DESARROLLO DE UNA METODOLOGÍA DE SEGURIDAD PARA EL SERVICIO DE CORREO ELECTRÓNICO CORPORATIVO EN LOS DISPOSITIVOS MÓVILES BLACKBERRY DE LA EMPRESA CHEVYPLAN COLOMBIA

CAMILO ANDRÉS ÁLVAREZ
EDISON JAVIER VALENCIA GUERRERO

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2014

DESARROLLO DE UNA METODOLOGÍA DE SEGURIDAD PARA EL SERVICIO DE CORREO ELECTRÓNICO CORPORATIVO EN LOS DISPOSITIVOS MÓVILES BLACKBERRY DE LA EMPRESA CHEVYPLAN COLOMBIA

CAMILO ANDRÉS ÁLVAREZ
EDISON JAVIER VALENCIA GUERRERO

Tesis para optar al título de
Especialista en Seguridad Informática

Asesora
JENNY ALEJANDRA VARELA SEGURA
Docente

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2014

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Bogotá D.C., Marzo de 2014

Dedicamos este trabajo a nuestras familias con inmensa gratitud y cariño, por su paciencia y quienes estuvieron apoyándonos día a día.

AGRADECIMIENTOS

Nuestros agradecimientos a nuestra Asesora del Trabajo de Grado JENNY ALEJANDRA VARELA SEGURA, por su guía y acompañamiento en este proceso,

A todos los docentes por las enseñanzas que nos brindaron que nos permitieron un aprendizaje integral como personas y profesionales.

A la Universidad Piloto de Colombia por abrirnos sus puertas y permitirnos ser parte de su historia.

A todos nuestros compañeros de Especialización, con los cuales compartimos deseos, esperanzas y metas.

CONTENIDO

LISTA DE CUADROS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

BLACKBERRY ENTERPRISE SERVER EXPRESS: sincroniza en forma inalámbrica los smartphones BlackBerry con Microsoft Exchange o IBM Lotus Domino. BlackBerry Enterprise Server Express le ofrece las funciones empresariales avanzadas que distinguen a los smartphones BlackBerry sin costos de licencias de software ni licencias de usuario adicionales. Además ofrece protección remota de dispositivos.

- Borrado de datos o bloqueo de smartphones BlackBerry perdidos o robados.
- Prevención de acceso no autorizado a la información corporativa (uso de contraseñas para desbloquear los dispositivos).
- Implementación de configuraciones de seguridad (como bloqueo de Bluetooth®) en forma inalámbrica.
- Más de 75 políticas de TI para controlar la implementación de smartphones BlackBerry.
- Métodos de encriptación Advanced Encryption Standard (AES) y Triple Data Encryption Standard (Triple DES) y compatibilidad con S/MIME[1].

CHEVYPLAN COLOMBIA. ChevyPlan® S.A. Sociedad Administradora de Planes de Autofinanciamiento Comercial en adelante ChevyPlan®, es una empresa de General Motors Colmotores y la red de concesionarios Chevrolet de todo el país, está vigilada por la Superintendencia de Sociedades. En 18 años de operación con ChevyPlan®, más de 66.000 familias colombianas han estrenado un Chevrolet cero kilómetros a un costo muy bajo y al mes de octubre de 2013, el 13% de las ventas de la marca se hacen por este exitoso sistema.

ChevyPlan® es una marca multinacional con cobertura regional y representa el Sistema de Autofinanciamiento Comercial en Colombia, Venezuela y Ecuador.

La marca registrada CHEVYPLAN® pertenece a General Motors Corporation, usado bajo la licencia a Megaplan S.A[2]

---

[1] http://mx.blackberry.com/business/software/besx.html

[2] CHEVYPLAN. ¿Qué es cheviplan. [Consultado 11 de Diciembre de 2013]. Disponible en Internet:< ehttps://www.chevyplan.com.co/Chevyplan/Chevyplan/paginas/documento.aspx?idr=1483

CONSOLA EXCHANGE: la Consola de administración de (EMC) Exchange es una herramienta basada en Microsoft Management Console (MMC) 3.0 de Microsoft que proporciona a los administradores de Exchange una interfaz gráfica de usuario (GUI) para administrar la configuración de las organizaciones de Exchange. También puede agregar el complemento de la EMC para personalizar herramientas basadas en MMC[3].

CORREO ELECTRÓNICO CORPORATIVO: es una cuenta en Microsoft Exchange Server. Exchange Server es un servidor de comunicación basado en el correo de colaboración empresarial[4].

DISPOSITIVOS MÓVILES. son todos los dispositivos que se conectan a la red a través de una lista de bloqueados/admitidos. Esta lista garantiza que sólo los dispositivos aprobados se conecten a los datos de mensajería mientras se continúa ofreciendo un amplio abanico de dispositivos habilitados con Exchange ActiveSync[5].

FUGA DE INFORMACIÓN: es el incidente que permite que una persona ajena a la empresa obtenga información confidencial que solo debe estar disponible para el personal de que labora en ella.

INFORMACIÓN CONFIDENCIAL: es toda la información secreta y privada de una organización a la cual solo debe tener acceso personal autorizado.

INTEGRIDAD: propiedad de salvaguardar la exactitud y estado completo de los activos[6].

LEY 1581 PROTECCIÓN DE DATOS: la presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se

---

[3] EXCHANGE**.** Consola de administración de Exchange. **2010.** [Consultado 11 de Diciembre de2013]. Disponible en Internet:< http://technet.microsoft.com/es-es/library/bb123762(v=exchg.141).aspx

[4] OFFICE COM. ¿Qué es una cuenta de correo electrónico de Exchange Server? ". [Consultado 11 de Diciembre de 2013]. Disponible en Internet:< http://office.microsoft.com/es-es/outlook-help/que-es-una-cuenta-de-correo-electronico-de-exchange-server-HA001095504.aspx

[5] MICROSOFT .EXCHANGE. Dispositivos móviles. [Consultado 11 de Diciembre de 2013]. Disponible en Internet:< http://www.microsoft.com/exchange/2010/es/xl/mobile-devices.aspx

[6] INSTITUTO COLOMBIANA DE NORMAS TÉCNICAS. Norma Técnica Colombiana NTC-ISO/IEC 27001.para la Tecnología de la información, técnicas de seguridad, sistemas de gestión de la seguridad de la información (SGSI), requisitos. Bogotá D.C., ICONTEC, 2006. p. 2

refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma[7].

METODOLOGÍA: es el método o plan de investigación que permite cumplir con unos objetivos en el marco de un proyecto.

POLÍTICAS DE SEGURIDAD: es una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos. Estos permiten a la compañía desarrollarse y mantenerse en su sector de negocios[8].

SMARTPHONE: teléfono inteligente que permite el procesamiento de datos y conectividad

S.O BLACKBERRY: sistema desa o por RIM para los dispositivos BlackBerry[9]

TABLET: dispositivo que funciona como computador portátil.[10]

TÉCNICOS: grupo de ingenieros enfocados en el área de telecomunicaciones y seguridad de la información.

---

[7] CONGRESO DE COLOMBIA. Ley Estatutaria 1581 de 2012 (Octubre 17). Por la cual se dictan disposiciones generales para la protección de datos personales. Bogotá D.C**.:** Diario Oficial 48587 de octubre 18 de 2012.

[8] SEGURIDAD DE LA INFORMACIÓN. Políticas de seguridad. Consultado 11 de Diciembre de 2013]. Disponible en Internet>: http://www.segu-info.cor icas/

[9] http://es.blackberry.com/software.html

[10] REAL ACADEMIA DE LA LENGUA ESPAÑOLA. Tablet. Definición. Consultado 11 de Diciembre de 2013]. Disponible en Internet:< http://lema.rae.es/drae/>

RESUMEN

Se desarrolló una metodología de seguridad para el servicio de correo electrónico corporativo en los dispositivos móviles BlackBerry de la empresa *ChevyPlan Colombia*. Este proyecto surge de la necesidad de establecer procesos y medidas de seguridad para reducir la posibilidad de pérdida o fuga de información. El diseño de la metodología se efectuó en tres etapas. La primera fue la explorativa, donde se realizó una encuesta para determinar el fin del uso del dispositivo móvil, posteriormente una etapa descriptiva en la cual se creó un documento de condiciones y responsabilidades al igual que un registro de las políticas implícitas del Software BlackBerry Enterprise Server Express. Por último una fase de finalización en la que se efectuó un estudio para determinar el impacto que tendría la implementación de la metodología. Finalmente se concluyó que el proyecto fue un aporte para la seguridad de la compañía porque se logra prevenir un inminente riesgo.

Palabras clave: metodología de seguridad, correo electrónico, dispositivos móviles blackberry

ABSTRACT

Security methodology was developed for the corporate email service on Blackberry mobile devices in the enterprise Chevy Plan Colombia. This project arises from the need to establish processes and safety measures to reduce the possibility of loss or information leakage. The methodology design was carried out in three stages. The first was exploratory, where a survey was conducted to determine the end use of the mobile device, then a descriptive stage in which a document status and responsibilities was created as a record of the policies implied Software BlackBerry Enterprise Server Express. Finally, an ending a stage in which a study was conducted to determine the impact that would have the methodology implementation. Finally it was concluded that the project was a contribution to the company's safety because it does prevent imminent risk.

Keywords: security methodology, email, mobile devices, blackberry

INTRODUCCIÓN

La portabilidad de la información es un tema que día a día causa mayor interés en todas las organizaciones a nivel nacional debido a que es una arista más que el negocio necesita para mantenerse competitivo en el medio, y que brinda la posibilidad de tener la información disponible en tiempo real, lo cual permite tomar decisiones de una manera más eficiente, darle continuidad a los procesos del negocio sin importar el momento ni lugar de donde se esté, y que el empleado sea más productivo. Sin embargo el desafío es que estos dispositivos tienen un mayor riesgo de perderse o ser robados, con la probabilidad de caer en manos equivocadas generando pérdida de datos personales o fuga de datos corporativos.

En este orden de ideas el presente proyecto tiene como objetivo primordial, diseñar una metodología de seguridad que permita proteger la información del correo electrónico corporativo en dispositivos móviles BlackBerry de ChevyPlan Colombia.

Este desarrollo implica realizar una investigación previa para conocer el estado de la compañía en cuanto al manejo que se le da a los smartphones y tablets. Posteriormente analizar y plantear las políticas que deben ser implementadas desde la consola del Software Blackberry Enterprise Server Express, al igual que instituir un documento donde el usuario conocerá las responsabilidades y obligaciones a las que está comprometido.

Finalmente la metodología estará expuesta a una evaluación para medir la efectividad y el nivel de seguridad por parte de los técnicos, donde el resultado nos indicará posibles correcciones y/o actualizaciones.

Lo que se pretende es entregar a ChevyPlan Colombia una metodología óptima, funcional que cumpla con el objetivo y el alcance aquí documentados.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

El servicio de correo electrónico es una herramienta vital para la gestión de los procesos de la compañía, a través de este viaja a diario información esencial para el cumplimiento de las actividades propias del negocio. Dicha información está catalogada como uno de los activos más valiosos de la organización y es por tal motivo que surge la necesidad de establecer metodologías que permitan ofrecer el servicio de manera segura y administrada.

