EMPRESA DEPARTAMENTAL DE SERVICIOS PÚBLICOS DE BOYACÁ S.A. E.S.P. – EPB

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - 2020

LUZ MARIETHA AVILA FERNANDEZ

Gerencia

Empresa Departamental de Servicios Públicos de Boyacá S.A E.S.P.
Dirección: Cr 11 N° 20-54 Tel. 7445126-7449389-7441216
Web: www.espb.gov.co, correo institucional: empresa@espb.gov.co

I. - Información general del Plan

Codigo Interno del Plan 77

Nombre del Plan PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - 2020

Objetivo General Controlar y minimizar los riesgos asociados a los procesos tecnológicos existentes, en el EMPRESA DEPARTAMENTAL DE SERVICIOS PUBLICOS DE BOYACA S.A ESP con el fin de salvaguardar los activos de información, el manejo de medios, control de acceso y gestión de usuarios.

Vigencia del plan	
Fecha Inicio	28-ene.-20
Fecha Terminación	31-dic.-20

Presentación

La gestión de los riesgos de seguridad de la información tiene que ver con los procesos que reducen las perdidas y brindan protección a la información, permitiendo identificar las debilidades que afectan durante todo el ciclo de vida del servicio. Es muy importante que las organizaciones cuenten con un Plan de gestión del riesgo para garantizar la continuidad del negocio. Por este motivo, es necesario realizar el análisis de riesgos de seguridad de la información aplicado a la Empresa Departamental de Servicios Públicos de Boyacá SA ESP. Antes de formular este Plan de gestión se ha revisado el documento con el diagnóstico del sistema actual de la empresa, donde se reconoce la situación actual de la organización y la identificación de los activos con sus respectivas amenazas, para continuar con la medición de riesgos existentes y sugerir las protecciones necesarias que podrían formar parte del Plan de gestión de riesgos en la seguridad de la información. El Plan permite identificar el nivel de riesgo en que se encuentra los activos mediante el nivel de madurez de la seguridad existente e incentivar al personal a seguir las normas y procedimientos referentes a la seguridad de la información y los recursos.

Empresa Departamental de Servicios Públicos de Boyacá S.A E.S.P.
Dirección: Cr 11 N° 20-54 Tel. 7445126-7449389-7441216
Web: www.espb.gov.co, correo institucional: empresa@espb.gov.co

II. - Normatividad aplicada

Tipo de norma	Norma	Objeto de Ley	Aplicabilidad
Ley ordinaria	LEY 527 DE 1999	Por medio del cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, se establecen las entidades de certificación y se dictan otras dispisiciones.	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.
Decretos, Resoluciones y circulares de orden nacional	DECRETO 1122 DE 1999	Por el cual se dictan normas para suprimir trámites, facilitar la actividad de los ciudadanos, contribuir a la eficiencia y eficacia de la Administración Pública y fortalecer el principio de la buena fe.	Por el cual se dictan normas para suprimir trámites, facilitar la actividad de los ciudadanos, contribuir a la eficiencia y eficacia de la Administración Pública y fortalecer el principio de la buena fe.
Decretos, Resoluciones y circulares de orden nacional	DECRETO 1151 DE 2008	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones.	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones.
Ley ordinaria	LEY 1341 DE 2009	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.
Ley ordinaria	LEY 1581 DE 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.	Por la cual se dictan disposiciones generales para la protección de datos personales.

Decretos, Resoluciones y circulares de orden nacional	DECRETO 2693 DE 2012	Gestor Normativo Función Pública	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.
Ley ordinaria	LEY 1712 DE 2014	Por mediod ea cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones	Por medio de la cual se crea la ley de Transparencia y del Derecho de Acceso a la información pública nacional y se dictan otras Disposiciones.
Decretos, Resoluciones y circulares de orden nacional	DECRETO 2573 DE 2014		Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Decretos, Resoluciones y circulares de orden nacional	DECRETO 0103 DE 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decretos, Resoluciones y circulares de orden nacional	DECRETO 1078 DE 2015	Estrategia de Gobierno Digital	Por medio del cual se expide el Decreto Único Reglamentario del Sector de tecnología de la Información y las Comunicaciones.
Decretos, Resoluciones y circulares de orden nacional	DECRETO 415 DE 2016	Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública,	Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información

III. - Diagnostico del Plan

Descripción de diagnostico

Descrición del Problema	Objetivo solución
Insuficiente conocimiento de las políticas y normas de seguridad de la información, lo cual conlleva a actuaciones inadecuadas de los servidores que afectan los activos de información e informáticos.	Capacitar a los funcionarios de la ESPB en políticas y normas de seguridad de la información

Valoración Inicial

Probabilidad	Impacto	Categoria
Posible	Menor	Riesgo Bajo

Valoración Residual

Probabilidad	Impacto	Categoria
Improbable	Riesgo Bajo	Riesgo Bajo

Causa

Insuficiente socialización, y capacitación a los servidores públicos vinculados a la Empresa respecto de las políticas ynormas de seguridad.

Objetivo

socializar, y capacitar a los servidores públicos vinculados a la Empresa respecto de las políticas y normas de seguridad.

