8%**
b) Directivo	**3,9%**
c) Desarrollador o programador	**23,5%**
d) Soporte de aplicativo	**5,9%**
e) Usuario Final Interno	**56,9%**
f) Usuario Final Externo	**0,0%**
g) Programador /desarrollador externo	**0,0%**

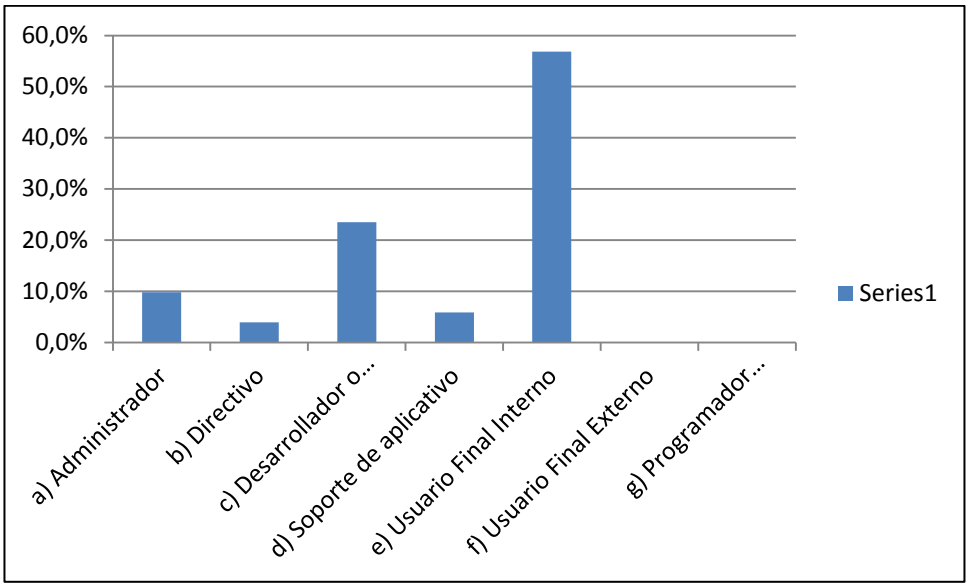


Figura 2. Roles de los funcionarios del DPS

3) ¿De los siguientes controles de seguridad de la información, cuáles son aplicados en su desempeño laboral?

Resultado:

Como se evidencia, todos los controles son utilizados en alguna medida por los funcionarios del Departamento para la Prosperidad SOCIAL – DPS, en la realización de sus actividades diarias.

El 90.2% de los encuestados manifiesta utilizar el control relacionado con el uso del computador en el trabajo, adicionalmente, se observa que ninguna de los controles son aplicados con una rigurosidad del 100%, el resultado de utilización de cada control se observa en el siguiente cuadro No. 3. y la gráfica No 3

Cuadro 3. Controles en la Entidad

Respuesta	Valor
a) Control sobre el uso general del computador en el trabajo,	90,2%
b) Control para el uso de dispositivos de almacenamiento externo (memorias o discos USB)	7,8%
c) Control para el manejo de claves de usuario	82,4%
d) Control para el uso de enlaces Inalámbricos	9,8%
e) Control para el uso del internet	9,8%
f) Control para realizar copias de seguridad de la información	58,8%
g) Control en el uso del correo electrónico.	31,4%
h) Control para el cierre de sesión y bloqueo de acceso al equipo ante ausencias temporales	82,4%
i) Control sobre el resguardo y protección de la información	66,7%
j) Control para el mantenimiento del computador	3,9%
k) Control para atención de ayuda a usuarios – help desk	7,8%

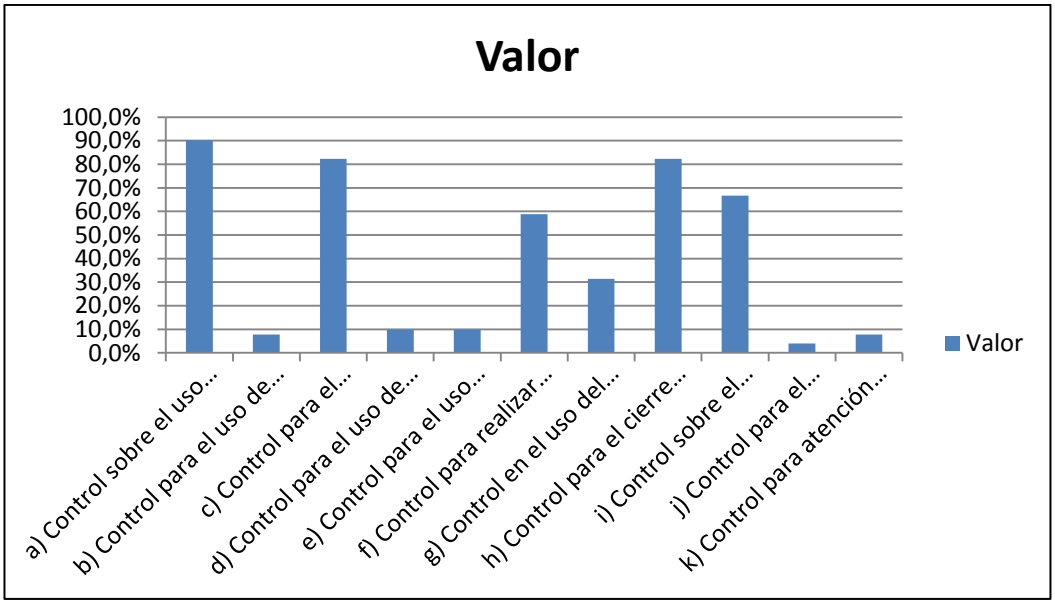


Figura 3. controles en la Entidad

4) ¿Para el manejo de contraseñas de su equipo y/o programas qué tipo de combinación de caracteres utiliza?

Resultado:

Como política de acceso al sistema de información se obtiene un 52.9% de los usuarios utilizan una combinación de todo tipo de caracteres para conformar sus contraseñas. Los porcentajes más bajos corresponden al 2% y se asocia con la utilización de fechas conocidas y el empleo de letras mayúsculas y minúsculas para conformar las contraseñas, como se indica en el cuadro No.4. y Figura No 4

Cuadro 4. Formación de contraseñas

Respuesta	Valor
a) Solo nombres conocidos	0,0%
b) Fechas conocidas	2,0%
c) Solo minúsculas	5,9%
d) Solo mayúsculas	0,0%
e) Combinación de mayúsculas y minúsculas	2,0%
f) Combinación de letras y números	37,3%
g) Combinación de todo tipo de caracteres	52,9%

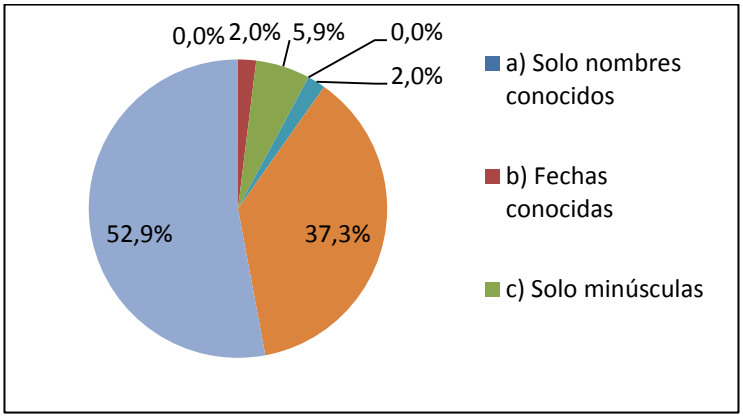


Figura 4. formación de contraseñas

5) ¿Cuantos caracteres o letras utiliza para sus contraseñas?

Resultado:

Este factor importante en la utilización formación de contraseñas, se observar que el 41, 2% de los funcionarios encuestados utiliza una contraseña fuerte que contribuye a una mayor seguridad de la información.

El 7,8% utiliza entre cuatro y seis caracteres, esto podría representar una debilidad cuando algún extraño trata de averiguar la contraseña que por diccionario o fuerza bruta tarda menos tiempo en conseguirlo, el resumen se aprecia en el cuadro No 5 y gráfica No 5.

Cuadro 5. Longitud de las contraseñas

Respuesta	Valor
a) Entre uno y tres	0,0%
b) Entre cuatro y seis	7,8%
c) Entre siete y nueve	25,5%
d) Entre diez y doce	41,2%
e) Más de doce caracteres	25,5%

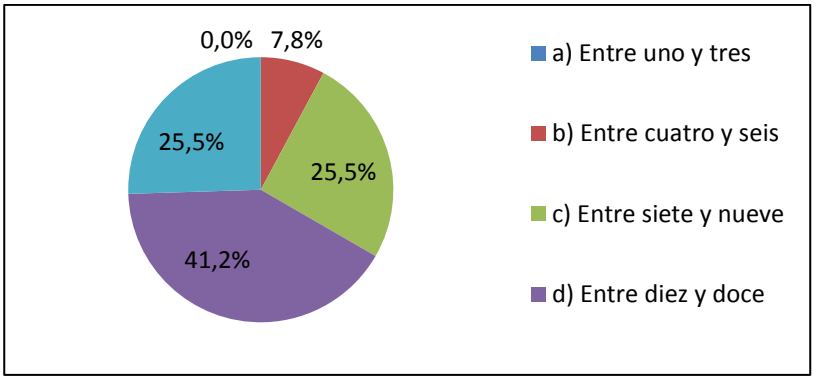


Figura 5. Longitud de las contraseñas

6) Por labores propias de su desempeño en el trabajo usted?

Resultado:

Realizando un análisis a la información contenida en el cuadro No 6 y la gráfica No 6 se evidencia que existen vulnerabilidades en el tratamiento de la información, ya que el 52.9% se conecta al computador de la Entidad y el 49.0% procesa información fuera de la Entidad, el 31.4% no requiere llevar información para la casa, así como el 19.6% no requiere conectarse remotamente, y tan sólo el 2% manifiesta recibir asesorías utilizando el escritorio remoto.

En conclusión existen vulnerabilidades para procesar información fuera de la Entidad, generando una amenaza que atenta contra la confidencialidad e integridad de la información.