En el caso de *CHEVYPLAN COLOMBIA,* el servicio de correo electrónico actualmente se encuentra configurado en varios equipos móviles sin previa autorización y control, dejando así una falencia enorme en el tema de seguridad de la información corporativa, ya que se podría presentar la pérdida o robo de un equipo y en el peor de los escenarios caer en manos de personas que puedan poner en riesgo la integridad de la información confidencial que administra la compañía. Los trabajadores no son conscientes del inminente peligro al que exponen a la empresa manipulando el correo corporativo desde sus dispositivos móviles personales, debido a que no existe un proceso o metodología que garantice la seguridad de los datos y administre el personal que realmente debe tener este servicio configurado en su dispositivo.

De acuerdo a lo anterior y a la ley 1581 de protección de datos, se ve la necesidad de administrar los recursos tecnológicos con los que cuentan la compañía y controlar el uso del servicio de correo electrónico de tal manera que sea utilizado única y exclusivamente por el personal autorizado, todo esto mediante el desarrollo de una metodología que garantice el uso de este servicio de forma segura.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo proteger el servicio de correo electrónico corporativo en los dispositivos móviles Blackberry de la empresa CHEVYPLAN COLOMBIA?

2. JUSTIFICACIÓN

Es de vital importancia este proyecto ya que por medio de él, *CHEVYPLAN COLOMBIA* adquirirá el conocimiento de nuevas alternativas de seguridad que le permitirá gestionar y/o administrar sus procesos a través de dispositivos móviles de forma controlada y segura, mitigando los riesgos de pérdida o fuga de información corporativa.

Este trabajo presenta un impacto de carácter social considerable, puesto que el riesgo de pérdida de información será menor, ya que existirán controles sobre el correo electrónico corporativo, donde habrá un perfilamiento según el usuario, se hará entrega de un manual de uso, y un documento de términos y condiciones . El mayor propósito es poder brindar a esta organización una metodología apropiada para que puedan dar desarrollo a sus actividades sin ningún problema y así ofrecer una adecuada gestión, administración y protección de su información. La intención de esta metodología es aportar a la continuidad del negocio y mejorar el funcionamiento de los procesos.

Con base en las afirmaciones anteriores, se hace necesario dar a conocer a la compañía las alternativas de seguridad que ofrece el mercado, para la optimización de sus recursos humanos y financieros, generando espacios para la planeación y la proyección de la empresa.

Estas son algunas de las razones por las cuales es necesario realizar una metodología de seguridad para dispositivos móviles en *CHEVYPLAN*, que proteja la información corporativa a la que se va a consultar y modificar a través del correo electrónico corporativo desde un dispositivo móvil Blackberry. En consecuencia, este trabajo puede contribuir no solo al mejoramiento de los procesos, rendimiento y tiempos de respuesta, sino también al posicionamiento y el buen nombre de la compañía en cuanto a prestigio y calidad se refiere.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Desarrollar una metodología de seguridad que permita proteger la información del correo electrónico corporativo en dispositivos móviles Blackberry de la empresa CHEVYPLAN COLOMBIA.

3.2 OBJETIVOS ESPECÍFICOS

- Realizar estudio al personal de *CHEVYPLAN* para identificar el fin del uso del dispositivo móvil.

- Diseñar e implementar políticas de seguridad a los dispositivos móviles corporativos en la consola exchange y mediante el software Blackberry Enterprise Server Express.

- Entregar documento de término y condiciones de uso y/o aplicaciones en los dispositivos móviles.

- Conocer el impacto que tendría la implementación de esta metodología en la compañía.

4. ALCALCE

El alcance de este trabajo será el desarrollo de una metodología de seguridad para el correo corporativo en dispositivos móviles que la empresa *CHEVYPLAN COLOMBIA* entregará a sus trabajadores, que en este caso son smartphone de sistema operativo BlackBerry; lo anterior estará soportado y administrado de manera preventiva mediante un software que permita la parametrización de políticas requeridas para el aseguramiento de la información siguiendo los lineamientos misionales de la organización.

Por lo tanto, este trabajo estará orientado en la línea de investigación de gestión de la seguridad y el riesgo, con un tipo de investigación exploratoria que posteriormente será descriptiva.

5. PRESUPUESTO

Para realización de la metodología, se tendrá en cuenta el siguiente presupuesto.

Cuadro 1. Presupuesto de personal

Ítem	Descripción	Entidad	Horas	Vr. horas	Vr. total
1	Oficial de Seguridad	CHEVYPLAN	2	$35.000	$70.000
2	Ing. Infraestructura	CHEVYPLAN	4	$25.000	$50.000
	Operador	CHEVYPLAN	4	$15.000	$30.000
Total			10		$150.000

Es el tiempo del personal de ChevyPlan Colombia dedicará a realizar y proporcionar la información para el buen desarrollo de la metodología de seguridad enfocada en dispositivos móviles Blackberry.

Cuadro 2. Presupuesto Software y papelería

Ítem	Descripción	Entidad	Cantidad	Vr. unitario	Vr. total
1	ExChange	CHEVYPLAN	1	$0	$0
2	Blackberry Interprise Server	CHEVYPLAN	1	$0	$0
3	Impresión	Especialistas S.I.	300		$30.000
Total					$30.000

Los insumos de oficina como CD-RW, tinta, papelería etc. serán suministrados por los ingenieros que desarrollan la metodología (Especialistas S.I), en cuanto a las aplicaciones ExChange y Blackberry Interprise Server, no tendrán costos ya que son software con los que cuenta actualmente la compañía ChevyPlan.

Cuadro 3, Presupuesto de otros elementos

Ítem	Descripción	Entidad	Cantidad	Vr. unitario	Vr. total
1	Consumo energía	Especialistas S.I.			$50.000
2	Consumo internet	Especialistas S.I.			$20.000
3	Consumo teléfono (fijo y móvil)	Especialistas S.I.			$30.000
4	Transporte	Especialistas S.I.			$20.000
Total					$120.000

El presupuesto de otros elementos será responsabilidad de los ingenieros que desarrollan la metodología (Especialistas S.I.), debido a que el desarrollo del proyecto se llevará a cabo en algunas ocasiones en sus lugares de residencia.

Cuadro 4. Resumen de presupuesto

Ítem	Descripción	Costo
1	Personal	$150.000
2	Software y papelería	$30.000
3	Otros	$120.000
Total		$300.000

Con base en el cuadro anterior se observa que el costo total del desarrollo de la metodología es de $300.000 y se encuentra distribuido de la siguiente forma $150.000 para gastos de personal, $30.000 para gastos de papelería, $120.000 para otros gastos como consumo de energía, transporte, consumo de teléfono etc. Tal presupuesto es totalmente viable.

Cuadro 5. Presupuesto para el mantenimiento de la metodología

Ítem	Descripción	Entidad	Horas	Vr, horas	Vr, total
1	Capacitación	CHEVYPLAN	3	$35.000	$105.000
2	Soporte técnico	CHEVYPLAN	4	$15.000	$60.000
Total					$165.000

El valor de mantenimiento de la metodología está presupuestado en $165.000, es netamente informativo y no está incluido en el alcance del proyecto.

6. CRONOGRAMA

Para el desarrollo del proyecto se tendrá el siguiente cronograma de actividades comprendido desde el mes _____ hasta la _____ semana de _____.

Cuadro 6. Etapa 1

ACTIVIDADES	DICIEMBRE				
SEMANAS	1	2	3	4	5
Realizar estudio al personal ChevyPlan					
Diseño e implementación políticas de seguridad					

Cuadro 7. Etapa 2

ACTIVIDADES	ENERO				
SEMANAS	1	2	3	4	5
Elaboración documento de condiciones de uso					
Análisis de impacto					

7. DISEÑO METODOLÓGICO

Para dar estricto cumplimento a los objetivos propuestos en este proyecto, este se dividirá en tres etapas.

La primera etapa se conocerá como *etapa explorativa*. Será la encargada del análisis en cuanto al manejo y fin último que los usuarios le dan a sus dispositivos móviles, generando así una idea de la situación actual en ChevyPlan Colombia, lo cual suministra un enfoque prospectivo.

La segunda etapa será la *etapa descriptiva.* En la cual se documentaran políticas de seguridad a los dispositivos móviles corporativos mediante el Software BlackBerry Enterprise Server Express y se diseñará un documento de término y condiciones de uso para el usuario donde se dará a conocer sus responsabilidades.

Por último se encuentra la *etapa de finalización.* Donde se conocerá el impacto que tendrá la implementación de esta metodología en la compañía.

7.1 ETAPA EXPLORATIVA

7.1.1 Encuesta.

La encuesta fue realizada a 150 personas empleadas de diferentes áreas de la compañía ChevyPlan Colombia (ver Anexo A)

Cuadro 8.¿Utiliza algún tipo de dispositivo como SmartPhone o tablet?

SI	NO
145	5
96%	4%

Cuadro 9.¿Utiliza el dispositivo móvil con fin corporativo?

SI	NO
137	13
91%	9%

Si su anterior respuesta fue si, por favor continúe con la encuesta de lo contrario muchas gracias por su colaboración.

Cuadro 10.¿Cuáles son los fines empresariales del uso de los dispositivos?

Correo Electrónico	Acceso de Aplicaciones	No Usa
137	0	0
100%	0%	0%

Cuadro 11.¿Usted está autorizado o ha firmado un documento para utilizar algún servicio corporativo en su dispositivo móvil?

SI	NO
37	100
27%	73%

Cuadro 12. ¿Los dispositivos móviles son herramientas necesarias para su labor diaria del negocio?

SI	NO
119	18
86%	14%

Cuadro 13. ¿Su dispositivo móvil es personal o corporativo?

PERSONAL	CORPORATIVO
87	50
63%	37%

Cuadro 14.¿Qué sistema operativo maneja su dispositivo móvil?

IOS	13	10%
BlackBerry	92	67%
Android	32	23%

Cuadro. 15. ¿Consideran los dispositivos móviles viables para la funcionalidad de la compañía? ¿Por qué?

Aumentar las ventas	15%
Aumentar la agilidad del negocio	19%
Mejorar las relaciones con los clientes	22%
Mejorar la efectividad de los empleados	19%
Reducir los costos de hacer negocios	16%
Reducir tiempo para completar tareas del negocio	9%

De la anterior encuesta se evidencia la necesidad de implementar un control donde se solicite la autorización del uso del correo corporativo ya que es el único servicio al cual los distintos empleados están accesando desde sus dispositivos personales o empresariales. La idea es que firmen un documento de término y condiciones para que conozcan la forma de uso y responsabilidades referente al servicio, siempre y cuando esta persona se encuentre en la solicitud de autorización de acceso al correo, diligenciado debidamente por su jefe inmediato.

Las personas a las que se evidencien el servicio activo y no estén registradas en una solicitud de autorización, el ingeniero de infraestructura procederá a inactivar la cuenta para su uso desde su dispositivo móvil.

7.2 ETAPA DESCRIPTIVA

7.2.1 Diseño políticas de seguridad. A continuación se documentan una serie de políticas de seguridad para los dispositivos móviles Blackberry de la empresa ChevyPlan Colombia, las cuales están implícitas en el Software Blackberry Enterprise Server Express y es de consideración del administrador cual desea aplicar, en este caso para el desarrollo de la metodología todas las políticas son viables y se implementarán.