Cuadro 6. Vulnerabilidades en la Información

Respuesta	Valor
a) Procesa información fuera de la Entidad	**49,0%**
b) Se conecta a través de escritorio remoto al computador de la Entidad	**52,9%**
c) Recibe asesorías a través de escritorio remoto	**2,0%**
d) No requiere conectarse remotamente.	**19,6%**
e) No requiere llevar información a su casa	**31,4%**
f) Lo trabaja en horario extendido en la Entidad	**11,8%**

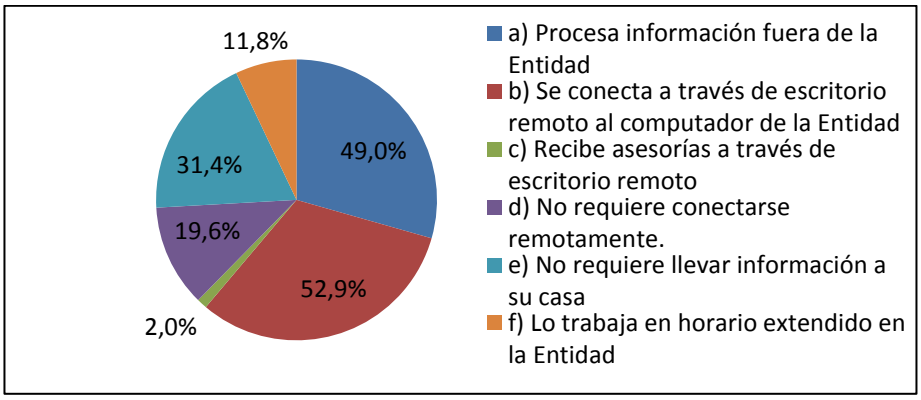


Figura 6. Vulnerabilidades en la Información

7) En su desempeño laboral, ha sufrido incidentes como:

Resultado: La respuesta es múltiple con respecto a los incidentes ocurridos existe un promedio del 80.4% que afirma haber sufrido algún tipo de incidente relacionado con la lentitud en los proceso o aplicaciones y la discontinuidad en algunos de los servicios corporativos (internet, aplicaciones, correo electrónico, etc.). Los incidentes más bajo porcentaje ocurridos son de Daño en su equipo de trabajo, como se indica en el cuadro No. 7 y la gráfica No 7.

Cuadro 7. Incidentes de seguridad de la Información

Respuesta	Valor
a) Ataque de virus informáticos	**72,5%**
b) Pérdida de información	**66,7%**
c) Lentitud en los procesos o aplicaciones	**80,4%**
d) Pérdida de conexión con algún aplicativo	**76,5%**
e) Discontinuidad en algunos de los servicios corporativos (internet, aplicaciones, correo electrónico, etc.)	**80,4%**
f) Daño en su equipo de trabajo	**9,8%**
g) Ninguno de los anteriores	**3,9%**
h) Todas las anteriores	**0,0%**

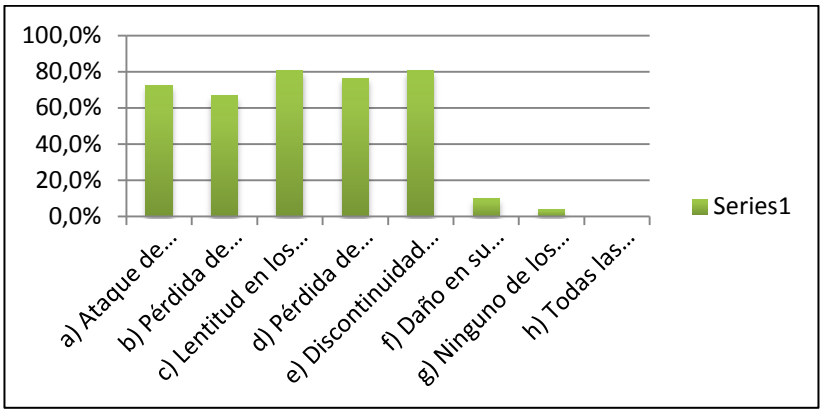


Figura 7. Incidentes de seguridad de la Información

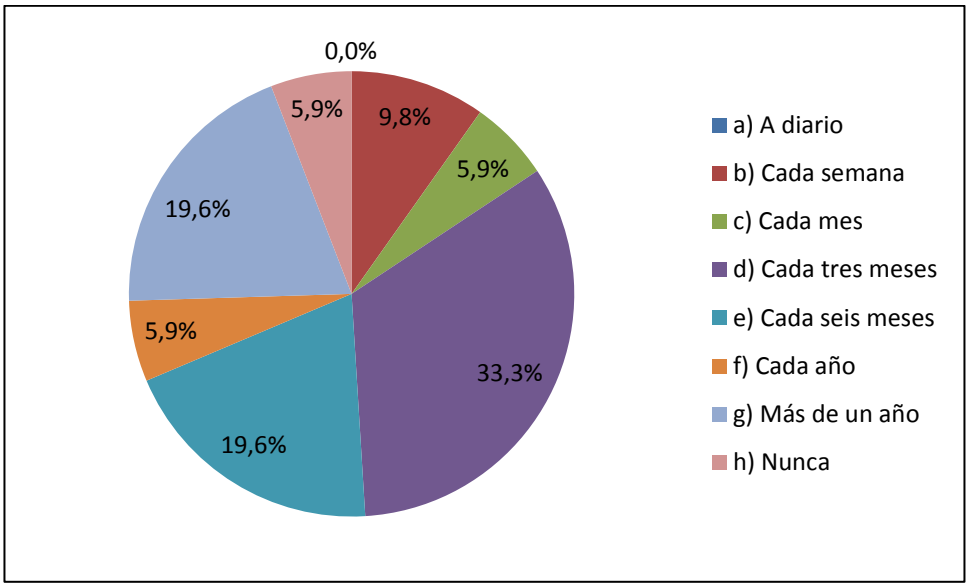
8) La frecuencia con que han sucedido los incidentes en su equipo de trabajo es:

Resultado:

Como respuestas más significativa esta el 33.3% de frecuencia de incidentes ocurrida cada tres meses seguida la del 19.6% que corresponden a las frecuencias de cada seis meses y más de un año, Lo anterior se puede observar en el cuadro No. 8 y gráfica No 8.

Cuadro 8. Frecuencias de Incidentes

Respuesta	Valor
a) A diario	**0,0%**
b) Cada semana	**9,8%**
c) Cada mes	**5,9%**
d) Cada tres meses	**33,3%**
e) Cada seis meses	**19,6%**
f) Cada año	**5,9%**
g) Más de un año	**19,6%**
h) Nunca	**5,9%**



Gráfica 8. Frecuencias de Incidentes.

9) ¿Utiliza el servicio de correo electrónico corporativo en su dispositivo móvil?

Resultado:

Al respecto las respuestas se evidencian en el cuadro No 9 y Figura No 9, en el cual se observa que el 72,5% no utiliza el servicio de correo electrónico corporativo en el dispositivo móvil.

Cuadro 9. Frecuencia de utilización del servicio de correo corporativo en los dispositivos móviles

Respuesta	Valor
a) Siempre	**7,8%**
b) Algunas veces	**19,6%**
c) Nunca	**72,5%**

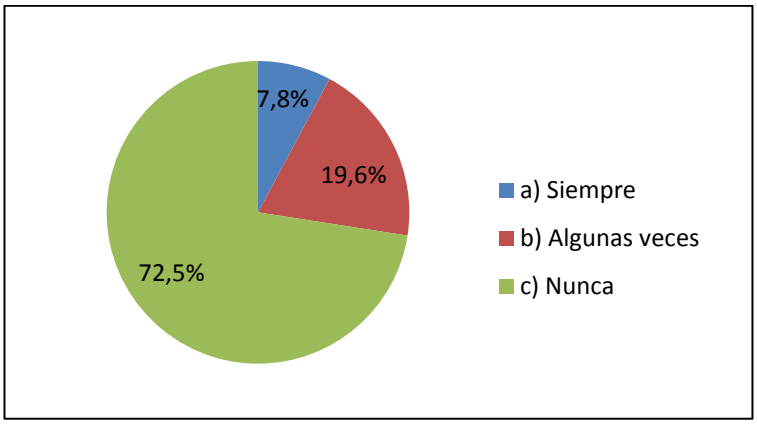


Figura 9. Frecuencia de utilización del servicio de correo corporativo en los dispositivos móviles.

10) ¿Para poder utilizar el servicio de correo electrónico corporativo desde su dispositivo móvil usted debe diligenciar alguna forma de registro?

Resultado:

Al respecto las respuestas se evidencian en el cuadro No 10 y Figura No 10, donde se observa que el 94,1% nunca diligencia alguna forma de registro de los dispositivos móviles, para utilizar el servicio de correo electrónico corporativo.

Cuadro 10. frecuencia de registro de dispositivos móviles

Respuesta	Valor
a) Siempre	**3,9%**
b) Algunas veces	**2,0%**
c) Nunca	**94,1%**

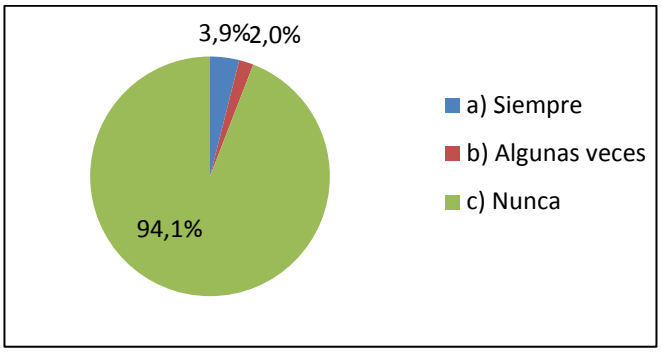


Figura 10. Frecuencia de registro de dispositivos móviles

11) ¿Al utilizar el servicio de correo electrónico corporativo desde su dispositivo móvil usted ha sufrido perdida de información?

Resultado:

Al respecto las respuestas se evidencian en el cuadro No 11 y gráfica No 11, donde se observa que el 94,1% manifiesta no haber sufrido perdida de información en la utilización del servicio de correo electrónico corporativo.

Cuadro 11. Frecuencia de perdida de información

Respuesta	Valor
a) Siempre	**0,0%**
b) Algunas veces	**5,9%**
c) Nunca	**94,1%**

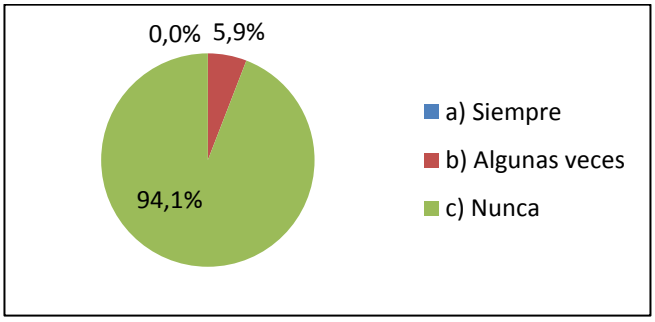


Figura 11. Frecuencia de pérdida de información

12) Si su respuesta a la pregunta anterior fue afirmativa ¿Cuántas veces ha sufrido perdida de información?

Resultado:

Al respecto las respuestas se evidencian en el cuadro No 12 y gráfica No 12, donde se observa que el 58,8% manifiesta no haber sufrido perdida de información en la utilización del servicio de correo electrónico corporativo en su dispositivo móvil.

Cuadro 12. Perdida de información

Respuesta	Valor
a) de 1 a 5 veces	**9,8%**
b) de 6 a 10 veces	**31,4%**
c) más de 10 veces	**0,0%**
c) Nunca	**58,8%**

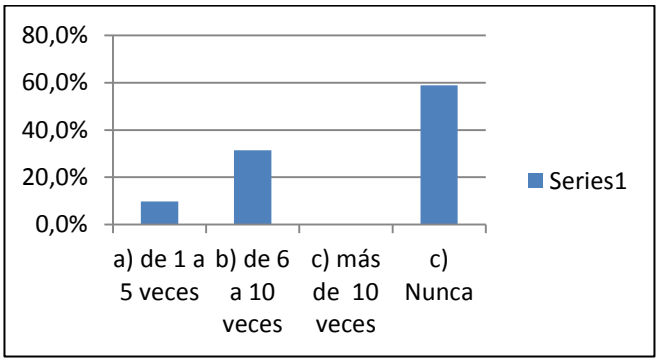


Figura 12. Perdida de información

13) ¿Es consciente de la responsabilidad como funcionario público al utilizar el servicio de correo electrónico corporativo desde su dispositivo móvil?

Resultado:

Según la información presentada en el cuadro No 13 y Figura No 13 donde se observa que el 49% de los encuestados manifiesta desconocer el grado de responsabilidad como funcionario público en la utilización del servicio de correo electrónico corporativo desde los dispositivos móviles.

Cuadro 13. Nivel de responsabilidad

Respuesta	Valor
a) Mucha	**45,1%**
b) Poca	**5,9%**
c) Ninguna	**49,0%**

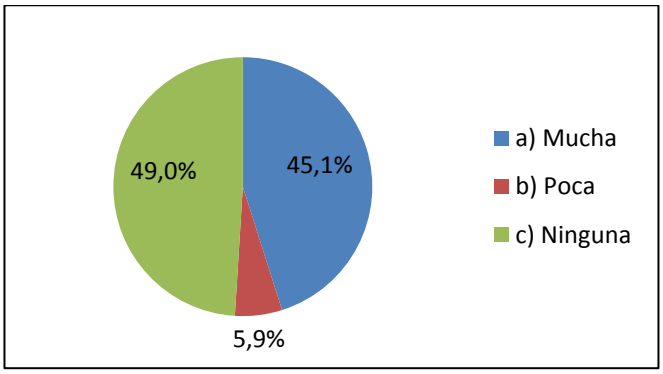


Figura 13. Nivel de responsabilidad

14) ¿La Entidad le ha brindado capacitación como funcionario público para utilizar el servicio de correo electrónico corporativo desde su dispositivo móvil?

Resultado:

Según la información presentada en el cuadro No 14 y gráfica No 14 donde se observa que el 98% de los encuestados manifiesta que la Entidad no ha adelantado capacitación alguna para utilizar el servicio de correo electrónico corporativo en los dispositivos móviles.

Cuadro 14. Nivel de capacitación

Respuesta	Valor
a) Suficiente	**2,0%**
b) Escasa	**0,0%**
c) Ninguna	**98,0%**

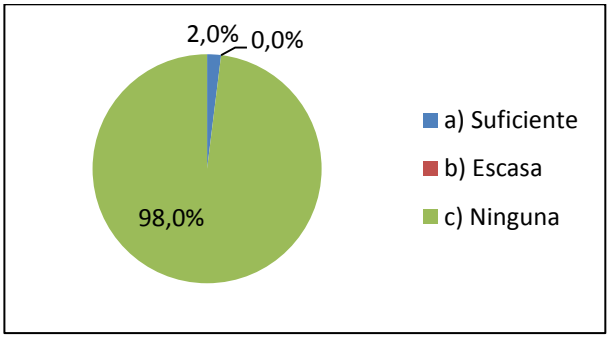


Figura 14. Nivel de capacitación

Análisis de resultados de la Entrevista con el oficial de seguridad

A continuación se presenta el temario de la entrevista que se realizó al oficial de seguridad de la información del DPS, quien es un contratista y dentro de sus funciones tiene asignado este rol dentro de la Entidad.

GUÍA DE ENTREVISTA PARA ADMINISTRADORES DE SERVICIOS INFORMATICOS Y OFICIAL DE SEGURIDAD DEL DPS

Objetivo: determinar los requerimientos relacionados con la prestación del servicio de correo corporativo y la utilización de dispositivos móviles en el Departamento para la Prosperidad Social - DPS.

La entrevista será grabada con autorización del entrevistado y será utilizada solo para el análisis de información y desarrollo del proyecto propuesto, con el compromiso de que la información será de estricta confidencialidad y nada de lo que se diga será divulgado.

Además, una vez analizada la entrevista esta será borrada.

TEMARIO DE PREGUNTAS:

1) ¿Cuál es su cargo en la Entidad? Oficial de la Información – contrato de prestación de servicios
2) ¿Cuál es su relación contractual con la Entidad? R. contratista
3) ¿Qué tipo de información maneja o administra en la Entidad? Oficial de Seguridad de la Información.
a) ¿Quién es el directo responsable de la información que maneja? El custodio y propietario de la información.
b) ¿Qué tan importante la considera para la institución? De vital importancia, activo de mayor valor.
c) ¿Considera que la información administrada es imprescindible, para el normal desarrollo de la Entidad? R. Si la información es el activo más importante para la Entidad.
d) ¿Califique de 1 a 10 el valor de la información 1 mínimo valor, 10 valor máximo? 10
4) ¿El DPS tiene implementado procedimientos escritos para la prestación de servicio de correo electrónico corporativo? Valor de la información 10 – máximo valor como activo
5) ¿Tiene implementado procedimientos escritos de custodia de la información? No se tiene
6) ¿Tiene implementado procedimientos escritos para la restauración de las copias de seguridad de la información? Si existen existe un cronograma.
7) ¿El DPS cuenta con una estrategia de continuidad del negocio? Si le contestan que no, puede preguntar por qué no……?si existe una psi y el DPS tiene contratado un contrato con un prestador del servicio.
8) ¿Cuál es el procedimiento para realizar la configuración de servidores tanto de aplicaciones como de bases de datos y otros? Existe este procedimiento y es la guía para

quienes administran los servicios de los servidores de aplicación y de bases de datos.

9) ¿Qué políticas de seguridad de acceso a la información aplica la Entidad a la prestación del servicio de correo electrónico corporativo y qué se encuentre implementado? No existe políticas

a) ¿Cómo se gestiona la protección de información sensible? Existe un algo riesgo de fuga de información

b) ¿Cómo se gestionan los privilegios de acceso a la información de la aplicación? Autenticación de usuarios a través del directorio activo.

c) ¿Qué procedimiento tiene implementado para la gestión de contraseñas? Complejidad tamaño y tiempo para realizar gestión de contraseñas.

d) ¿En qué horarios se tiene acceso a la aplicación? 24 horas al día 360 dias al año

e) ¿De qué manera se monitorea y revisa los derechos de acceso de los usuarios? Reportes

10) ¿Qué controles tiene implementado en la aplicación para salvaguardar la integridad disponibilidad y confidencialidad de la información? solo disponibilidad.

a) ¿Cómo se manejan los privilegios de los usuarios administradores?

i) Si

(1) ¿Para qué actividades utiliza estos privilegios? Soporte técnico a nivel de sistemas operativos y de aplicaciones.

(2) ¿Hasta qué nivel de privilegios tiene? Depende del rol del administrador.

ii) No

(1) ¿Por qué no existen más usuarios con este tipo de privilegios?

(2) ¿Los privilegios de administrador tiene clave compartida? Si

11) En cuanto al manejo de contraseñas para acceso al equipo y/o aplicaciones.

a) ¿Qué PSI tiene implementado? Las que se definieron con el SGSI de la Entidad.

b) ¿Cómo controla los privilegios?

c) ¿Cuál es el proceso de creación de contraseñas? Mediante el Directorio Activo

d) ¿Tiene algún procedimiento para los usuarios que han terminado su contrato, han sido Suspendidos o han salido de vacaciones? Sip. Varias políticas hablan de este aspecto.

e) ¿El ingreso a la aplicación o información tienen establecidos horarios de ingreso? No

f) ¿Cómo controlan los accesos a la aplicación en horarios extendidos? No.

g) ¿Cómo controlan las PSI implementadas? Auditorias.

12) ¿Cómo se gestiona y controla el servicio de correo electrónico corporativo desde dispositivos móviles? No está implementado.

a) ¿Qué tipo de dispositivos móviles utilizan los usuarios? De la Entidad y propios

b) ¿Cómo controlan este tipo de acceso? Directorio Activo

13) ¿La aplicación que maneja este servicio utiliza sistemas de encriptación?

a) Sobre las aplicaciones

b) Las Comunicaciones. SI

c) Soporte de la información

d) Sobre el correo electrónico

14) ¿Existe alguna aplicación / programa para monitorear el acceso de usuarios a la aplicación durante las 24 horas del día y los 360 días del año? No.

a) ¿Cómo se administran el monitoreo? y existe algún profesional encargado de analizar la información sensible de la base de datos. No

15) ¿Llevan algún registro de auditoria sobre el ingreso de los usuarios que gestionan el servicio de correo electrónico corporativo? No existe.

18) ¿Cuándo un dispositivo móvil requiere mantenimiento que procedimiento sigue? No se tiene implementado.

19) ¿Usted conoce de los incidentes que han vulnerado la seguridad de la información al hacer uso los usuarios de este servicio? Si.

a) ¿Qué incidentes se han presentado? Virus Malware

Análisis de resultados de la Entrevista con el administrador del servicio de correo electrónico

GUÍA DE ENTREVISTA PARA ADMINISTRADORES DE SERVICIOS INFORMATICOS DEL DPS

Objetivo: determinar los requerimientos relacionados con la prestación del servicio de correo corporativo y la utilización de dispositivos móviles en el Departamento para la Prosperidad Social - DPS.

Además, una vez analizada la entrevista esta será borrada.

TEMARIO DE PREGUNTAS:

1. ¿Cuál es su cargo en la Entidad?
   Profesional Especializado Administrador plataforma de colaboración

2. ¿Cuál es su relación contractual con la Entidad?
   Planta – Provisional

3. ¿Cuáles son los activos que están bajo su administración?
   La información relacionada con el Directorio Activo, Correo Electrónico Lync Server y otros

4. ¿Cuál es la disponibilidad del servicio que usted administra?

99.8

5. ¿En el DPS se presentan incidentes de seguridad de la información relacionados con el servicio de correo electrónico corporativo?
   Si lo que tiene que ver con SPAM

6. ¿Cuáles son los incidentes de seguridad de la información relacionados con el servicio de correo electrónico corporativo que se han presentado en la Entidad y con qué frecuencia?
   Los SPAM que se alcanzan a filtrar

7. ¿Actualmente en el DPS se cuenta con una política de seguridad de la información relacionada con el servicio de correo electrónico corporativo?
   Se tienen controles para esto, y la política de seguridad de la información relacionada con el servicio de correo electrónico corporativo.

8. ¿Existen procedimientos documentados para la administración y gestión del servicio de correo electrónico corporativo?
   Si
9. ¿Si la pregunta anterior fue afirmativa indique cuáles son esos procedimientos?
   Registro y gestión de usuarios del servicio de correo electrónico corporativo.

10. ¿Cuáles son los controles de gestión de usuarios y contraseñas para administrar el servicio de correo electrónico corporativo?
    La misma política de directorio activo de cambio de clave cada 30 días y bloqueo por intentos fallidos de 3 Y la clave de cumplir con unos requisitos mínimos de seguridad

11. ¿Qué procedimientos y controles se ejercen desde la administración del servicio de correo electrónico corporativo, sobre los dispositivos móviles en los que se accede al servicio?
    No hay una política como tal.

12. ¿Cuáles incidentes de seguridad de la información relacionada con uso del servicio de correo electrónico corporativo en dispositivos móviles se han

presentado y con qué frecuencia?