7.2.1.1 Bluetooth.

- *Desactivar el desvío inalámbrico***.** *(Valor: SI)* Especifique si un dispositivo BlackBerry activado para bluetooth puede realizar un desvío inalámbrico en una conexión bluetooth. Si no configura esta regla, se usará el valor predeterminado Sí. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 4.1.0 y superior.

- *Desactivar Bluetooth***.** *(Valor: SI)* Especifique si se ha desactivado la tecnología Bluetooth en el dispositivo BlackBerry. Si la radio inalámbrica bluetooth está activa cuando el dispositivo BlackBerry recibe esta regla de política de TI, el dispositivo BlackBerry debe restablecerse manualmente para que los cambios surtan efecto. Si no configura esta regla, se usará el valor predeterminado No. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 3.8.0 y superior.

7.2.1.2 Global

- *Permitir explorador. (Valor: SI)* Especifique si el usuario puede usar el explorador BlackBerry que se incluye en el dispositivo BlackBerry. Establezca esta regla en No, para ocultar el icono del explorador BlackBerry en el dispositivo BlackBerry. Si no configura esta regla, se usará el valor predeterminado Sí. Esta regla se aplica a dispositivos BlackBerry basados en Java, versión 3.6.0 y superior, y a dispositivos BlackBerry 85x/95x, versión 2.5.0 y superior.

- *Permitir teléfono***.** *(Valor: SI)* Especifique si la función de teléfono del dispositivo BlackBerry está disponible para el usuario. Establezca esta regla de política de TI en No, si desea que los usuarios no puedan realizar ni recibir llamadas que no sean llamadas de emergencia desde los dispositivos BlackBerry. El icono de teléfono sigue visible en los dispositivos BlackBerry. Si no configura esta regla, se usará el valor predeterminado Sí. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 3.6.0 y superior.

7.2.1.3 Sincronización de PIM

- *Desactivar toda la sincronización inalámbrica. (Valor: NO***)** Especifique si desea desactivar la sincronización inalámbrica de todas las bases de datos de la gestión PIM. Establezca esta regla en Sí para desactivar la sincronización de

los contactos, notas, tareas y calendario. Nota: esta regla no influye en la reconciliación inalámbrica de mensajes. Los usuarios pueden seguir enviando y recibiendo mensajes. Si no configura esta regla, se usará el valor predeterminado No. Esta regla se aplica a dispositivos BlackBerry basados en Java, versión 4.0.0 y superior, y a dispositivos BlackBerry 85x/95x, versión 2.7.0 y superior.

7.2.1.4 Sólo dispositivo

- *El usuario puede desactivar la contraseña. (Valor: NO)* Especifique si el usuario puede desactivar el requisito de una contraseña de seguridad para el dispositivo BlackBerry. Establezca esta regla en No, para impedir que los usuarios puedan desactivar el requisito de contraseña en el dispositivo BlackBerry. Dependencia de la regla: el dispositivo BlackBerry usa esta regla sólo si se ha establecido una contraseña de dispositivo BlackBerry. Para que se requiera una contraseña de dispositivo BlackBerry, establezca la regla contraseña necesaria en Sí. Si no configura esta regla, se usará el valor predeterminado Sí. Esta regla se aplica a dispositivos BlackBerry basados en Java, versión 3.6.0 a 4.0.0, y a dispositivos BlackBerry 85x/95x, versión 2.5.0 a 2.7.0.

- *Tiempo de espera de seguridad máximo. (Valor: 10*) Especifique el tiempo máximo, en minutos, que un usuario del dispositivo BlackBerry puede establecer como valor de tiempo de espera de seguridad (número de minutos de inactividad permitida a un usuario del dispositivo BlackBerry antes de que se active el tiempo de espera de seguridad y de que se solicite al usuario del dispositivo BlackBerry que escriba la contraseña para desbloquear el dispositivo BlackBerry). El usuario del dispositivo BlackBerry puede establecer el valor que desee para el tiempo de espera de seguridad siempre que sea inferior o igual al valor máximo, salvo que se haya definido el valor de la regla el usuario puede modificar el tiempo de espera en No. El valor del tiempo de espera de seguridad máximo disponible de forma predeterminada en el dispositivo BlackBerry es de 60 minutos. Utilice la regla Definir el tiempo de espera de contraseña para ajustar un valor de tiempo de espera específico. Dependencia de la regla: el dispositivo BlackBerry usa esta regla de política de TI sólo si la regla Contraseña necesaria se establece en Sí. El intervalo válido para el valor de esta regla es de 10 a 480 minutos. Esta regla se aplica a dispositivos BlackBerry basados en Java, versión 3.6.0 y superior, y a dispositivos BlackBerry 85x/95x, versión 2.5.0 y superior.

- *Activar el tiempo de espera a largo plazo. (Valor: NO*) Especifica si el dispositivo BlackBerry se bloquea después de un período de tiempo predefinido, independientemente de si se ha usado o no el dispositivo BlackBerry durante ese intervalo. Establezca esta regla en Sí para forzar el bloqueo automático del dispositivo BlackBerry después de 60 minutos. Nota: puede usar la regla Tiempo periódico de búsqueda para acortar el intervalo del tiempo de espera. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 3.6.0 y superior.

- *Permitir SMS. (Valor: SI*). Especifique si el dispositivo BlackBerry permite enviar mensajes de texto SMS (servicio de mensajes cortos). Establezca esta regla en No para ocultar la función de mensaje de texto en el dispositivo BlackBerry. Nota: para bloquear los mensaje de texto (SMS) entrantes, configure la regla de política de TI el firewall bloquea los mensajes entrantes en el grupo de políticas de seguridad. Si no configura esta regla, se usará el valor predeterminado Sí. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 3.6.0 y superior.

- *Activar configuración WAP. (Valor: SI).* Especifique si el usuario puede ver y usar el icono del explorador WAP en el dispositivo BlackBerry (si el proveedor de servicios de Internet suministra el explorador WAP y si los libros de servicios están en el dispositivo BlackBerry). Establezca esta regla en No para ocultar el icono del explorador WAP en el dispositivo BlackBerry. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 3.6.0 y superior.

- *Permitir la mensajería "punto a punto". (Valor: SI)* Especifique si el usuario puede enviar mensajes PIN desde el dispositivo BlackBerry. Establezca esta regla en No para ocultar la funcionalidad de mensajería PIN en el dispositivo BlackBerry. Nota: para bloquear los mensajes PIN entrantes, configure la regla de política de TI el firewall bloquea los mensajes entrantes en el grupo de políticas de seguridad. Si no configura esta regla, se usará el valor predeterminado Sí. Esta regla se aplica a dispositivos BlackBerry basados en Java, versión 3.6.0 y superior, y a dispositivos BlackBerry 85x/95x, versión 2.5.0 y superior.

- *Longitud mínima de la contraseña. (Valor: 8).* Escriba la longitud mínima requerida, en caracteres, de la contraseña de dispositivo BlackBerry. Esta regla solo controla la longitud mínima de la contraseña, no la longitud máxima de la contraseña. La longitud máxima de la contraseña es de 32 caracteres. Dependencia de la regla: el dispositivo BlackBerry usa esta regla sólo si se ha establecido una contraseña de dispositivo BlackBerry. Para que se requiera

una contraseña de dispositivo BlackBerry, establezca la regla Contraseña necesaria en Sí. Advertencia: si la regla nivel FIPS está establecida en 2, el dispositivo BlackBerry la ignorará y requerirá explícitamente una longitud mínima de cinco caracteres para la contraseña. El intervalo válido para el valor de esta regla es de 4 a 14 caracteres. Esta regla se aplica a dispositivos BlackBerry basados en Java, versión 3.6.0 y superior, y a dispositivos BlackBerry 85x/95x, versión 2.5.0 y superior.

- *Contraseña necesaria. (Valor: SI).* Especifique si el dispositivo BlackBerry requiere una contraseña. Establezca esta regla en Sí para que el usuario tenga que indicar una contraseña para desbloquear el dispositivo BlackBerry. Dependencia de la regla: si establece esta regla en Sí, deberá configurar la regla El usuario puede desactivar la contraseña en No para impedir que el usuario del dispositivo BlackBerry pueda desactivarla. Advertencia: si la regla Nivel FIPS se establece en 2, el dispositivo BlackBerry requerirá de forma explícita una contraseña e ignorará la configuración de esta regla. Si no configura esta regla, se usará el valor predeterminado No. Esta regla se aplica a dispositivos BlackBerry basados en Java, versión 3.6.0 y superior, y a dispositivos BlackBerry 85x/95x, versión 2.5.0 y superior.

- *Comprobaciones de patrones de contraseña*. (Valor: Al menos 1 carácter alfabético en mayúscula, 1 carácter alfabético en minúscula, 1 carácter numérico y 1 carácter especial). Especifique el patrón de caracteres que la contraseña del dispositivo BlackBerry deba cumplir. Dependencia de la regla: el dispositivo BlackBerry usa esta regla sólo si se ha establecido una contraseña de dispositivo BlackBerry. Para que se requiera una contraseña de dispositivo BlackBerry, establezca la regla Contraseña necesaria en Sí. Advertencia: si selecciona la opción 2 o la opción 3, se desactiva la comprobación del patrón de contraseñas en los dispositivos BlackBerry 95x/85x. Si no configura esta regla, se usará el valor predeterminado "Sin restricciones". Esta regla se aplica a dispositivos BlackBerry basados en Java, versión 3.6.0 y superior, y a dispositivos BlackBerry 85x/95x, versión 2.5.0 y superior.

- *Tiempo máximo de validez de la contraseña. (Valor: 60)* Escriba el número de días para que caduque la contraseña de dispositivo BlackBerry y que el dispositivo BlackBerry pida al usuario que establezca una contraseña nueva. Nota: establezca esta regla en 0 para impedir que la contraseña de dispositivo BlackBerry caduque. Dependencia de la regla: el dispositivo BlackBerry usa esta regla sólo si se ha establecido una contraseña de dispositivo BlackBerry. Para que se requiera una contraseña de dispositivo BlackBerry, establezca la regla Contraseña necesaria en Sí. El intervalo válido para el valor de esta regla

es de 0 a 65.535 días. Esta regla se aplica a dispositivos BlackBerry basados en Java, versión 3.6.0 y superior, y a dispositivos BlackBerry 85x/95x, versión 2.5.0 y superior.

- *El usuario puede modificar el tiempo de espera. (Valor: NO*) Especifique si el usuario del dispositivo BlackBerry puede modificar el tiempo de espera de seguridad a un valor inferior al valor que ha establecido usando la regla Tiempo de espera de seguridad máximo. Establezca esta regla en No para impedir al usuario modificar el valor del tiempo de espera. Si no configura esta regla, se usará el valor predeterminado Sí. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 3.6.0 y superior.

7.2.1.5 Actualizaciones del software con cable

- *Copia de seguridad de servicios criptográficos. (Valor: SI)* Especifique si desea desactivar la función del dispositivo BlackBerry para hacer una copia de seguridad de los datos de servicios criptográficos cuando un usuario actualiza BlackBerry Device Software. Si permite que un dispositivo BlackBerry haga una copia de seguridad de los datos de servicios criptográficos, el dispositivo BlackBerry puede seguir usando los servicios criptográficos después de completar el proceso de actualización sin que el usuario tenga que reactivar el dispositivo BlackBerry. Si no configura esta regla, se usará el valor predeterminado Sí. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 5.0.0 y superior.

- *Permitir la carga de software basado en web. (Valor: SI**).*** Especifique si el usuario puede actualizar BlackBerry Device Software utilizando la función de carga de software basado en web. Defina esta regla en No para impedir que un usuario utilice la función de carga de software basado en Web para actualizar BlackBerry Device Software. Si no configura esta regla, se usará el valor predeterminado No. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 5.0.0 y superior.

7.2.1.6 Wi-Fi

- *Desactivar Wi-Fi. (Valor: NO***)** Establezca esta regla en Sí para desactivar el uso de la Wi-Fi en el dispositivo. Si no configura esta regla, se usará el valor predeterminado No. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 4.2.1 y superior.

7.2.1.7 Cámara

- *Desactivar cámara de fotos. (Valor: NO*) Especifique si se puede utilizar la función para tomar fotos con la cámara del dispositivo BlackBerry. Si no configura esta regla, se usará el valor predeterminado No. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 4.2.0 y superior.

- *Desactivar cámara de vídeo. (Valor: NO)* Especifique si se pueden grabar vídeos con la cámara del dispositivo BlackBerry. Defina esta regla en Sí para desactivar la función de cámara de vídeo. Si no configura esta regla, se usará el valor predeterminado No. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 4.3.0 y superior.

7.2.1.8 Aplicaciones RIM Value-Added

- *Desactivar el acceso a los datos del organizador para aplicaciones de redes sociales. (Valor: SI)* Especifique si se impide que las aplicaciones de redes sociales accedan a los datos del organizador. Si se define en Sí, las aplicaciones de redes sociales como Facebook no tendrán acceso de lectura o escritura a la libreta de direcciones, el calendario y otros datos del organizador. Si no configura esta regla, se usará el valor predeterminado Sí. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 4.2.0 y superior.

7.2.1.9 Definido por el usuario

- *Regla Polit. B.B. Corporativa ChevyPlan. (Valor: SI)*

Común

- *Desactivar la grabación de notas de voz. (Valor: NO***)** Especifique si la función de grabación de nota de voz del dispositivo BlackBerry está activada. Defina esta regla en Sí para desactivar la función de grabación de nota de voz e impedir que aplicaciones del dispositivo BlackBerry tengan acceso a esta función. Si no configura esta regla, se usará el valor predeterminado No. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 4.3.0 y superior.

- *Desactivar MMS. (Valor: NO)* Especifique si desea impedir al usuario del dispositivo BlackBerry usar la funcionalidad MMS (servicio de mensajería multimedia) en el dispositivo BlackBerry. Establezca esta regla de política de TI en Sí para ocultar la funcionalidad MMS en el dispositivo BlackBerry. Nota: para bloquear los mensajes MMS entrantes, configure la regla de política de TI El firewall bloquea los mensajes entrantes en el grupo de políticas de seguridad. Si no configura esta regla, se usará el valor predeterminado No. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 4.0.2 y superior.

7.2.1.10 Dispositivos personales.

- *Requerir recursos de trabajo para realizar actividades de trabajo. (Valor: SI)* Especifique si el usuario de un dispositivo BlackBerry debe utilizar recursos de trabajo (por ejemplo, cuentas de correo electrónico o calendarios de trabajo) para realizar actividades de trabajo (por ejemplo, enviar mensajes de correo electrónico o invitaciones a reuniones a contactos de trabajo) en un dispositivo BlackBerry. Si establece esta regla en Sí, el usuario deberá realizar todas las actividades de trabajo mediante recursos de trabajo. Por ejemplo, el usuario deberá enviar mensajes de correo electrónico a contactos de trabajo mediante la cuenta de correo electrónico de trabajo, y deberá enviar invitaciones a reuniones a contactos de trabajo mediante el calendario de trabajo. Si establece esta regla en No, el dispositivo no obliga al usuario a realizar actividades de trabajo únicamente mediante recursos de trabajo. Si no configura esta regla, se usará el valor predeterminado No. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 6.0.0 y superior.

- *Permitir la separación del contenido de trabajo. (Valor: SI)* Esta regla controla qué aplicaciones del dispositivo BlackBerry pueden compartir y crear contenido de trabajo. Si establece esta regla en Sí, sólo las aplicaciones autorizadas podrán acceder al contenido de trabajo y finalizar tareas mediante el contenido de trabajo. Por ejemplo, sólo las aplicaciones autorizadas podrán pegar contenido de trabajo y el usuario sólo podrá enviar mensajes de correo electrónico a contactos de trabajo mediante su cuenta de correo electrónico de trabajo. Si establece esta regla en No, las aplicaciones del dispositivo BlackBerry no distinguirán entre el contenido de trabajo y el contenido personal en el dispositivo. Si no configura esta regla, se usará el valor predeterminado No. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 6.0.0 y superior.

- *Dominios de trabajo. (Valor: chevyplan.com.co)* Esta regla especifica una lista de nombres de recursos y ordenadores que identifican a su empresa. Puede

utilizar esta regla para especificar los nombres de dominio, nombres de servidores de certificados y dominios de direcciones de correo electrónico de su empresa. Por ejemplo, si el nombre de dominio de su empresa es ejemplo.com, escriba ejemplo.com. Todos los subdominios del dominio especificado se incluyen automáticamente. Si incluye varios nombres, separe cada entrada con una coma, un punto y coma o un espacio. Por ejemplo, escriba ejemplo.com, ejemplo.net, ejemplo.org. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 6.0.0 y superior.

- *Desactivar el reenvío de contenido de trabajo mediante canales personales. (Valor: SI)* Esta regla especifica si el usuario de un dispositivo BlackBerry no puede reenviar datos de trabajo a sus contactos mediante un canal personal, como BlackBerry Internet Service, la mensajería de texto SMS, la mensajería MMS o la mensajería PIN. Si establece esta regla en Sí, el usuario sólo podrá reenviar datos de trabajo a sus contactos mediante un canal de trabajo, como BlackBerry Enterprise Server. El usuario no podrá reenviar datos de trabajo mediante canales personales. Si establece esta regla en No, el dispositivo BlackBerry no distinguirá entre datos de trabajo y datos personales al reenviar los mensajes. Si no configura esta regla, se usará el valor predeterminado No. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 6.0.0 y superior.

7.2.1.11 BlackBerry App World

- *Activar la facturación del proveedor de servicios inalámbricos. (Valor: NO)* Especifique si un usuario de dispositivo BlackBerry puede adquirir aplicaciones del escaparate de BlackBerry App World mediante el plan de adquisición del proveedor de servicios inalámbricos de su empresa. Para permitir que un usuario adquiera aplicaciones de BlackBerry App World mediante el plan de adquisición del proveedor de servicios inalámbricos, establezca esta regla en Sí. Para impedir que un usuario adquiera aplicaciones de BlackBerry App World mediante el plan de adquisición del proveedor de servicios inalámbricos, establezca esta regla en No. Esta regla afectará sólo a los clientes de App World 2.0 o posterior. Si no configura esta regla, se usará el valor predeterminado No. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 5.0.0 y superior.

7.2.1.12 Mensajería de correo electrónico

- *Desactivación del correo electrónico con contenido multimedia. (Valor: NO)* Especifique si BlackBerry Enterprise Server envía mensajes de correo electrónico al dispositivo con contenido multimedia (HTML). Si no configura esta regla, se usará el valor predeterminado No. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 4.5.0 y superior.

- *Desactivación de la descarga manual de imágenes externas. (Valor: NO)* Especifique si el usuario del dispositivo BlackBerry puede solicitar manualmente contenido con referencia a URL (imágenes) que se incluya en los mensajes de correo electrónico que recibe el dispositivo BlackBerry. Si no configura esta regla, se usará el valor predeterminado No. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 4.5.0 y superior.

- *Confirmar la descarga de imágenes externas. (Valor: SI)* Especifica si el dispositivo BlackBerry muestra un cuadro de diálogo de confirmación a un usuario cuando se hace clic en Obtener imágenes en un mensaje de correo electrónico formateado en HTML. El mensaje del cuadro de diálogo de confirmación informa al usuario de que la descarga de imágenes desde Internet puede revelar la dirección de correo electrónico. Si no configura esta regla, se usará el valor predeterminado No. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 5.0.0 y superior.

- *Desactivar reenviar y responder a mensajes de cifrado nativo de Lotus Notes. (Valor: SI*) Especifique si desea impedir a un usuario del dispositivo BlackBerry reenviar y responder a mensajes cifrados con IBM Lotus Notes recibidos en los dispositivos BlackBerry. Si configura esta regla en Sí, los usuarios del dispositivo BlackBerry no pueden reenviar ni responder a mensajes cifrados de IBM Lotus Notes que se hayan recibido en los dispositivos BlackBerry. De forma predeterminada, el usuario de un dispositivo BlackBerry que pueda leer mensajes cifrados de IBM Lotus Notes en el dispositivo BlackBerry puede reenviar o responder a un mensaje cifrado que el dispositivo BlackBerry ha recibido, descifrado y descomprimido. BlackBerry Enterprise Server para IBM Lotus Domino descifra el mensaje antes de que el dispositivo BlackBerry envíe el mensaje al destinatario como texto sin formato. Si no configura esta regla, se usará el valor predeterminado No. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 4.2.1 y superior.

7.2.1.13 Contraseña

- *Definir los intentos máximos de contraseña. (Valor: 10)* Establezca el número de intentos permitidos para la contraseña (contraseñas incorrectas entradas) que se permiten en el dispositivo BlackBerry antes de que se borren los datos y que se desactive el dispositivo BlackBerry. Configuración predeterminada: 10 intentos de contraseña. Puede usar esta regla para reducir el número de intentos de contraseña. Dependencia de la regla: el dispositivo BlackBerry usa esta regla sólo si se ha establecido una contraseña de dispositivo BlackBerry. Para que se requiera una contraseña de dispositivo BlackBerry, establezca la regla Contraseña necesaria en Sí. El intervalo válido para el valor de esta regla es de 3 a 10 intentos. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 3.6.0 y superior.

- *Suprimir el eco de la contraseña. (Valor: SI*) Establezca esta regla en Sí para suprimir el eco (impresión en pantalla) de los caracteres que se insertan en la pantalla de contraseña después de que el usuario realice varios intentos de contraseña fallida para tratar de desbloquear el dispositivo BlackBerry. Dependencia de la regla: el dispositivo BlackBerry usa esta regla sólo si se ha establecido una contraseña de dispositivo BlackBerry. Para que se requiera una contraseña, establezca la regla Contraseña necesaria en Sí. Nota: puede establecer un número de intentos de contraseña fallida que el dispositivo BlackBerry autorice antes de se realice el eco de la contraseña (si está permitido), usando la regla Definir los intentos máximos de contraseña. Nota: si se establece la regla Nivel FIPS en 2, el dispositivo BlackBerry ignorará esta regla e impedirá de forma explícita el eco de la contraseña. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 3.6.0 y superior.