No ha habido

13. ¿Qué herramienta tecnológica es empleada para gestionar los usuarios que utilizan el servicio de correo electrónico corporativo en dispositivos móviles?

exchange.

Anexo C. Política de uso de correo electrónico.

Objetivo: Definir las pautas generales para asegurar una adecuada protección de la información del DPS en el uso del servicio de correo electrónico por parte de los usuarios autorizados.

Usos aceptables del servicio

1. Este servicio debe utilizarse exclusivamente para las tareas propias de la función desarrollada en el DPS, no debe utilizarse para ningún otro fin, así mismo se deberá utilizar de manera ética, razonable, eficiente, responsable, no abusiva y sin generar riesgos para la operación de equipos o sistemas de información del DPS.

2. Los usuarios autorizados para usar el servicio de correo electrónico son responsables de todas las actividades realizadas con sus usuarios de acceso a los buzones de correo, así como de mantener un comportamiento ético y acorde a la ley (especialmente las actividades delictivas mencionadas en Ley 1273 de 2009), y de evitar prácticas o usos que puedan comprometer la seguridad de la información del DPS.

3. El servicio de correo electrónico debe ser empleado para servir a una finalidad operativa y administrativa en relación con el DPS. Todas las comunicaciones establecidas mediante este servicio, sus buzones y copias de seguridad se consideran de propiedad del DPS y pueden ser revisadas por el administrador del servicio o cualquier instancia de vigilancia y control, en caso de investigaciones o incidentes de seguridad de la información.

4. Cuando un Proceso, Programa o Dependencia, tenga información de interés institucional para divulgar, lo debe hacer a través de la Oficina de Comunicaciones del DPS.

5. Todos los mensajes enviados deberán respetar el estándar de formato e imagen corporativa definido por el DPS y deberán conservar en todos los casos el mensaje legal corporativo.

6. El único servicio de correo electrónico controlado en la entidad es el asignado directamente por el Grupo de Trabajo de Infraestructura y Soporte de TI, el cual cumple con todos los requerimientos técnicos y de seguridad, evitando ataques de virus, spyware y otro tipo de software malicioso. Además este servicio tiene respaldo de diferentes procesos de copia de respaldo (backup) aplicados de manera periódica y segura. Los demás servicios de correo electrónico serán utilizados a cuenta y riesgo de los usuarios, siendo necesaria la aprobación y firma por parte del Director, Jefe de Oficina, Subdirector o Coordinador de Grupo de Trabajo; de un documento de análisis de riesgos para la autorización de sistemas de correo electrónico diferentes al institucional.

7. El servicio de correo electrónico debe prestarse siempre por medio de un canal cifrado. Este control está a cargo del Grupo de Trabajo de Soporte e Infraestructura.

8. Es responsabilidad del usuario etiquetar el mensaje de correo electrónico de acuerdo a los niveles de clasificación para los cuales se requiere etiquetado (Reservado, Confidencial) según lo definido en el documento Guía de Clasificación y Etiquetado de la Información. Igualmente los adjuntos deben estar etiquetados de acuerdo a lo establecido en dicha guía.

9. El tamaño del buzón de correo electrónico se asignará de manera estandarizada, la capacidad específica será definida y administrada por el Grupo de Trabajo de Infraestructura y Soporte de TI.

10. Todo usuario es responsable de informar si tiene acceso a contenidos o servicios que no le estén autorizados y no correspondan a sus funciones/actividades designadas dentro del DPS, para que de esta forma el Grupo de Trabajo de Infraestructura y Soporte de TI realice el ajuste de permisos requerido.

11. El usuario deberá informar cuando reciba correos de tipo SPAM, correo no deseado o no solicitado, correos de dudosa procedencia o con virus, al Grupo de Infraestructura y Soporte de TI, para que este tome la medidas pertinentes y acciones que impidan el ingreso de ese tipo de correo. De la misma forma el usuario deberá informar al Grupo de Trabajo de Infraestructura y Soporte de TI, cuando no reciba correo y este seguro que este no es de tipo SPAM, de esta forma el Grupo de Trabajo de Infraestructura y Soporte de TI evaluará el origen y tomará las medidas pertinentes.

12. Cuando un Colaborador al que le haya sido autorizado el uso de una cuenta de acceso a la red y al servicio de correo corporativo se retire del DPS, deberá abstenerse de continuar empleándolas y deberá verificar que su cuenta y acceso a los servicios sean cancelados.

13. Los mensajes y la información contenida en los buzones de correo son de propiedad del DPS. Los buzones no deberán contener mensajes con antigüedad superior a un (1) año. El usuario podrá crear un histórico de su correo siempre y cuando sea local (almacenado en el disco duro del

usuario) y bajo su propia responsabilidad.

14. Para el uso del servicio de correo electrónico, el usuario se debe guiar por lo establecido en el Protocolo de Comunicaciones del DPS.

15. Cada usuario se debe asegurar que en el reenvío de correos electrónicos, la dirección de destino es correcta, de manera que esté siendo enviado a las personas apropiadas. Si tiene listas de distribución se deben depurar en el mismo sentido. El envío de información a personas no autorizadas es responsabilidad de quien envía el mensaje de correo electrónico.

16. La información almacenada en los archivos de tipo .PST es responsabilidad de cada uno de los usuarios y cada usuario debe realizar la depuración periódica del buzón para evitar que alcance su límite.

Usos no aceptables del servicio

Este servicio no debe ser usado para:

- Envío de correos masivos que no hayan sido autorizados por un propietario de un proceso misional, estratégico o de apoyo, de acuerdo al mapa de procesos del DPS.

- Envío, reenvío o intercambio de mensajes no deseados o considerados SPAM, cadena de mensajes o publicidad.

- Envío de correos con archivos adjuntos de tamaño superior a la cuota permitida (Quince (15) Mb).

- Envío o intercambio de mensajes con contenido que atente contra la integridad de las personas o instituciones, tales como: ofensivo, obsceno, pornográfico, chistes, información terrorista, cadenas de cualquier tipo, racista, o cualquier contenido que represente riesgo de virus.

- Envío o intercambio de mensajes que promuevan la discriminación sobre la base de raza, género, nacionalidad de origen, edad, estado marital, orientación sexual, religión o discapacidad, o que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluidas el lavado de activos.
- Envío de mensajes que contengan amenazas o mensajes violentos.

- Creación, almacenamiento o intercambio de mensajes que violen las leyes de material protegido por la Ley de derechos de autor.

- Distribución de información del DPS, no PÚBLICA, a otras entidades o ciudadanos sin la debida autorización.

- Crear, enviar, alterar, borrar mensajes de otro usuario sin su autorización.

- Apertura, uso o revisión indebida de la cuenta de correo electrónico de otro usuario como si fuera propia sin la debida autorización.

- Cualquier otro propósito inmoral, ilegal o diferente a los considerados en el apartado “Usos aceptable del servicio” de la presente política.

- Adulterar o intentar adulterar mensajes de correo.

- Enviar mensajes de correo utilizando la cuenta de correo de otra persona exceptuando la administración de calendarios compartidos cuando el Jefe

inmediato lo autorice.

- Enviar correos masivos, con excepción de funcionarios con nivel de Director o superior, quienes sean previamente autorizados por estos para ello, o de funcionarios que en calidad de sus funciones amerite la excepción.

- Intentar acceder a una cuenta de correo de otro usuario o a carpetas y archivos de otra persona sin su autorización. A menos que exista una investigación, un incidente de seguridad de la información o un problema reportado por el usuario.

- Enviar información Confidencial o Reservada del DPS a personas u organizaciones externas, salvo en los casos expresamente previstos en la Constitución Política y en la Ley, y por parte de los funcionarios autorizados internamente para ello.

Condiciones de uso del servicio

1. La configuración del archivo de carpetas de datos personales en el equipo asignado deberá ser regularmente del tipo .PST para todos los usuarios y por excepción del tipo .OST.

2. El servicio de correo electrónico notificará automáticamente (vía correo electrónico) a los usuarios cuando su buzón haya o este por alcanzar su límite. El tamaño de los buzones por defecto es de 300 MB.

3. El usuario será el responsable de la no entrega y/o recepción de mensajes en su buzón cuando se supere la cuota de almacenamiento.

4. Existirán excepciones de capacidad para ciertos buzones que tenga una cuota mayor como el caso de los directores o algunos buzones especiales pero en ningún caso se superará la cuota de 1 GB.

5. Las cuentas institucionales (Ejemplo: Comunica, Servicio al Ciudadano, Soporte, etc.) deben tener una persona responsable que haga depuración del buzón.

6. El password o clave de acceso al servicio es la mejor defensa contra el uso no autorizado de la cuenta de acceso al servicio y/o a la red de datos del DPS por lo tanto se requiere que se mantenga en la mayor reserva posible, no debe suministrarse a otras personas o exhibirse en público.

7. El DPS puede supervisar cualquier cuenta de correo institucional para certificar que se está usando para los propósitos legítimos. El incumplimiento de esta política puede conducir a acciones disciplinarias tales como terminación de la relación laboral o contractual.

8. Todo usuario es responsable por la destrucción de todo mensaje cuyo origen es desconocido, y asume la responsabilidad de las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. En los casos en que el Colaborador desconfíe del remitente de un correo electrónico debe remitir la consulta al correo de seguridad de la información del Grupo de Trabajo de Soporte e Infraestructura (seguridaddelainformacion@dps.gov.co).

9. Si una cuenta de correo es capturada por hackers o se reciben excesiva cantidad de correo no deseado (SPAM), el Grupo de Trabajo de Infraestructura y Soporte de TI tiene libertad para generar una nueva cuenta y borrar la anterior.

10. En caso de que el tamaño de los archivos adjuntos sea muy grande, se recomienda que se compacten o se dividan para evitar que se tengan inconvenientes de recepción o envió. Así también se evitaría el consumo innecesario de recursos.

11. Los Usuarios deben ser conscientes de los riesgos legales que implica la utilización de los medios electrónicos, especialmente en cuanto a la responsabilidad disciplinaria, penal y/o civil en la que pueden incurrir por los inconvenientes, perjuicios y/o reclamaciones de cualquier tipo que llegaren a presentarse como resultado de cualquiera de las siguientes conductas, entre otras:

12. Enviar o reenviar información sensible, sin estar legalmente autorizado para ello.

13. Reenviar o copiar sin permiso mensajes "Confidenciales" o protegidos por las normas sobre derechos de autor, o contra expresa prohibición del originador.

14. El grupo de soporte de TI se reserva el derecho de filtrar los tipos de archivo que vengan anexos al correo electrónico para evitar amenazas de virus y otros programas destructivos. Todos los mensajes electrónicos serán revisados para evitar que tengan virus u otro programa destructivo. Si el

virus u otro programa destructivo no puede ser eliminado, el mensaje será borrado.

15. El usuario debe evitar suscribirse en boletines en líneas con el correo institucional, para evitar la llegada de cadenas de correo, publicidad, etc.

16. Las listas de distribución son administradas por el responsable del grupo de soporte de TI y para su creación se requiere autorización del jefe inmediato.