- *Contraseñas prohibidas. (Valor: Chevyplan, chevy, aveo, optra, captiva, spark, tracker, sail, cobalt, traverse, dmax, colombia, chevrolet, password, contraseña, 1234, Sonic*) Escriba una lista de valores de cadena separados por una coma con las palabras que los usuarios no pueden usar para definir sus contraseñas. Dependencia de la regla: el dispositivo BlackBerry usa esta regla sólo si se ha establecido una contraseña de dispositivo BlackBerry. Para que se requiera una contraseña de dispositivo BlackBerry, establezca la regla Contraseña necesaria en Sí. Nota: el dispositivo BlackBerry impide automáticamente la sustitución de las letras. Por ejemplo, si incluye la palabra "contraseña" en la lista de palabras prohibidas, los usuarios no pueden usar "contr@seña", "contra$eña", o "contraseña123" en el dispositivo BlackBerry. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 4.1.0 y superior.

- *Historial máximo de contraseñas. (Valor: 12).* Defina el número máximo de contraseñas anteriores que el dispositivo BlackBerry debe contrastar con las contraseñas nuevas para impedir la reutilización de las contraseñas antiguas. Nota: establezca esta regla como 0 para impedir que el dispositivo BlackBerry compruebe las contraseñas utilizadas. Dependencia de la regla: el dispositivo BlackBerry usa esta regla sólo si se ha establecido una contraseña de dispositivo BlackBerry. Para que se requiera una contraseña de dispositivo BlackBerry, establezca la regla Contraseña necesaria en Sí. El intervalo válido para el valor de esta regla es de 0 a 15 contraseñas. Si no configura esta regla, se usará el valor predeterminado 0. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 3.6.0 y superior.

- *Definir el tiempo de espera de contraseña. (Valor: 5)* Especifique la cantidad de tiempo (en minutos), que se permite al usuario del dispositivo BlackBerry estar inactivo antes de que produzca una desconexión de seguridad y que el dispositivo BlackBerry requiera que el usuario escriba la contraseña del dispositivo BlackBerry para desbloquearlo. Nota: el intervalo de tiempo de espera de seguridad predeterminado es de 2 minutos de inactividad para versiones de BlackBerry Device Software anteriores a la 4.7 y de 30 minutos de inactividad para BlackBerry Device Software versión 4.7 y posteriores. Dependencias de la regla: el dispositivo BlackBerry usa esta regla sólo si la regla Contraseña necesaria se establece en Sí. Si no se configura la regla El usuario puede modificar el tiempo de espera en No, el usuario del dispositivo BlackBerry puede establecer el tiempo de espera de la contraseña en uno de los intervalos de valores. El valor máximo predeterminado de tiempo de espera de seguridad disponible para el dispositivo BlackBerry es de 60 minutos. El intervalo válido para el valor de esta regla es de 0 a 60 días. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 3.6.0 y superior.

7.2.1.14 Seguridad

- *Intensidad de protección de contenido. (Valor: Alta).* Especifique si la protección de contenido se activa al seleccionar la intensidad criptográfica que el dispositivo BlackBerry utiliza para cifrar el contenido que recibe cuando está bloqueado. Cuando la protección de contenido está activada, el contenido del dispositivo BlackBerry está siempre protegido con el algoritmo de cifrado AES de 256 bits. Si el dispositivo BlackBerry está bloqueado cuando recibe el contenido, genera de forma aleatoria una clave de protección de contenido (una clave de cifrado AES de 256 bits) y un par de claves ECC, obtiene una clave de cifrado AES de 256 bits efímera de la contraseña del dispositivo BlackBerry y usa la clave efímera para cifrar la clave de protección de

contenido y la clave privada ECC. Alta: ofrece una seguridad y rendimiento buenos. Esta configuración es adecuada para la mayoría de las situaciones. Más alta: ofrece una seguridad mayor, pero un rendimiento más lento. Si usa esta configuración, RIM le recomienda establecer la regla de política de TI Longitud mínima de la contraseña en 12 caracteres. La más alta: ofrece el mayor nivel de seguridad, pero el rendimiento más lento. Si usa esta configuración, RIM le recomienda que solicite al usuario una contraseña de al menos 21 caracteres. Nota: establezca esta regla para priorizar la intensidad de cifrado o el tiempo de descifrado. Cuando BlackBerry Enterprise Server descifra el mensaje usando la clave de cifrado principal del dispositivo BlackBerry, utiliza primero una clave ECC pública en la operación de descifrado, seguida de una operación de descifrado AES de 256 bits. La operación de descifrado ECC añade tiempo al proceso de descifrado. Dependencia de la regla: el dispositivo BlackBerry usa esta regla de política de TI sólo si la regla Contraseña necesaria se establece en Sí. En los dispositivos BlackBerry versión 6.0.0 y superior, la regla Utilización de la protección de contenido también debe establecerse en Permitido. Nota: si no configura esta regla, BlackBerry Enterprise Server no fuerza la protección de contenido en el dispositivo BlackBerry; si el usuario activa la protección de contenido en el dispositivo BlackBerry, fuerza la configuración Alta que es la configuración predeterminada. Para dispositivos BlackBerry versión 5.0.0 y superior, al establecer esta política de TI también se cifrará el sistema de archivos internos (MMC incorporado) con la contraseña del usuario y una clave generada por el dispositivo si ya existe un sistema de archivos interno en el dispositivo. Los archivos multimedia ubicados en el sistema de archivos interno no se cifrará a menos que lo especifique el administrador con la política de TI "Forzar cifrado en archivos multimedia del sistema de archivos interno" o a menos que lo especifique el usuario. Para dispositivos BlackBerry con versiones inferiores a la 5.0.0, se puede usar la política de TI "Nivel de cifrado del sistema de archivos externo" para lograr un efecto similar. Esta opción también cifrará el sistema de archivos externo. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 4.0.0 y superior.

- *Permitir conexiones en ambos sentidos. (Valor: SI)* Especifique si las aplicaciones pueden abrir conexiones internas y externas simultáneamente. Nota: si establece esta regla en Sí, las aplicaciones pueden recabar datos subrepticiamente desde dentro del firewall y enviarlas fuera del firewall sin realizar ninguna auditoría, creando un posible problema de seguridad. Si no configura esta regla, se usará el valor predeterminado No. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 3.6.0 y superior.

- *Desactivar GPS. (Valor: NO).* Especifique si la funcionalidad GPS del dispositivo BlackBerry está activada. Si no configura esta regla, se usará el

valor predeterminado No. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 4.3.0 y superior.

- *Desactivar módem IP. (Valor: NO).* Especifique si se desactiva la característica de módem de protocolo de Internet (IP) de los dispositivos BlackBerry correspondientes. Si no configura esta regla, se usará el valor predeterminado No. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 4.0.0 y superior.

- *Desactivar la memoria externa. (Valor: NO).* Especifique si desea impedir que la característica de memoria ampliable (microSD) funcione en los dispositivos BlackBerry. Si no configura esta regla, se usará el valor predeterminado No. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 4.2.0 y superior.

- *Forzar bloqueo si en la funda. (Valor: SI).* Especifique si el dispositivo BlackBerry tiene un bloqueo de seguridad cuando se coloca en la funda. Si no configura esta regla, se usará el valor predeterminado No. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 3.6.0 y superior.

- *Permitir conexiones externas. (Valor: NO.* Especifique si las aplicaciones pueden iniciar una conexión externa (por ejemplo, hacia WAP, SMS u otros gateway públicos) en el dispositivo BlackBerry. Si no configura esta regla, se usará el valor predeterminado Sí. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 3.6.0 y superior.

- *Desactivar la descarga de aplicaciones de otros fabricantes. (Valor: NO)*.Especifique si un usuario puede instalar una aplicación (ya haya sido creada por RIM o no) en un dispositivo BlackBerry. Si establece esta regla en Sí, el usuario no podrá instalar aplicaciones de terceros y sólo podrá instalar aplicaciones creadas por RIM si usted no envía las aplicaciones al dispositivo mediante la configuración de software o si el usuario no está utilizando BlackBerry Browser (por ejemplo, el usuario puede instalar aplicaciones creadas por RIM con BlackBerry Desktop Manager). Si no configura esta regla, se usará el valor predeterminado No. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 3.6.0 y superior.

- *Permitir que aplicaciones de otros fabricantes usen el puerto serie. (Valor: NO)* Especifique si las aplicaciones de otros fabricantes del dispositivo BlackBerry

pueden usar el puerto serie y los puertos USB o IrDA. Si no configura esta regla, se usará el valor predeterminado Sí. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 3.6.0 y superior.

- *Nivel de cifrado del sistema de archivos externo. (Valor: Cifrar con la clave del dispositivo (incluyendo los directorios multimedia).* Especifique el nivel de cifrado del sistema de archivos que el dispositivo BlackBerry usa para cifrar archivos que almacena en un sistema de archivos externo. Puede usar esta regla de política de TI para requerir que un dispositivo BlackBerry cifre un sistema de archivos externo, incluyendo o no los directorios multimedia. Nota: el cifrado del sistema de archivos externo no se aplica a archivos que el usuario del dispositivo BlackBerry transfiere manualmente al dispositivo de memoria externo (por ejemplo, desde un dispositivo USB de almacenamiento masivo). Si no configura esta regla, se usará el valor predeterminado "No requerido". Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 4.2.0 y superior.

- *Desactivar el almacenamiento masivo USB. (Valor: NO).* Especifique si desea impedir que la característica de almacenamiento masivo USB o el Protocolo de transferencia multimedia funcionen en los dispositivos BlackBerry compatibles. Si establece esta regla de política de TI en Sí, el dispositivo BlackBerry no puede usar un sistema de archivos externo conectado al puerto USB. Esto significa que no está activada la capacidad de transferir archivos a un sistema de archivos externos utilizando Media Manager en BlackBerry Desktop Manager versión 4.2.2 y 4.3. Si no configura esta regla, se usará el valor predeterminado No. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 4.2.0 y superior.

- *Restablecer los valores predeterminados de serie al borrar. (Valor: NO)* Especifique si el dispositivo BlackBerry se restablece por sí sólo a la configuración predeterminada de serie cuando recibe el comando de administración de TI Eliminar todos los datos del dispositivo y desactivar dispositivo por la red inalámbrica. Establezca esta regla de política de TI en Sí para requerir que el dispositivo BlackBerry borre de forma permanente las políticas de TI guardadas, elimine todas las aplicaciones de otros fabricantes y realice además el proceso de borrado del dispositivo BlackBerry. Para dispositivos BlackBerry versión 5.0.0 y superior, la política de TI no sólo se impone en el borrado remoto sino también en el borrado local, es decir, cuando el usuario supera el número máximo de intentos de contraseña o realiza un borrado de seguridad. Si no configura esta regla, se usará el valor predeterminado No. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 4.2.2 y superior.

- *Permitir el restablecimiento del temporizador de inactividad. (Valor: NO)* Especifique si BlackBerry permitirá que aplicaciones de otros fabricantes restablezcan el temporizador de inactividad del dispositivo, omitiendo el tiempo de espera de seguridad. Si no configura esta regla, se usará el valor predeterminado No. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 4.2.1 y superior.

- *Desactivar 3DES Transport Crypto. (Valor: NO*) Especifique si desea impedir que el dispositivo BlackBerry use el algoritmo Triple DES para cifrar y descifrar los paquetes que el dispositivo BlackBerry y BlackBerry Enterprise Server (que envía la política de TI) se envían entre sí. Configure esta regla de política de TI en Sí para que sea necesario que el dispositivo BlackBerry y BlackBerry Enterprise Server usen el algoritmo AES para cifrar y descifrar la comunicación entre ellos. Si no configura esta regla, se usará el valor predeterminado No. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 4.0.0 y superior.

7.2.1.15 Explorador

- **Desactivar Java Script en el explorador. (Valor:** NO**)** Especifique si se impide la ejecución de código JavaScript en un dispositivo BlackBerry. Si no configura esta regla, se usará el valor predeterminado No. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 4.0.0 y superior.

7.2.1.16 Actualizaciones inalámbricas de software

- *Desactivar la descarga de revisiones a través de WAN en itinerancia. (Valor: SI)* Especifique si desea impedir que la aplicación de la actualización inalámbrica de software del dispositivo BlackBerry descargue archivos del paquete de actualización de software a través de una conexión WAN en itinerancia. Si no configura esta regla, se usará el valor predeterminado No. Esta regla se aplica sólo a los dispositivos BlackBerry basados en Java, versión 4.5.0 y superior.

De igual manera el documento de término y condiciones, el cual cada usuario firmara para indicar que está de acuerdo y que cumplirá con las obligaciones y responsabilidades implícitas en el formato. (Ver Anexo B y Anexo C)

7.3 ETAPA DE FINALIZACIÓN

Para conocer el impacto de la implementación de la metodología en la compañía, se realizó una reunión con los distintos directores de las áreas involucradas en el proyecto, donde se efectuó una retroalimentación del diseño, e implementación del mismo, enviando posteriormente un memorando interno informativo acerca del proceso para que se cumpla a cabalidad con las políticas y condiciones de uso estipuladas en la metodología de seguridad.

7.3.1 Encuesta a los técnicos. Igualmente se formuló una encuesta a diez técnicos, para medir los atributos de efectividad y de nivel de seguridad de la metodología, (ver Anexo D). estos diez técnicos son ingenieros que laboran actualmente en la compañía, los cuales tienen el conocimiento y las competencias necesarias del tema para poder evaluarla. Cada variable fue medida en una escala de cinco valores: Muy baja, Baja, Media, Alta, Muy alta. El resultado fue el siguiente.

Atributo Seguridad

Cuadro 16. . ¿Cómo califica la herramienta BlackBerry Enterprise Server en el cumplimiento del esquema de complejidad para las contraseñas establecido por la compañía?

VALORACIÓN				
Muy baja	Baja	Media	Alta	Muy alta
			6	4

Atributo efectividad

Cuadro 17. ¿Qué importancia tiene el bloqueo automático en los dispositivos móviles BlackBerry para proteger su información?

VALORACIÓN				
Muy baja	Baja	Media	Alta	Muy alta
			3	7

Atributo Seguridad

Cuadro 18. ¿Qué relevancia tiene en cuanto a seguridad el cifrado de memoria tanto interno como externo?

VALORACIÓN				
Muy baja	Baja	Media	Alta	Muy alta
			5	5

Atributo Efectividad

Cuadro 19. . Como considera usted la administración de políticas de forma centraliza a los dispositivos móviles BlackBerry?

VALORACIÓN				
Muy baja	Baja	Media	Alta	Muy alta
			2	8

Atributo Seguridad

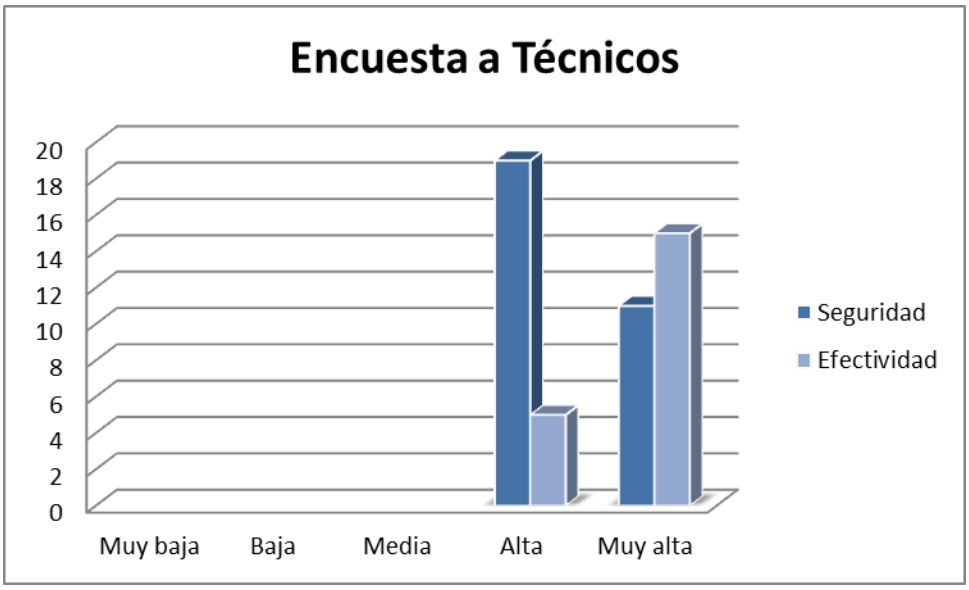
Cuadro 20. ¿De qué manera cree que la metodología minimiza la probabilidad de pérdida o fuga de información?

VALORACIÓN				
Muy baja	Baja	Media	Alta	Muy alta
			8	2

Cuadro 21. Resultado de la encuesta.

Atributos	**VALORACIÓN**				
	Muy baja	Baja	Media	Alta	Muy alta
Seguridad				19	11
Efectividad				5	15

Gráfico 1. Resultado encuesta a técnicos



Elaborado por el autor.

Todos los técnicos valoraron o calificaron la metodología en cuanto a efectividad y nivel de seguridad como muy alta o alta, lo cual expresa el reconocimiento y la necesidad que había de diseñar e implementar un proyecto de estas características. De igual manera los ingenieros consideraron que la metodología propuesta es pertinente, la cual puede convertirse en una herramienta útil para el desarrollo de los procesos de la organización.

A continuación se documentan los perfiles de los técnicos con el fin de dar una perspectiva de sus competencias y conocimientos. Los nombres han sido cambiados por seguridad de la información y por solicitud de los mismos.

Ingeniero: Angélica Martin
Empresa: Equidad Seguros O.C
Perfil.

Profesional en Ingeniería de Sistemas, con experiencia en Seguridad de la información, conocimientos sólidos en ISO 27001, metodología de análisis y gestión MAGERIT, Experiencia en Análisis de riegos, gestión de activos, gestión de riesgos y gestión de incidentes (PHVA). Conocimiento en continuidad del negocio (BCP, DRP, BIA). Arquitectura de red basada en seguridad, direccionamiento IP y protocolos. Legislación de seguridad de la información (Ley 1581:2012 Protección de datos, 527 Firmas digitales, circular 042:2012). Dominio

en consola de comandos, conexiones y aplicaciones (SSH, FTP. Capacidad para trabajar bajo presión, trabajo en equipo, adaptabilidad al cambio y continuo aprendizaje.

Ingeniero: Carlos Valbuena
Empresa: ChevyPlan Colombia
Perfil.

Administración de servidores en la plataforma Microsoft, administración y monitoreo de redes, administración de equipos de seguridad informática perimetral, switches antivirus cliente y consola con la experticia y conocimiento en tecnología. Cumplimiento, responsabilidad y apoyo en todas las labores encomendadas. Además poseo fortalezas en la atención del usuario final, manejo correcto de las herramientas informáticas.

Ingeniero: Diego Moreno
Empresa: Equidad Seguros O.C
Perfil.

Mi formación académica y mi desempeño profesional en las telecomunicaciones me permiten desplegar mis habilidades para desarrollar trabajos en el área de redes y telemática, conocimiento en CCNA, Competencias en seguridad informática, protocolos de red en Cisco, Huawei, Junniper, TELDAT. Adaptabilidad taal cambio y aprendizaje continuo orientado a la consecución de resultados.
Destacado por ser una persona con sentido de investigación y profundización; puntual, de actitud emprendedora, disciplinada, conducta intachable y sólida formación ética. Me considero una persona con apropiación de los ambientes laborales, sentido de pertenencia y responsabilidad.

Ingeniero: Andrés García
Empresa: ChevyPlan Colombia
Perfil.

Ingeniero de Telecomunicaciones experiencia en administración de servidores Linux y Windows 2008 Server y versiones anteriores. Administración de firewall Check Point, Junniper, Fortinet, Proventia, así como consolas de Antivirus Epo, herramientas de correo seguro como Ironport Herramientas de correlación de eventos y de monitoreo de disponibilidad y terminador VPNs Juniper. Manejo de cuentas, administrador de switch cisco. Poseo como habilidad la constante renovación y actualización técnica y tecnológica, Me caracterizo por ser una persona responsable, comprometida con el trabajo, con liderazgo para realizar

cualquier actividad laboral o personal y con una fuerte motivación al logro de los objetivos propuestos.

Ingeniero: Walter Urriago
Empresa: Equidad Seguros O.C
Perfil.

Ingeniero de Sistemas en formación, y Técnico en Sistemas & Desarrollo Informático, Certificado en Arquitectura HP, capacitado con profundos conocimientos en Sistemas Operativos, Bases de Datos, Programación Orientada a Objetos y Análisis de Sistemas, basados en las últimas tecnologías, que me permiten afrontar retos en la solución de problemas de las diferentes áreas de la industria informática general. Habilidades para desempeñarme en empresas de comunicaciones, industriales, comerciales o de mantenimiento, operando, monitoreando ó diseñando soluciones Corporativas de legado HP ProLiant BL/ML/DL con sistemas operativos como: VmWare ESX / ESXi, RedHat Enterprise Server y Microsoft Windows Server. Habilidades en Diagnósticos, liderazgo trabajo en equipo, garantizando tiempos de respuesta, calidad y cumplimiento.

Ingeniero: Juan Hernández
Empresa: ChevyPlan Colombia
Perfil.

Ingeniero de sistemas líder, proactivo con experiencia en diseño y desarrollo en proyectos de implementación de software a la medida. Mejora de procesos internos, control de calidad en productos de software, conocimiento de buenas prácticas de desarrollo, trabajo en equipo y bajo presión. Amplia experiencia en consultorías y resolviendo problemas en las áreas de servicio al cliente, soporte con tiempos de entrega muy cortos. Excelentes relaciones interpersonales.

Ingeniero: Omar Gómez
Empresa: Equidad Seguros O.C
Perfil.

Ingeniero de sistemas con especialización en telecomunicaciones, con la capacidad de analizar y gestionar los recursos tecnológicos teniendo en cuenta las necesidades empresariales y que estén a la vanguardia. Experiencia en asesorías para procesos de implementación de redes LAN, WAN y seguridad de redes Wi-Fi. Habilidad para la negociación. Amplio conocimiento en solución de errores para equipos, instalación y actualización. Fácil aprendizaje, trabajo individual o en grupo, honestidad, compromiso y respeto.

Ingeniero: Camilo Sierra
Empresa: ChevyPlan Colombia
Perfil.

Profesional en Ingeniería de Sistemas proactivo, de conocimientos sólidos. Especialización en Gerencia de proyectos de telecomunicaciones, con el conocimiento para establecer estándares de calidad. Experiencia en mantenimiento de diversos sistemas operativos, redes LAN, WAN, experiencia en el diseño de buenas prácticas para la gestión del personal y recursos, enfocadas en los objetivos misionales de la empresa. Experto en configuración de dispositivos de red. Responsable, ético y adaptable a lo cambios.