17. El usuario no debe responder mensajes donde le solicitan información personal o financiera para participar en sorteos, ofertas laborales, ofertas comerciales o peticiones de ayuda humanitaria. Estas situaciones se deben informar al Grupo de Infraestructura y Soporte de TI con el fin de bloquear dicho remitente y evitar que esos mensajes lleguen a más funcionarios. Igualmente se deben marcar estos mensajes como no deseados desde el cliente de correo.

18. Toda cuenta de correo mantenida en el sistema de correo electrónico es de propiedad del DPS. Las cuentas de correo que no sean utilizadas por más de cuarenta y cinco (45) días podrán ser desactivadas por el Grupo de Infraestructura y Soporte de TI.

19. Los correos electrónicos dirigidos a otros dominios deben contener una sentencia de confidencialidad con un contenido como el siguiente (ejemplo):

****

CONFIDENCIALIDAD: Este correo electrónico es correspondencia confidencial del Departamento Administrativo para la Prosperidad Social. Si Usted no es el

destinatario, le solicitamos informe inmediatamente al correo electrónico del remitente o a seguridaddelainformacion@dps.gov.co, así mismo por favor bórrelo y por ningún motivo haga público su contenido, de hacerlo podrá tener repercusiones legales. Si Usted es el destinatario, le solicitamos tener absoluta reserva sobre el contenido, los datos e información de contacto del remitente o a quienes le enviamos copia y en general la información de este documento o archivos adjuntos, a no ser que exista una autorización explícita a su nombre.

****

CONFIDENTIALITY: This email is confidential correspondence of Departamento Administrativo para la Prosperidad Social. If you are not the receiver, you are requested to immediately inform the sender or email seguridaddelainformacion@dps.gov.co, likewise please delete it and do not publicize its content for any reason, due to it may have legal repercussions. If you are the receiver, we ask to have absolute secrecy about the content, data and contact information of the sender and in general about the information in this document or attachments, unless there is an explicit consent under your name.

****

Para todos los usuarios de correo electrónico, el tamaño máximo para recibir o enviar correo será de 15 MB (incluyendo la suma de todos los adjuntos).

Responsabilidades

1. La Subdirección de Talento humano es la responsable de solicitar la creación, modificación o cancelación de las cuentas de acceso a la red y al servicio de Correo electrónico corporativo al Grupo de Trabajo de Infraestructura y Soporte de TI. Cuando se solicite una cuenta institucional se debe justificar e informar de la persona responsable de dicho buzón. Si se detecta que se solicita una cuenta institucional y que no se hace uso de ella,

el Grupo de Trabajo de Infraestructura y Soporte de TI podrá eliminar dicha cuenta.

2. Todos los Colaboradores, en el desarrollo de sus tareas habituales u ocasionales que utilicen cualquier servicio de tecnología de la información y comunicaciones (TIC) que provea el DPS, son responsables del cumplimiento y seguimiento de esta política.

3. El Grupo de Trabajo de Infraestructura y Soporte de TI es el responsable de administrar la plataforma tecnológica que soporta el acceso a la red/cuentas de usuario y/o al servicio de Correo electrónico corporativo para los Colaboradores que desempeñen labores o actividades en el DPS.

4. El Grupo de Trabajo de Infraestructura y Soporte de TI se reserva el derecho de monitorear las comunicaciones y/o información que se comuniquen mediante el servicio de correo electrónico corporativo.

5. El Grupo de Trabajo de Infraestructura y Soporte de TI se reserva el derecho de filtrar los contenidos que se trasmitan en la red del DPS y en uso del servicio de Correo electrónico corporativo.

Anexo D. Riesgos del correo electrónico corporativo

Tipo	nombre	Total Criticidad	Amenaza	Vulnerabiilidad	Impacto (Inventario)	Probabilidad de Ocurrencia Actual	Valor del Riesgo (Impacto x Probabili	Tratamiento del Riesgo	Controles Actuales	Controles Actuales	Controles Actuales	Controles Actuales	Controles Actuales	Controles Actuales	Controles Actuales	Probabilidad de Ocurrencia Residual	Total Riesgo Residual
Información	Información correo electrónico	4	Acceso no autorizado	Acceso remoto no seguro	4	4	16	TRATAR	11.4.1 Políticas para el uso de los servicios de la red de datos	11.4.2 Autenticación de usuarios para conexiones externas	11.4.3 Identificación de equipos en la red	11.4.4 Diagnóstico remoto y protección de la configuración de puertos	11.4.5 Separación en la redes	11.4.6 Control de conexión a la red de trabajo	11.4.7 Control de enrutamiento de red	1	4
Información	Información correo electrónico	4	Acceso no autorizado	Conexiones a red pública desprotegidas	4	2	8	ACEPTABLE	10.6.1 Controles de la Red	10.6.2 Seguridad de los Servicios de Red	11.4.5 Separación en la redes	11.4.6 Control de conexión a la red de trabajo	11.4.7 Control de enrutamiento de red			1	4
Información	Información correo electrónico	4	Acceso no autorizado	Eliminación o reutilizacion de medios sin borrar	4	4	16	TRATAR	10.7.1 Gestión de medios removibles	10.7.2 Destrucción de medios						1	4
Información	Información correo electrónico	4	Acceso no autorizado	Gestión del control de acceso ineficiente	4	3	12	ACEPTABLE	11.6.1 Restricción de acceso a los sistemas de	11.6.2 Aislamiento de sistemas sensibles						1	4
Información	Información correo electrónico	4	Acceso no autorizado	No existen mecanismos de autenticación y validación del usuario	4	3	12	ACEPTABLE	11.5.1 Procedimientos para inicio de sesión de las estaciones de trabajo	11.5.2 Identificación y autenticación de los usuarios.	11.5.3 Sistema de gestión de contraseñas.	11.5.5 Tiempo de la inactividad de la sesión	11.5.6 Limitación en los periodos de tiempo de conexión a servicios y			1	4
Información	Información correo electrónico	4	Acceso no autorizado	No existen procedimientos formales de revisión de accesos	4	3	12	ACEPTABLE	10.1.4 Separación de los ambientes de Desarrollo, prueba y	11.2.4 Revisión de los permisos asignados a los usuarios						1	4
Información	Información correo electrónico	4	Acceso no autorizado	No existen procedimientos formales para alta y baja de usuarios	4	4	16	TRATAR	11.1.1 Política de Control de Acceso	11.2.1 Registro de Usuarios	11.2.2 Gestión de privilegios	11.2.3 Gestión de Contraseñas (passwords)	11.3.1 Uso de las contraseñas	11.4.2 Autenticación de usuarios para conexiones	11.5.2 Identificación y autenticación de los usuarios.	1	4
Información	Información correo electrónico	4	Acceso no autorizado	Uso medios removibles no controlado	4	5	20	TRATAR	7.1.1 Inventario de activos tecnológicos y de la información.	7.1.2 Responsables de los activos tecnológicos	7.1.3 Uso aceptable de las activos tecnológicos	10.7.1 Gestión de medios removibles	10.7.2 Destrucción de medios	10.8.3 Medios físicos en transito		1	4
Información	Información correo electrónico	4	Escuchas no autorizadas	Cableado desprotegido	4	1	4	ACEPTABLE	9.2.3 Seguridad en el cableado							1	4

Información correo electrónico	4	Escuchas no autorizadas	Comunicaciones a través de redes públicas o desprotegidas	4	1	4	ACEPTABLE	10.6.1 Controles de la Red	10.6.2 Seguridad de los Servicios de Red	10.8.4 Mensajería Electrónica	11.4.5 Separación en la redes	11.4.6 Control de conexión a la red de trabajo	11.4.7 Control de enrutamiento de red		1	4
Información correo electrónico	4	Escuchas no autorizadas	No existe protección contra código malicioso	4	3	12	ACEPTABLE	10.4.1 Controles contra código	10.4.2 Controles contra código móvil						1	4
Información correo electrónico	4	Escuchas no autorizadas	No existen procedimientos de monitorización de las instalaciones	4	4	16	TRATAR	9.1.2 Controles físicos de entrada	9.1.3 Aseguramiento de oficinas, cuartos e instalaciones	9.1.5 Trabajo en áreas restringidas / seguras	9.1.6 Acceso público, envíos y áreas de carga				1	4
Información correo electrónico	4	Manipulación de los registros	No existe control sobre el uso de utilidades de sistema	4	3	12	ACEPTABLE	15.3.1 Controles para auditoría del sistema	15.3.2 Protección de las herramientas para auditoría del						1	4
Información correo electrónico	4	Manipulación de los registros	No existen registros de auditoría	4	4	16	TRATAR	10.10.1 Registros de Auditoría	10.10.2 Monitoreo del uso del sistema	10.10.3 Protección de registros de monitoreo	10.10.4 Registros de monitoreo de administradores y operadores	10.10.5 Registro de fallas	10.10.6 Sincronía / sincronización de relojes		1	4
Información correo electrónico	4	Pérdida o corrupción de la información	No existe protección contra código malicioso	4	3	12	ACEPTABLE	10.4.1 Controles contra código	10.4.2 Controles contra código móvil	10.5.1 Respaldo de la información.					1	4
Información correo electrónico	4	Revelación de contraseñas	No existe concienciación y formación en seguridad	4	3	12	ACEPTABLE	8.2.2 Conciencia de la seguridad, educación y entrenamient							1	4
Información correo electrónico	4	Revelación de contraseñas	No existen procesos disciplinarios claros para incidentes de seguridad de la información	4	5	20	TRATAR	8.2.3 Procesos disciplinarios							1	4
Información correo electrónico	4	Revelación de contraseñas	Uso no aceptable de activos	4	4	16	TRATAR	7.1.3 Uso aceptable de las activos tecnológicos							1	4

Información	Información correo electrónico	4	Revelación de información	No existe control para copia de información	4	4	16	TRATAR	10.5.1 Respaldo de la información.	10.7.1 Gestión de medios removibles	10.7.4 Seguridad de la documentación de los sistemas intercambio de información.					1	4
Información	Información correo electrónico	4	Revelación de información	No existen procedimientos de autorización para la información pública	4	4	16	TRATAR	10.9.3 Información pública / disponible al público							1	4
Información	Información correo electrónico	4	Revelación de información	No existen procedimientos para el etiquetado y manejo de la información	4	5	20	TRATAR	7.2.1 Normas para clasificación de la información	7.2.2 Identificación y Manejo de la información						1	4
Información	Información correo electrónico	4	Robo de documentación	Control de acceso al edificio y a las salas ineficiente	4	3	12	ACEPTABLE	9.1.2 Controles físicos de entrada	9.1.3 Aseguramiento de oficinas, cuartos e	9.1.5 Trabajo en áreas restringidas / seguras	9.1.6 Acceso público, envíos y áreas de carga	9.2.1 Ubicación y protección de equipos tecnológico			1	4
Información	Información correo electrónico	4	Robo de documentación	No existen procedimientos de monitorización de las instalaciones	4	4	16	TRATAR	9.1.1 Perímetro de Seguridad Física							1	4
Información	Información correo electrónico	4	Robo de información	Eliminación o reutilizacion de soportes sin borrar	4	5	20	TRATAR	8.3.2 Devolución de activos tecnológicos	9.2.6 Eliminación, destrucción y reutilización de equipos	10.7.2 Destrucción de medios					1	4
Información	Información correo electrónico	4	Robo de información	No existe control para copia de información	4	5	20	TRATAR	10.5.1 Respaldo de la información.	10.7.1 Gestión de medios removibles	10.8.3 Medios físicos en transito	10.10.2 Monitoreo del uso del sistema	11.7.2 Teletrabajo / trabajo remoto			1	4
Servicio	Servicio de correo electrónico	4	Fallo en la provisión	No existen acuerdos de calidad de servicio (SLA)	4	3	12	ACEPTABLE	6.2.3 Aproximación a la seguridad en acuerdos	10.2.1 Prestación de servicios	10.2.2 Monitoreo y revisión de servicios de terceros	10.2.3 Gestión de cambios a servicios de terceros				1	4
Software	Software de correo electrónico	4	Elevación de privilegios	Fallos conocidos en versiones	4	5	20	TRATAR	12.5.3 Restricciones a cambios en paquetes de software	12.6.1 Control técnico de vulnerabilidades						1	4

Software	Software de correo electrónico	4	Elevación de privilegios	Gestión de actualizaciones de seguridad ineficiente	4	4	16	TRATAR	12.4.1 Control del software operacional(operativo)	12.5.1 Procedimientos para el control de cambios	12.5.2 Revisión técnica de aplicaciones después de cambios al sistema					1	4
Software	Software de correo electrónico	4	Elevación de privilegios	Gestión ineficiente de contraseñas	4	3	12	ACEPTABLE	11.2.3 Gestión de Contraseñas (passwords)	11.2.4 Revisión de los permisos asignados a los usuarios						1	4
Software	Software de correo electrónico	4	Elevación de privilegios	No existen registros de auditoría	4	3	12	ACEPTABLE	10.10.1 Registros de Auditoría	10.10.2 Monitoreo del uso del sistema	10.10.3 Protección de registros de monitoreo	10.10.4 Registros de monitoreo de administradores y operadores				1	4
Software	Software de correo electrónico	4	Fallo de sistemas	Configuración de parámetros errónea	4	4	16	TRATAR	12.2.1 Validación de los datos de entrada	12.2.2 Control del procesamiento interno	12.2.3 Integridad de los mensajes	12.2.4 Validación de los datos de salida				1	4
Software	Software de correo electrónico	4	Fallo de sistemas	Especificaciones para desarrolladores incompletas o confusas	4	3	12	ACEPTABLE	12.1.1 Análisis y especificaciones de los requerimientos de seguridad	12.5.5 Desarrollo de software por parte de Outsourcing / contratado externament						1	4
Software	Software de correo electrónico	4	Fallo de sistemas	Fallos conocidos en versiones	4	5	20	TRATAR	10.8.5 Sistemas de información de la entidad	12.5.2 Revisión técnica de aplicaciones después de cambios al sistema	12.6.1 Control técnico de vulnerabilidades					1	4
Software	Software de correo electrónico	4	Fallo de sistemas	Gestión de actualizaciones de seguridad ineficiente	4	4	16	TRATAR	10.3.2 Aceptación de sistemas	12.4.1 Control del software operacional(operativo)	12.5.1 Procedimientos para el control de cambios	12.5.3 Restricciones a cambios en paquetes de software				1	4
Software	Software de correo electrónico	4	Fallo de sistemas	No existen registros de auditoría	4	3	12	ACEPTABLE	12.4.3 Control de acceso a las librerías de	12.5.4 Fuga de información						1	4
Software	Software de correo electrónico	4	Fallo de sistemas	Pruebas de software insuficientes	4	3	12	ACEPTABLE	12.4.2 Protección de los datos en sistemas de prueba							1	4

Software	Software de correo electrónico	4	Incumplimiento legal, reglamentario o contractual	Violación de la legislación aplicable	4	4	16	TRATAR	12.3.1 Política para el uso de controles criptográfico							1	4
Software	Software de correo electrónico	4	Uso de sistemas por usuarios no autorizados	Acceso remoto no seguro	4	4	16	TRATAR	12.3.1 Política para el uso de controles criptográfico	12.3.2 Gestión de llaves						1	4
Software	Software de correo electrónico	4	Uso de sistemas por usuarios no autorizados	Asignación errónea de derechos de acceso	4	2	8	ACEPTABLE	11.5.4 Uso de las utilidades del sistema							1	4
Fisico	Servidor database correo electronico VM1:JANUS.accionsocial.col, VM2:JANUS.accionsocial.col Host1:mercurio.accionsocial.col Host2:vmerc	4	Acceso a soportes no autorizado	Instalación desprotegida	4	3	12	ACEPTABLE	9.1.3 Aseguramiento de oficinas, cuartos e instalaciones	9.1.5 Trabajo en áreas restringidas / seguras	9.1.6 Acceso público, envíos y áreas de carga	9.2.1 Ubicación y protección de equipos tecnológicos	9.2.3 Seguridad en el cableado			1	4
Fisico	Servidor database correo electronico VM1:JANUS.accionsocial.col, VM2:JANUS.accionsocial.col Host1:mercurio.accionsocial.col Host2:vmerc	4	Acceso a soportes no autorizado	Uso incorrecto de software	4	3	12	ACEPTABLE	10.3.2 Aceptación de sistemas	11.5.4 Uso de las utilidades del sistema						1	4
Fisico	Servidor database correo electronico VM1:JANUS.accionsocial.col, VM2:JANUS.accionsocial.col Host1:mercurio.accionsocial.col Host2:vmerc	4	Acceso a soportes no autorizado	Uso no aceptable de activos	4	3	12	ACEPTABLE	7.1.3 Uso aceptable de las activos tecnológicos	8.2.2 Conciencia de la seguridad, educación y entrenamiento	8.2.3 Procesos disciplinarios					1	4

Fisico	Servidor database correo electronico VM1:JANUS.accionsocial.col, VM2:JANUS.accionsocial.col Host1:mercurio.accionsocial.col Host2:vmerc	4	Daño por agua	Susceptibilidad a polvo, humedad.	4	4	16	TRATAR	9.1.3 Aseguramiento de oficinas, cuartos e instalaciones	9.1.4 Protección contra amenazas externas y ambientales	9.2.1 Ubicación y protección de equipos tecnológicos	9.2.3 Seguridad en el cableado				1	4
Fisico	Servidor database correo electronico VM1:JANUS.accionsocial.col, VM2:JANUS.accionsocial.col Host1:mercurio.accionsocial.col Host2:vmerc	4	Daño por terceras partes	Gestión inadecuada de terceras partes	4	3	12	ACEPTABLE	6.2.1 Identificación de riesgos	6.2.2 Aproximación a la seguridad al tratar con clientes	6.2.3 Aproximación a la seguridad en acuerdos con terceros						1	4
Fisico	Servidor database correo electronico VM1:JANUS.accionsocial.col, VM2:JANUS.accionsocial.col Host1:mercurio.accionsocial.col Host2:vmerc	4	Daño por terceras partes	No existe concientización y formación en seguridad	4	3	12	ACEPTABLE	8.2.2 Conciencia de la seguridad, educación y entrenamiento								1	4
Fisico	Servidor database correo electronico VM1:JANUS.accionsocial.col, VM2:JANUS.accionsocial.col Host1:mercurio.accionsoc	4	Daño por terceras partes	No existe supervisión de terceros dentro de la organización	4	2	8	ACEPTABLE	9.1.3 Aseguramiento de oficinas, cuartos e instalaciones								1	4

Fisico	Servidor database correo electronico VM1:JANUS.accionsocial.col, VM2:JANUS.accionsocial.col Host1:mercurio.accionsocial.col Host2:vmerc	4	Daño por terceras partes	Proceso de contratación ineficiente	4	2	8	ACEPTABLE	8.1.1 Roles y responsabilidades	8.1.2 Investigación del personal que va a ser contratado	8.1.3 Términos y condiciones laborales	10.2.3 Gestión de cambios a servicios de terceros				1	4
Fisico	Servidor database correo electronico VM1:JANUS.accionsocial.col, VM2:JANUS.accionsocial.col Host1:mercurio.accionsocial.col Host2:vmerc	4	Destrucción	Exposición a temperaturas extremas	4	4	16	TRATAR	9.1.4 Protección contra amenazas externas y ambientales							1	4
Fisico	Servidor database correo electronico VM1:JANUS.accionsocial.col, VM2:JANUS.accionsocial.col Host1:mercurio.accionsocial.col Host2:vmerc	4	Destrucción	No existe sistema estabilizador de tensión	4	2	8	ACEPTABLE	9.2.2 Seguridad en el suministro de electricidad y servicios (utilities)							1	4
Fisico	Servidor database correo electronico VM1:JANUS.accionsocial.col, VM2:JANUS.accionsocial.col Host1:mercurio.accionsoc	4	Destrucción	Uso incorrecto de equipos	4	2	8	ACEPTABLE	8.2.2 Conciencia de la seguridad, educación y entrenamiento	9.2.5 Seguridad de equipos fuera de las áreas seguras						1	4

Fisico	Servidor database correo electronico VM1:JANUS.accionsocial.col, VM2:JANUS.accionsocial.col Host1:mercurio.accionsocial.col Host2:vmerc	4	Deterioro de los soportes equipos	Mantenimiento insuficiente	4	5	20	TRATAR	9.2.4 Mantenimiento de los equipos							1	4
Fisico	Servidor database correo electronico VM1:JANUS.accionsocial.col, VM2:JANUS.accionsocial.col Host1:mercurio.accionsocial.col Host2:vmerc	4	Falta de mantenimiento de equipos	Gestión de cambios ineficiente	4	4	16	TRATAR	10.1.2 Contro de cambios	10.3.2 Aceptación de sistemas						1	4
Fisico	Servidor database correo electronico VM1:JANUS.accionsocial.col, VM2:JANUS.accionsocial.col Host1:mercurio.accionsocial.col Host2:vmerc	4	Falta de mantenimiento de equipos	Mantenimiento insuficiente	4	4	16	TRATAR	9.2.4 Mantenimiento de los equipos							1	4
Fisico	Servidor database correo electronico VM1:JANUS.accionsocial.col, VM2:JANUS.accionsocial.col Host1:mercurio.accionsoc	4	Falta de mantenimiento de equipos	No existe gestión de activos	4	2	8	ACEPTABLE	7.1.1 Inventario de activos tecnológicos y de la información.	7.1.2 Responsables de los activos tecnológicos	7.1.3 Uso aceptable de las activos tecnológicos					1	4