Ingeniero: Ricardo Castiblanco
Empresa: Equidad Seguros O.C
Perfil.

Ingeniero de Sistemas con el conocimiento para desarrollar propuestas costo/beneficio para proyectos de TI, liderar y coordinar equipos de trabajo, habilidad para toma de decisiones bajo presión. Experiencia en análisis de problemas diseño de soluciones mediante modelo y nuevas tecnologías de la información siempre enfocadas a la obtención de los mejores resultados y satisfacción al cliente. Alto sentido de profesionalismo, excelente presentación personal.

Ingeniero: Alexander Medina
Empresa: ChevyPlan Colombia
Perfil.

Ingeniero de Sistemas con más de cuatro años de experiencia liderando proyectos de redes; con claridad para analizar y evaluar los requerimientos de la empresa, generando soluciones para automatizar los procesos internos; autodidacta con habilidad para adaptarme al cambio y a las nuevas tecnologías. Enfocado a la transmisión de datos, disciplinado, emprendedor, tengo capacidad de asumir riesgos responsablemente. También tengo conocimiento y dominio de diversos sistemas operativos como lo son Linux, Mac y Windows. Poseo un alto nivel de compromiso, diligente y responsable.

7.3.2 Encuesta a los usuarios. En cuanto a los usuarios involucrados directamente con la metodología, también se les realizó una encuesta. La idea era conocer si estaban cumpliendo con las obligaciones y responsabilidades implícitas en el documento de término y condiciones. Esta pequeña investigación se aplicó a 30 personas, con el siguiente resultado. (ver Anexo E).

Cuadro 22. ¿Permite que personas diferentes a usted use los servicios y aplicaciones de ChevyPlan® configuradas en el dispositivo?

SI	NO
0	30
0%	100%

Cuadro 23. ¿Ha conectado el dispositivo móvil a computadores públicos (café internet, hoteles, aeropuertos, etc.)? ¿Así sea sólo para cargar la batería?

SI	NO
0	30
0%	100%

Cuadro 24. ¿Desde que se hizo entrega de su dispositivo móvil ha cambiado la contraseña al menos una vez?

SI	NO
30	0
100%	0%

Cuadro 25. ¿Ha conectado el dispositivo a redes WiFi desconocidas o públicas?

SI	NO
0	30
0%	100%

Cuadro 26. ¿Mantiene bajo absoluta confidencialidad y reserva la información que trabaja desde su dispositivo móvil?

SI	NO
30	0
100%	0%

Partiendo de la ética profesional de cada empleado, del compromiso adquirido firmando el documento de término y condiciones, de las políticas mandatorias administradas e implementadas desde la aplicación Blackberry Enterprise Server, Se puede afirmar que la metodología de seguridad para el servicio de correo electrónico corporativo en los dispositivos móviles BlackBerry de ChevyPlan

Colombia, está cumpliendo con el objetivo de proteger la información, mitigando la probabilidad de pérdida o fuga de datos. Esta implementación esta reduciendo el riesgo que existía hace algunos meses atrás, ya que se manipulaba información confidencial de la empresa mediante equipos móviles sin ningún tipo de control y muchos menos una política que definiera el uso y acceso a estos datos.

El no tener una autorización y un orden de quien realmente podía tener configurado el correo electrónico es su dispositivo y quien no, era una vulnerabilidad a la cual en algún momento se le podría sacar provecho por parte de personas malintencionadas. Una debilidad a la cual no se le hacía un seguimiento, ni monitoreo, por tal razón la información crítica estaba siempre expuesta a muchos riesgos. El desarrollo de la presente metodología permite que esta falencia deje de existir, debido a que ahora hay un tratamiento, un control y unas responsabilidades del uso de la información que llega y se envía a través del correo electrónico desde los dispositivos móviles BlackBerry de la compañía.

Finalmente y de acuerdo a los resultado obtenidos en las encuestas, a lo que se evidencia desde la aplicación Blackberry Enterprise y al compromiso adquirido por los distinto directores de cada área, se puede indicar que el impacto del proyecto es muy positivo, dado que hay un sentido de pertinencia y de colaboración por cada una de las personas involucradas en el desarrollo de la metodología de seguridad.

8. CONCLUSIONES

El desarrollo de cualquier modelo o metodología de seguridad es de gran importancia en cualquier tipo de empresa, porque permite obtener un conocimiento del estado actual a nivel de seguridad, las falencias, y necesidades, al igual que el diseñar controles y buenas prácticas para el correcto funcionamiento de los procesos de una compañía. Pero teniendo en cuenta que debe ser factible, y viable económicamente. También se debe considerar los requerimientos del sistema, core de negocio para así diseñar e implementar un proyecto de seguridad.

En el caso puntual de ChevyPlan Colombia, más que debilidades se evidenció procesos que debían estar documentados y establecidos, los cuales no existían, generando falencias de seguridad, con la probabilidad de que hubiera pérdida o fuga de información confidencial. Un inminente riesgo que podría traer consecuencias a futuro. Implementada la metodología para dispositivos móviles BlackBerry lo que se consiguió fue prevenir y cerrar esa brecha que existía, tanto así que cualquier funcionario puede recibir y enviar información desde su Smartphone sin importar su ubicación ya que este dispositivo está asociado a políticas y restricciones obligatorias desde una plataforma centralizada.

El detectar la no existencia de estos procesos fue un punto de partida para la toma de decisiones y las etapas de desarrollo. En este momento según la valoración de unos técnicos la metodología es efectiva y segura, pero es importante aclarar que debe pasar por una fase de verificación periódica (trimestral) para seguir midiendo la eficacia de los controles o para identificar mejoras.

BIBLIOGRAFÍA

ARROYO Rosalía. “El 26% de los españoles ha perdido datos de su empresa”. [Consultado 28 de Septiembre de 2013]..Disponible en Internet:< http://www.itespresso.es/el-26-de-los-espanoles-ha-perdido-datos-de-su-empresa-109204.html>

CONGRESO DE COLOMBIA. Ley Estatutaria 1581 de 2012 (Octubre 17). Por la cual se dictan disposiciones generales para la protección de datos personales. Bogotá D.C**.:** Diario Oficial 48587 de octubre 18 de 2012.

CHEVYPLAN. ¿Qué es cheviplan. [Consultado 11 de Diciembre de 2013]. Disponible en Internet:< ehttps://www.chevyplan.com.co/Chevyplan/Chevyplan/paginas/documento.aspx?idr=1483

EXCHANGE**.** Consola de administración de Exchange. **2010.** [Consultado 11 de Diciembre de2013]. Disponible en Internet:< http://technet.microsoft.com/es-es/library/bb123762(v=exchg.141).aspx

INSTITUTO COLOMBIANA DE NORMAS TÉCNICAS. Norma Técnica Colombiana NTC-ISO/IEC 27001.para la Tecnología de la información, técnicas de seguridad, sistemas de gestión de la seguridad de la información (SGSI), requisitos. Bogotá D.C., ICONTEC, 2006

INSTITUTO COLOMBIANA DE NORMAS TÉCNICAS. Norma Técnica Colombiana NTC-ISO/IEC 27002.para la Tecnología de la información, técnicas de seguridad, sistemas de gestión de la seguridad de la información (SGSI), requisitos. Bogotá D.C., ICONTEC, 2006.

INSTITUTO COLOMBIANA DE NORMAS TÉCNICAS. Norma Técnica Colombiana NTC 1486 para la presentación de tesis, trabajos de grado, y otros trabajos de investigación. Bogotá D.C., ICONTEC, 2008.

LA OPINION. “El acceso desde dispositivo móviles debe cumplir las políticas de seguridad”. [Consultado 11 de Diciembre de2013]. Disponible en Internet:<

http://www.laopinion.com.co/demo/index.php?option=com_content&task=view&id=375092&Itemid=32>.

METALOBOS J, & CARRILLO, J. “Análisis de Riesgo de Seguridad de la Información”. [Consultado 11 de Diciembre de 2013]. Disponible en Internet:< http://www.tesisde.com/t/analisis-de-riesgos-de-seguridad-de-la-i/322/>.

MICROSOFT .EXCHANGE. Dispositivos móviles. [Consultado 11 de Diciembre de 2013]. Disponible en Internet:< http://www.microsoft.com/exchange/2010/es/xl/mobile-devices.aspx

OFFICE COM. ¿Qué es una cuenta de correo electrónico de Exchange Server? ”. [Consultado 11 de Diciembre de 2013]. Disponible en Internet:< http://office.microsoft.com/es-es/outlook-help/que-es-una-cuenta-de-correo-electronico-de-exchange-server-HA001095504.aspx

REAL ACADEMIA DE LA LENGUA ESPAÑOLA. Tablet. Definición. Consultado 11 de Diciembre de 2013]. Disponible en Internet:< http://lema.rae.es/drae/>

REDMAN Phillip, GIRARD John, & BASSO, Mónica. Magic Quadrant for Mobile Device: Software de Gestion. [Consultado 13 de Septiembre de 2013]. Disponible en Internet:< https://dell.symantec.com/system/files/Magic_Quadrant_for_Mobile_Device_Management_Software.pdf>.

SEGURIDAD DE LA INFORMACIÓN. Políticas de seguridad. Consultado 11 de Diciembre de 2013]. Disponible en Internet>: http://www.segu-info.com.ar/politicas/

SYMANTEC. ”Encuesta de movilidad 2012”. [Consultado 13 de septiembre de 2013]. Disponible en Internet>: http://www.symantec.com/es/mx/theme.jsp?themeid=mobiletrends>

ANEXOS

ANEXO A

FORMATO ENCUESTA A EMPLEADOS DE CHEVYPLAN COLOMBIA

La encuesta fue realizada a 150 personas empleadas de diferentes áreas de la compañía ChevyPlan Colombia.

1. **¿**Utiliza algún tipo de dispositivo como SmartPhone o tablet?
2. ¿Utiliza el dispositivo móvil con fin corporativo?
3. ¿Cuáles son los fines empresariales del uso de los dispositivos?
4. ¿Usted está autorizado o ha firmado un documento para utilizar algún servicio corporativo en su dispositivo móvil?
5. ¿Los dispositivos móviles son herramientas necesarias para su labor diaria del negocio?
6. ¿Su dispositivo móvil es personal o corporativo?
7. ¿Qué sistema operativo maneja su dispositivo móvil?
8. ¿Consideran los dispositivos móviles viables para la funcionalidad de la compañía? ¿Por qué?

ANEXO B

CARTA DE CHEVYPLAN COLOMBIA

Buenas Tardes

Para ChevyPlan® la información es uno de sus principales activos y continuando con nuestra misión de protegerla hemos diseñado un nuevo procedimiento que nos ayudará a proteger los correos corporativos a los que accedemos a través de nuestros dispositivos móviles.

Por tal motivo, a partir del lunes 27 de enero del 2.014, empezaremos una actividad de depuración y aseguramiento del servicio, para lo cual solicitamos a todo el personal que hoy día tienen el correo de ChevyPlan® configurado en su Smartphone o Tablet tenga en cuenta:

Valide con su Director de Área si tiene aprobado la continuidad de este servicio.

Si es así, ingrese a la Intranet al sitio de Seguridad de la Información a la opción de Dispositivos Móviles y revise el documento de Términos y condiciones de uso en el siguiente link.

1. Si su dispositivo es propio, realice la configuración mínima de seguridad exigida con la ayuda de la Guía de buenas prácticas (clic aquí) y el personal de Soporte Técnico.

2. Si no está en la lista de aprobados, pídale a su Director de Área que tramite su aprobación.

Como siempre contamos con su colaboración y compromiso con la Seguridad de la Información de Chevyplan®.

Cualquier inquietud, comunicarse con Soporte Técnico.

Cordialmente;

Camilo Andrés Álvarez
Oficial de Seguridad Informática
ChevyPlan® S.A
Carrera 7 N° 75 - 26
Bogotá, Colombia
Tel. (57) (1) 6286820
Ext. (4067)
camilo.alvarez@chevyplan.com.co

ANEXO C.

TÉRMINOS Y CONDICIONES DE USO SEGURO DE SERVICIOS Y/O APLICACIONES EN DISPOSITIVOS MÓVILES DENTRO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Yo, _____ identificado (a) con cédula de ciudadanía número _____ de _____, manifiesto que he leído y entiendo el contenido del presente documento. En consecuencia, libre y voluntariamente me obligo con ChevyPlan® S.A. a dar uso seguro a los servicios y aplicaciones de la compañía configuradas en el dispositivo móvil tipo (personal/corporativo): _____, fabricante: _____ y modelo: _____, y a cumplir estrictamente con el contenido de la Política de Seguridad de la Información y del presente documento:

1. INTRODUCCIÓN:

El presente documento se encuentra alineado con la Política de Seguridad de la Información de ChevyPlan®, a la cual tengo permanente acceso y conocimiento.

2. OBJETIVO:

Desarrollar a través de este documento los términos y condiciones del uso seguro de aplicaciones y/o servicios en dispositivos móviles cumpliendo con la Política de Seguridad de la información de la compañía.

3. OBLIGACIONES:

3.1 EQUIPO:

- Mantener el dispositivo configurado con bloqueo por contraseña, PIN o patrón de desbloqueo.
- Mantener activo el parámetro de bloqueo del dispositivo por inactividad y que se ejecute a partir de 1 minuto.
- Mantener activa la opción de seguridad de borrado de datos y configurarlo para que se ejecute después de 10 intentos fallidos.

- Mantener activo el cifrado de la memoria tanto interna como externa.

- Mantener activo el servicio de borrado remoto.

- Instalar y mantener actualizado un antivirus para dispositivos móviles.

- Mantener deshabilitado el bluetooth.

- Mantener actualizado el dispositivo siempre que el sistema notifique que existe una actualización disponible.

- Realizar toda la gestión dentro de lo que la normatividad sobre datos personales permite y en particular no usar, guardar, compartir, o permitir acceso por parte de terceros a los datos que reciba de ChevyPlan® de ninguna manera diferente a lo previsto en la Política de Tratamiento de la Información.

3.2 CONTRASEÑAS

- Usar contraseñas que cuenten con los siguientes parámetros:

- Longitud mínima de 8 caracteres.
- Alfanumérica (letras y números).
- Incluir mayúsculas y minúsculas.
- Contener caracteres especiales como #$%&/*

- Cambiar las contraseñas del dispositivo al menos una vez cada 2 meses.

3 .3 APLICACIONES Y SERVICIOS:

- Por aplicación se entiende que es un tipo de programa informático diseñado como herramienta para permitir a un usuario realizar uno o diversos tipos de trabajos. ii) Por servicio se entiende toda aquella disponibilidad de un recurso tecnológico que busca responder a una necesidad; por ejemplo el correo electrónico corporativo.

- No debo permitir que nadie diferente a mí use los servicios y aplicaciones de ChevyPlan® configuradas en el dispositivo.

- Todas las marcas, derechos de autor, bases de datos y otros derechos de propiedad intelectual de la aplicación, cualquiera que sea su naturaleza son de propiedad de ChevyPlan® o los licenciadores de ChevyPlan®.

- Por el presente ChevyPlan® ofrece un uso revocable, gratuito y no exclusivo para utilizar los servicios y aplicaciones en el ámbito estrictamente profesional.

- No actuar ni permitir que terceras personas actúen en mi nombre para (i) hacer y distribuir copias de la aplicación; (ii) intentar copiar, reproducir, alterar, modificar, transferir, intercambiar o traducir la aplicación; (iii) crear ninguna clase de proyecto derivado de la Aplicación.

- ChevyPlan® se reserva el derecho a modificar o deshabilitar la aplicación y/o el servicio en cualquier momento y por cualquier motivo.

- En caso de pérdida, robo o daño del dispositivo debo informarlo a la brevedad posible y por cualquier medio al área de Soporte Técnico de ChevyPlan®.

- En caso de desvinculación laboral, si el dispositivo móvil es corporativo lo devolveré al área correspondiente, ó si el dispositivo móvil es personal eliminaré toda aquella información que pertenezca a ChevyPlan® S.A.; así como también desvincularé todos los servicios y aplicaciones que hayan sido instalados o configurados, absteniéndome una vez terminado el contrato por cualquier causa, de mantener copia parcial o total de la información y documentos obtenidos o generados con ocasión del vínculo con ChevyPlan®

- Tipo de Información qué podrá ser almacenada en el dispositivo móvil: La compañía definirá el tipo de información que los dispositivos móviles pueden almacenar, gestionar y recibir (pública, interna, sensible).

- Definición de los dispositivos móviles permitidos en función de su propietario: La compañía definirá si se admite un dispositivo personal, o dispositivo perteneciente a la organización, o ambos.

3.4 RECOMENDACIONES:

- No conectar el dispositivo a computadores públicos (café internet, hoteles, aeropuertos, etc.) así sea sólo para cargar la batería.

- No conectar el dispositivo a redes WiFi desconocidas o públicas.

3.5 DECLARACIONES

Entiendo y acepto que debo mantener bajo absoluta confidencialidad y reserva:

La información privilegiada a la que tenga acceso de la sociedad, en relación con su objeto social, sus políticas comerciales y de mercadeo, sus negocios, sus empleados, clientes, proveedores, sus cifras, proyecciones a futuro, decisiones administrativas, comerciales y financieras de cualquier naturaleza, su situación financiera, logística o de cualquiera otra índole, los programas de software desarrollados o adquiridos, las bases de datos.

La información y documentación concerniente a todos los procesos, formas de desarrollar su actividad, datos, informaciones, procedimientos, ideas, planes, equipos, estrategias de mercadeo y negocios, precios así como sobre los contratos u órdenes de servicios contratados.

De igual manera, me comprometo a no divulgar, ni utilizar, ni difundir por ningún medio, dicho conocimiento e información para el beneficio directo o indirecto de alguna persona, entidad o compañía, competidores o el mercado en general, sin autorización previa y escrita de la sociedad.

Exonero a ChevyPlan® de cualquier tipo de responsabilidad por un eventual robo de mi identidad o información personal por parte de terceros.

Acepto en nombre propio que he aprobado y estoy de acuerdo que me sean instaladas aplicaciones y servicios en mi dispositivo móvil personal, y que adicional a este documento, ChevyPlan® me ha compartido la *guía de buenas prácticas en el uso corporativo de dispositivos móviles*, a través de sus canales oficiales de comunicación.

Libre y voluntariamente declaro que es mi deseo utilizar mi dispositivo móvil personal para tener acceso a los servicios y aplicativos autorizados por ChevyPlan®, como una herramienta para facilitar el desarrollo de mis funciones.

3.6 AUTORIZACIONES

Autorizo expresa y previamente a CHEVYPLAN® o a quien esta designe a:

Efectuar monitorización del equipo físico *corporativo* que me fue asignado, así como de los mensajes y toda información corporativa o no, incluyendo datos personales que reciba, envíe o almacene en el mismo con el objeto de velar por la seguridad de la información y el uso adecuado del dispositivo móvil, según lo establecido en este documento. Entre los datos almacenados se incluyen a manera de ejemplo mensajes de correo electrónico, información de llamadas de telefonía, documentos privados y confidenciales, la agenda de contactos, el calendario con información de eventos y actividades, fotografías, videos, grabaciones de voz, listas de tareas, entre otros.

Efectuar monitorización del equipo físico *así sea de mi propiedad*, así como de los mensajes y toda información corporativa o no, incluyendo datos personales que reciba, envíe o almacene en el mismo con el objeto de velar por la seguridad de la información y el uso adecuado del dispositivo móvil, según lo establecido en este documento. Entre los datos almacenados se incluyen a manera de ejemplo mensajes de correo electrónico, información de llamadas de telefonía, documentos privados y confidenciales, la agenda de contactos, el calendario con información de eventos y actividades, fotografías, videos, grabaciones de voz, listas de tareas, entre otros.

Lo anterior únicamente en el evento de presentarse una eventual investigación interna de la compañía relacionada con la seguridad de la información o por orden judicial.

3.7 EFECTOS

Los servicios y aplicaciones en dispositivos móviles son herramientas de productividad que permiten gestionar actividades a tiempo y desde cualquier lugar; sin embargo una pérdida, robo o descuido del dispositivo puede llegar a causar consecuencias graves como lo es la pérdida de confidencialidad de la información de los accionistas, clientes, empleados y/o proveedores.

3.8 SANCIONES

El no cumplimiento de estos términos y condiciones de uso seguro de aplicaciones y/o servicios en dispositivos móviles podrán conllevar a la aplicación de las sanciones estipuladas en la POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA EMPLEADOS DIRECTOS o POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EMPLEADOS EN MISIÓN Y TERCEROS de acuerdo al tipo de contratación que tenga la persona que presta sus servicios a ChevyPlan® S.A.

_____

FIRMA
NOMBRE:
C.C.:
CARGO:
Copia a RRHH

ANEXO D

ENCUESTA A TÉCNICOS DE CHEVYPLAN COLOMBIA

Para atributos de efectividad y de nivel de seguridad de la metodología

1. ¿Cómo califica la herramienta BlackBerry Enterprise Server en el cumplimiento del esquema de complejidad para las contraseñas establecido por la compañía?

2. ¿Qué importancia tiene el bloqueo automático en los dispositivos móviles BlackBerry para proteger su información?

3. ¿Qué relevancia tiene en cuanto a seguridad el cifrado de memoria tanto interno como externo?

4. Como considera usted la administración de políticas de forma centraliza a los dispositivos móviles BlackBerry?

5. ¿De qué manera cree que la metodología minimiza la probabilidad de pérdida o fuga de información?

ANEXO E

ENCUESTA A USUARIOS INVOLUCRADOS DE CHEVYPLAN COLOMBIA

1. ¿Permite que personas diferentes a usted use los servicios y aplicaciones de ChevyPlan® configuradas en el dispositivo?

2. ¿Ha conectado el dispositivo móvil a computadores públicos (café internet, hoteles, aeropuertos, etc.)? ¿Así sea sólo para cargar la batería?

3. ¿Desde que se hizo entrega de su dispositivo móvil ha cambiado la contraseña al menos una vez?

4. ¿Ha conectado el dispositivo a redes WiFi desconocidas o públicas?

5. ¿Mantiene bajo absoluta confidencialidad y reserva la información que trabaja desde su dispositivo móvil?