Fisico	Servidor database correo electronico VM1:JANUS.accionsocial.col, VM2:JANUS.accionsocial.col Host1:mercurio.accionsocial.col Host2:vmerc	4	Falta de mantenimiento de equipos	Planificación y monitorización de capacidad inadecuada	4	4	16	TRATAR	10.3.1 Gestión de la capacidad							1	4
Fisico	Servidor database correo electronico VM1:JANUS.accionsocial.col, VM2:JANUS.accionsocial.col Host1:mercurio.accionsocial.col Host2:vmerc	4	Fuego	No existen equipos de detección de incendios	4	3	12	ACEPTABLE	9.1.3 Aseguramiento de oficinas, cuartos e instalaciones							1	4
Fisico	Servidor database correo electronico VM1:JANUS.accionsocial.col, VM2:JANUS.accionsocial.col Host1:mercurio.accionsocial.col Host2:vmerc	4	Fuego	No existen equipos de extinción de incendios	4	3	12	ACEPTABLE	9.1.4 Protección contra amenazas externas y ambientales							1	4
Fisico	Servidor database correo electronico VM1:JANUS.accionsocial.col, VM2:JANUS.accionsocial.col Host1:mercurio.accionsoc	4	Inundación	Ubicaciones suceptibles a inundación	4	1	4	ACEPTABLE	9.1.3 Aseguramiento de oficinas, cuartos e instalaciones	9.1.4 Protección contra amenazas externas y ambientales	9.2.1 Ubicación y protección de equipos tecnológicos					1	4

Fisico	Servidor database correo electronico VM1:JANUS.accionsocial.col, VM2:JANUS.accionsocial.col Host1:mercurio.accionsocial.col Host2:vmerc	4	Inundación	Ubicaciones suceptibles a inundación	4	1	4	ACEPTABLE	9.1.3 Aseguramiento de oficinas, cuartos e instalaciones	9.1.4 Protección contra amenazas externas y ambientales	9.2.1 Ubicación y protección de equipos tecnológicos					1	4
Fisico	Servidor database correo electronico VM1:JANUS.accionsocial.col, VM2:JANUS.accionsocial.col Host1:mercurio.accionsocial.col Host2:vmerc	4	Manipulación de los equipos	No existe control de los activos fuera de las instalaciones	4	1	4	ACEPTABLE	9.2.5 Seguridad de equipos fuera de las áreas seguras	9.2.7 Extracción de activos informáticos						1	4
Fisico	Servidor database correo electronico VM1:JANUS.accionsocial.col, VM2:JANUS.accionsocial.col Host1:mercurio.accionsocial.col Host2:vmerc	4	Manipulación de los equipos	No existe gestión de activos	4	1	4	ACEPTABLE	7.1.1 Inventario de activos tecnológicos y de la información.	7.1.2 Responsables de los activos tecnológicos						1	4
Fisico	Servidor database correo electronico VM1:JANUS.accionsocial.col, VM2:JANUS.accionsocial.col Host1:mercurio.accionsoc	4	Manipulación de los equipos	No existe procedimiento para el control de cambios	4	4	16	TRATAR	10.1.2 Contro de cambios							1	4

Fisico	Servidor database correo electronico VM1:JANUS.accionsocial.col, VM2:JANUS.accionsocial.col Host1:mercurio.accionsocial.col Host2:vmerc	4	Manipulación de los equipos	No existen políticas para el uso de dispositivos portátiles	4	1	4	ACEPTABLE	11.7.1 Computación Móvil y comunicaciones							1	4
Fisico	Servidor database correo electronico VM1:JANUS.accionsocial.col, VM2:JANUS.accionsocial.col Host1:mercurio.accionsocial.col Host2:vmerc	4	Manipulación de los equipos	Uso no aceptable de activos	4	4	16	TRATAR	7.1.3 Uso aceptable de las activos tecnológicos							1	4
Fisico	Servidor database correo electronico VM1:JANUS.accionsocial.col, VM2:JANUS.accionsocial.col Host1:mercurio.accionsocial.col Host2:vmerc	4	Polvo, humedad, corrosión	Exposición a humedad, polvo, suciedad	4	4	16	TRATAR	9.1.4 Protección contra amenazas externas y ambientales	9.2.1 Ubicación y protección de equipos tecnológicos	9.2.4 Mantenimiento de los equipos					1	4
Fisico	Servidor database correo electronico VM1:JANUS.accionsocial.col, VM2:JANUS.accionsocial.col Host1:mercurio.accionsocial.col Host2:vmerc	4	Recuperación de medios reciclados o descartados	No existe gestión de activos	4	1	4	ACEPTABLE	7.1.1 Inventario de activos tecnológicos y de la información.	7.1.2 Responsables de los activos tecnológicos	7.1.3 Uso aceptable de las activos tecnológicos					1	4
Fisico	Servidor database correo electronico VM1:JANUS.accionsocial.col, VM2:JANUS.accionsocial.col Host1:mercurio.accionsoc	4	Recuperación de medios reciclados o descartados	No existe gestión de activos	4	1	4	ACEPTABLE	7.1.1 Inventario de activos tecnológicos y de la información.	7.1.2 Responsables de los activos tecnológicos	7.1.3 Uso aceptable de las activos tecnológicos					1	4

Fisico	Servidor database correo electronico VM1:JANUS.accionsocial.col, VM2:JANUS.accionsocial.col Host1:mercurio.accionsocial.col Host2:vmerc	4	Recuperación de medios reciclados o descartados	No existen procedimiento para devolución de activos	4	4	16	TRATAR	8.3.2 Devolución de activos tecnológicos	10.7.2 Destrucción de medios						1	4
Fisico	Servidor database correo electronico VM1:JANUS.accionsocial.col, VM2:JANUS.accionsocial.col Host1:mercurio.accionsocial.col Host2:vmerc	4	Robo de equipos	Instalación desprotegida	4	3	12	ACEPTABLE	9.1.6 Acceso público, envíos y áreas de carga	9.2.1 Ubicación y protección de equipos tecnológicos						1	4
Fisico	Servidor database correo electronico VM1:JANUS.accionsocial.col, VM2:JANUS.accionsocial.col Host1:mercurio.accionsocial.col Host2:vmerc	4	Robo de equipos	No existe de protección en puertas y ventanas	4	3	12	ACEPTABLE	9.1.1 Perímetro de Seguridad Física	9.1.2 Controles físicos de entrada	9.1.3 Aseguramiento de oficinas, cuartos e instalaciones					1	4
Fisico	Servidor database correo electronico VM1:JANUS.accionsocial.col, VM2:JANUS.accionsocial.col Host1:mercurio.accionsoc	4	Robo de equipos	No existe gestión de activos	4	2	8	ACEPTABLE	7.1.1 Inventario de activos tecnológicos y de la información.	7.1.2 Responsables de los activos tecnológicos						1	4

Fisico	Servidor database correo electronico VM1:JANUS.accionsocial.col, VM2:JANUS.accionsocial.col Host1:mercurio.accionsocial.col Host2:vmerc	4	Robo de equipos	No existen políticas para el uso de dispositivos portátiles	4	1	4	ACEPTABLE	9.2.5 Seguridad de equipos fuera de las áreas seguras	9.2.7 Extracción de activos informáticos						1	4
Fisico	Servidor database correo electronico VM1:JANUS.accionsocial.col, VM2:JANUS.accionsocial.col Host1:mercurio.accionsocial.col Host2:vmerc	4	Robo de equipos	No existen procedimiento para devolución de activos	4	1	4	ACEPTABLE	8.3.2 Devolución de activos							1	4
Fisico	Servidor correo electronico unified management VMtarvos.accionsocial.col Host: vyemir.accionsocial.col	4	Acceso a soportes no autorizado	Instalación desprotegida	4	3	12	ACEPTABLE	9.1.3 Aseguramiento de oficinas, cuartos e instalaciones	9.1.5 Trabajo en áreas restringidas / seguras	9.1.6 Acceso público, envíos y áreas de carga	9.2.1 Ubicación y protección de equipos tecnológicos	9.2.3 Seguridad en el cableado			1	4
Fisico	Servidor correo electronico unified management VMtarvos.accionsocial.col Host: vyemir.accionsocial.col	4	Acceso a soportes no autorizado	Uso incorrecto de software	4	3	12	ACEPTABLE	10.3.2 Aceptación de sistemas	11.5.4 Uso de las utilidades del sistema						1	4

Fisico	Servidor correo electronico unified management VMtarvos.accionsocial.col Host: vyemir.accionsocial.col	4	Acceso a soportes no autorizado	Uso no aceptable de activos	4	3	12	ACEPTABLE	7.1.3 Uso aceptable de las activos tecnológicos	8.2.2 Conciencia de la seguridad, educación y entrenamiento	8.2.3 Procesos disciplinarios					1	4
Fisico	Servidor correo electronico unified management VMtarvos.accionsocial.col Host: vyemir.accionsocial.col	4	Daño por agua	Susceptibilidad a polvo, humedad.	4	4	16	TRATAR	9.1.3 Aseguramiento de oficinas, cuartos e instalaciones	9.1.4 Protección contra amenazas externas y ambientales	9.2.1 Ubicación y protección de equipos tecnológicos	9.2.3 Seguridad en el cableado				1	4
Fisico	Servidor correo electronico unified management VMtarvos.accionsocial.col Host: vyemir.accionsocial.col	4	Daño por terceras partes	Gestión inadecuada de terceras partes	4	3	12	ACEPTABLE	6.2.1 Identificación de riesgos	6.2.2 Aproximación a la seguridad al tratar con clientes	6.2.3 Aproximación a la seguridad en acuerdos con terceros					1	4
Fisico	Servidor correo electronico unified management VMtarvos.accionsocial.col Host: vyemir.accionsocial.col	4	Daño por terceras partes	No existe concientización y formación en seguridad	4	3	12	ACEPTABLE	8.2.2 Conciencia de la seguridad, educación y entrenamiento							1	4
Fisico	Servidor correo electronico unified management VMtarvos.accionsocial.col Host: vyemir.accionsocial.col	4	Daño por terceras partes	No existe supervisión de terceros dentro de la organización	4	2	8	ACEPTABLE	9.1.3 Aseguramiento de oficinas, cuartos e instalaciones							1	4

Fisico	Servidor correo electronico unified management VMtarvos.accionsocial.col Host: vyemir.accionsocial.col	4	Daño por terceras partes	Proceso de contratación ineficiente	4	2	8	ACEPTABLE	8.1.1 Roles y responsabilidades	8.1.2 Investigación del personal que va a ser contratado	8.1.3 Términos y condiciones laborales	10.2.3 Gestión de cambios a servicios de terceros				1	4
Fisico	Servidor correo electronico unified management VMtarvos.accionsocial.col Host: vyemir.accionsocial.col	4	Destrucción	Exposición a temperaturas extremas	4	4	16	TRATAR	9.1.4 Protección contra amenazas externas y ambientales							1	4
Fisico	Servidor correo electronico unified management VMtarvos.accionsocial.col Host: vyemir.accionsocial.col	4	Destrucción	No existe sistema estabilizador de tensión	4	2	8	ACEPTABLE	9.2.2 Seguridad en el suministro de electricidad y servicios (utilities)							1	4
Fisico	Servidor correo electronico unified management VMtarvos.accionsocial.col Host: vyemir.accionsocial.col	4	Destrucción	Uso incorrecto de equipos	4	2	8	ACEPTABLE	8.2.2 Conciencia de la seguridad, educación y entrenamiento	9.2.5 Seguridad de equipos fuera de las áreas seguras						1	4
Fisico	Servidor correo electronico unified management VMtarvos.accionsocial.col Host: vyemir.accionsocial.col	4	Deterioro de los soportes equipos	Mantenimiento insuficiente	4	5	20	TRATAR	9.2.4 Mantenimiento de los equipos							1	4

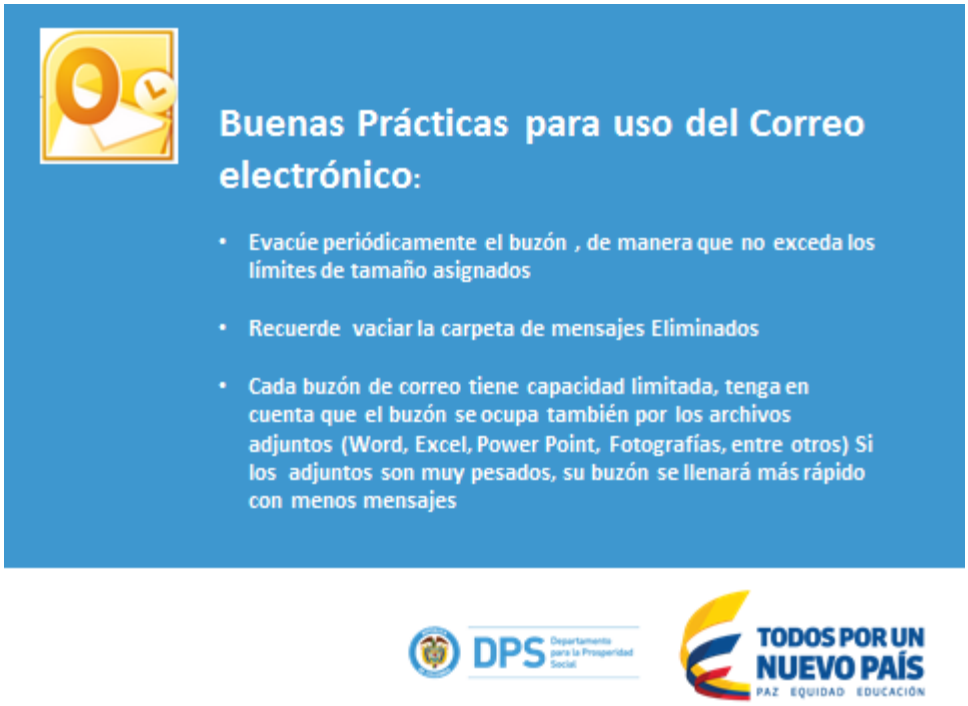
Fisico	Servidor correo electronico unified management VMtarvos.accionsocial.col Host: vyemir.accionsocial.col	4	Falta de mantenimiento de equipos	Gestión de cambios ineficiente	4	4	16	TRATAR	10.1.2 Contro de cambios	10.3.2 Aceptación de sistemas						1	4
Fisico	Servidor correo electronico unified management VMtarvos.accionsocial.col Host: vyemir.accionsocial.col	4	Falta de mantenimiento de equipos	Mantenimiento insuficiente	4	4	16	TRATAR	9.2.4 Mantenimiento de los equipos							1	4
Fisico	Servidor correo electronico unified management VMtarvos.accionsocial.col Host: vyemir.accionsocial.col	4	Falta de mantenimiento de equipos	No existe gestión de activos	4	2	8	ACEPTABLE	7.1.1 Inventario de activos tecnológicos y de la información.	7.1.2 Responsables de los activos tecnológicos	7.1.3 Uso aceptable de las activos tecnológicos					1	4
Fisico	Servidor correo electronico unified management VMtarvos.accionsocial.col Host: vyemir.accionsocial.col	4	Falta de mantenimiento de equipos	Planificación y monitorización de capacidad inadecuada	4	4	16	TRATAR	10.3.1 Gestión de la capacidad							1	4
Fisico	Servidor correo electronico unified management VMtarvos.accionsocial.col Host: vyemir.accionsocial.col	4	Fuego	No existen equipos de detección de incendios	4	3	12	ACEPTABLE	9.1.3 Aseguramiento de oficinas, cuartos e instalaciones							1	4

Fisico	Servidor correo electronico unified management VMtarvos.accionsocial.col Host: vyemir.accionsocial.col	4	Fuego	No existen equipos de extinción de incendios	4	3	12	ACEPTABLE	9.1.4 Protección contra amenazas externas y ambientales							1	4
Fisico	Servidor correo electronico unified management VMtarvos.accionsocial.col Host: vyemir.accionsocial.col	4	Inundación	Ubicaciones suceptibles a inundación	4	1	4	ACEPTABLE	9.1.3 Aseguramiento de oficinas, cuartos e instalaciones	9.1.4 Protección contra amenazas externas y ambientales	9.2.1 Ubicación y protección de equipos tecnológicos					1	4
Fisico	Servidor correo electronico unified management VMtarvos.accionsocial.col Host: vyemir.accionsocial.col	4	Manipulación de los equipos	No existe control de los activos fuera de las instalaciones	4	1	4	ACEPTABLE	9.2.5 Seguridad de equipos fuera de las áreas seguras	9.2.7 Extracción de activos informáticos						1	4
Fisico	Servidor correo electronico unified management VMtarvos.accionsocial.col Host: vyemir.accionsocial.col	4	Manipulación de los equipos	No existe gestión de activos	4	1	4	ACEPTABLE	7.1.1 Inventario de activos tecnológicos y de la información.	7.1.2 Responsables de los activos tecnológicos						1	4
Fisico	Servidor correo electronico unified management VMtarvos.accionsocial.col Host: vyemir.accionsocial.col	4	Manipulación de los equipos	No existe procedimiento para el control de cambios	4	4	16	TRATAR	10.1.2 Contro de cambios							1	4

Fisico	Servidor correo electronico unified management VMtarvos.accionsocial.col Host: vyemir.accionsocial.col	4	Manipulación de los equipos	No existen políticas para el uso de dispositivos portátiles	4	1	4	ACEPTABLE	11.7.1 Computación Móvil y comunicaciones							1	4
Fisico	Servidor correo electronico unified management VMtarvos.accionsocial.col Host: vyemir.accionsocial.col	4	Manipulación de los equipos	Uso no aceptable de activos	4	4	16	TRATAR	7.1.3 Uso aceptable de las activos tecnológicos							1	4
Fisico	Servidor correo electronico unified management VMtarvos.accionsocial.col Host: vyemir.accionsocial.col	4	Polvo, humedad, corrosión	Exposición a humedad, polvo, suciedad	4	4	16	TRATAR	9.1.4 Protección contra amenazas externas y ambientales	9.2.1 Ubicación y protección de equipos tecnológicos	9.2.4 Mantenimiento de los equipos					1	4
Fisico	Servidor correo electronico unified management VMtarvos.accionsocial.col Host: vyemir.accionsocial.col	4	Recuperación de medios reciclados o descartados	No existe gestión de activos	4	1	4	ACEPTABLE	7.1.1 Inventario de activos tecnológicos y de la información.	7.1.2 Responsables de los activos tecnológicos	7.1.3 Uso aceptable de las activos tecnológicos					1	4
Fisico	Servidor correo electronico unified management VMtarvos.accionsocial.col Host: vyemir.accionsocial.col	4	Recuperación de medios reciclados o descartados	No existen procedimiento para devolución de activos	4	4	16	TRATAR	8.3.2 Devolución de activos tecnológicos	10.7.2 Destrucción de medios						1	4

Fisico	Servidor correo electronico unified management VMtarvos.accionsocial.col Host: vyemir.accionsocial.col	4	Robo de equipos	Instalación desprotegida	4	3	12	ACEPTABLE	9.1.6 Acceso público, envíos y áreas de carga	9.2.1 Ubicación y protección de equipos tecnológicos						1	4
Fisico	Servidor correo electronico unified management VMtarvos.accionsocial.col Host: vyemir.accionsocial.col	4	Robo de equipos	No existe de protección en puertas y ventanas	4	3	12	ACEPTABLE	9.1.1 Perímetro de Seguridad Física	9.1.2 Controles físicos de entrada	9.1.3 Aseguramiento de oficinas, cuartos e instalaciones					1	4
Fisico	Servidor correo electronico unified management VMtarvos.accionsocial.col Host: vyemir.accionsocial.col	4	Robo de equipos	No existe gestión de activos	4	2	8	ACEPTABLE	7.1.1 Inventario de activos tecnológicos y de la información.	7.1.2 Responsables de los activos tecnológicos						1	4
Fisico	Servidor correo electronico unified management VMtarvos.accionsocial.col Host: vyemir.accionsocial.col	4	Robo de equipos	No existen políticas para el uso de dispositivos portátiles	4	1	4	ACEPTABLE	9.2.5 Seguridad de equipos fuera de las áreas seguras	9.2.7 Extracción de activos informáticos						1	4
Fisico	Servidor correo electronico unified management VMtarvos.accionsocial.col Host: vyemir.accionsocial.col	4	Robo de equipos	No existen procedimiento para devolución de activos	4	1	4	ACEPTABLE	8.3.2 Devolución de activos							1	4

Anexo E. Campaña de Concientización



Anexo F. Formato de Aceptación de Condiciones para la Instalación de correo electrónico en dispositivos Móviles

DPS Departamento para la Prosperidad Social	**Formato de Aceptación de Condiciones para la Instalación de Correo Electrónico en Dispositivos Móviles**	Código:
		Fecha aprobación:
	GRUPO DE INFRAESTRUCTURA Y SOPORTE DE TI	Versión: 01

Yo, _____, identificado(a) con la Cédula de Ciudadanía No._____ de_____, mediante el presente documento acepto las siguientes condiciones para la instalación del correo electrónico corporativo en el dispositivo móvil que se encuentra bajo mi custodia:

- En caso de pérdida o robo del dispositivo móvil que contenga información del DPS, incluida la información del correo electrónico, debo avisar inmediatamente al GT de Infraestructura y Soporte de TI.
- En caso de pérdida o robo del dispositivo móvil que contenga información del DPS, el GT de Infraestructura y Soporte de TI tiene autonomía para iniciar un proceso de borrado remoto de toda la información contenida en el dispositivo móvil.
- El dispositivo móvil debe poseer un sistema de autenticación, basado al menos en un patrón de movimiento, un código de desbloqueo o una contraseña.
- El dispositivo móvil debe tener un software de antivirus.
- Los dispositivos móviles que son propiedad del DPS pueden estar sometidos a un control sobre el tipo y la versión de aplicaciones instaladas, al igual que pueden estar sometidos a restricciones de conexión hacia ciertos servicios de información que sean considerados maliciosos. Igualmente, estos dispositivos deben cumplir con las medidas de aseguramiento definidas por el GT de Infraestructura y Soporte de TI para garantizar la preservación de la confidencialidad e integridad de la información del DPS.
- Los dispositivos móviles que son propiedad de los funcionarios, pueden tener almacenada información de correo electrónico corporativo, siempre y cuando dichos equipos se encuentren registrados, identificados e implementen las medidas de aseguramiento definidas por el GT de Infraestructura y Soporte de TI para garantizar la preservación de la confidencialidad e integridad de la información del DPS.

Nombre del usuario:	
CC. No.	
Dependencia:	
Cargo que desempeña:	
Fecha de retiro o terminación de contrato (para contratistas):	día/mes/año
Nombre Jefe inmediato o Supervisor de Contrato	
Municipio:	
Departamento:	
Teléfono de Contacto:	
Email:	

Firma Usuario: _____