Consecuencias

Acciones no adecuadas en el tratamiento de los activos de información e informáticos que generan afectaciones.

Fines - Medios

políticas y normas de seguridad.

Descripción de diagnostico

Descrición del Problema	Objetivo solución
La red implementada no es la más adecuada para la estructura física de la Empresa y la cantidad de equipos informáticos y Las fallas en la señal de internet son constantes.	Elaborar de Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información

Valoración Inicial

Probabilidad	Impacto	Categoria
Posible	Menor	Riesgo Bajo

Valoración Residual

Probabilidad	Impacto	Categoria
Improbable	Riesgo Bajo	Riesgo Bajo

Causa

Falta de Implantar un modelo de red basado en cableado Estructurado.

Objetivo

Implantar un modelo de red basado en cableado Estructurado.

Consecuencias

Retraso en las actividades que desarrolla la Empresa.

Fines - Medios

Red de internet

Descripción de diagnostico

Descrición del Problema	Objetivo solución
No se están siguiendo protocolos y normas para garantizar la seguridad de la información en la Empresa.	Realizar seguimiento a los protocolos y normas para garantizar la seguridad de la información en la Empresa.

Valoración Inicial

Probabilidad	Impacto	Categoria
Posible	Menor	Riesgo Bajo

Valoración Residual

Probabilidad	Impacto	Categoria
Improbable	Riesgo Bajo	Riesgo Bajo

Causa	Objetivo
Insuficiente socialización, y capacitación a los servidores públicos vinculados a la Empresa respecto de las políticas y normas de seguridad.	socialización, y capacitación a los servidores públicos vinculados a la Empresa respecto de las políticas y normas de seguridad.

Consecuencias	Fines - Medios
Insuficiente transferencia de conocimiento y falta de capacitación que propician acciones no adecuadas en el tratamiento de los activos de información e informáticos que generan afectaciones.	Tratamiento de los activos de información e informáticos

Descripción de diagnostico

Descrición del Problema	Objetivo solución
La documentación e información en física está siendo archivada en sitios que no cumplen con todos los estándares para ello.	Diseñar una matriz de análisis de riesgos para detectar las amenazas y debilidades en los sistemas de información.

Valoración Inicial

Probabilidad	Impacto	Categoria
Posible	Menor	Riesgo Bajo

Valoración Residual

Probabilidad	Impacto	Categoria
Improbable	Riesgo Bajo	Riesgo Bajo

Causa	Objetivo
Falta de Digitalizar el 100% de la información contenida en Pape	Digitalizar el 100% de la información contenida en Pape

Consecuencias	Fines - Medios
El de la EPSB no puede identificar las amenazas y debilidades de la información.	Identificar las amenazas y debilidades de la información.

Empresa Departamental de Servicios Públicos de Boyacá S.A E.S.P.
Dirección: Cr 11 N° 20-54 Tel. 7445126-7449389-7441216
Web: www.espb.gov.co, correo institucional: empresa@espb.gov.co

Descripción de diagnostico

Descrición del Problema	Objetivo solución
Los funcionarios no realizan las suficientes copias de seguridad a la información producida en ejercicio de sus funciones.	Realizar las suficientes copias de seguridad a la información producida en ejercicio de sus funciones.

Valoración Inicial

Probabilidad	Impacto	Categoria
Posible	Menor	Riesgo Bajo

Valoración Residual

Probabilidad	Impacto	Categoria
Improbable	Riesgo Bajo	Riesgo Bajo

Causa	Objetivo
No existen instructivos que condiciones a los servidores públicos a realizar copias de seguridad periódicamente	Realizar instructivos que condiciones a los servidores públicos a realizar copias de seguridad periódicamente
Falta de capacitación al personal de la Empresa para el dominio de este tema.	Realizar Capacitación al personal de la Empresa para el dominio de este tema.
Falta de un servidor para almacenar las copias deseguridad.	Adquirir un servidor para almacenar las copias deseguridad.
Falta de un lugar para almacenamiento deinformación	Adquirir de un método y/o herramienta informática para almacenamiento deinformación
No existen cuentas de usuario	Crear cuentas de usuario con claves.

Consecuencias	Fines - Medios
Alta probabilidad que la entidad tenga una falta grave por no tener una Política de Seguridad.	Realizar identificación de riesgos con los líderes de procesos.

Descripción de diagnostico

Descrición del Problema	Objetivo solución
Valoración del riesgo residual.	Disminuir el riesgo de valoración residual.

Valoración Inicial

Probabilidad	Impacto	Categoria
Posible	Menor	Riesgo Bajo

Valoración Residual

Probabilidad	Impacto	Categoria
Improbable	Riesgo Bajo	Riesgo Bajo

Causa	Objetivo
Falta de formulación y ejecución de la Política de Seguridad	Disminuir el riesgo de valoración residual.
Incremento de la vulnerabilidad de las herramientas informáticas en la entidad.	Proteger la información de la entidad

Consecuencias	Fines - Medios
Incremento del riesgo de valoración residual.	Formulación y ejecución de la Política de Seguridad.
Fuga información	Proteger la información confidencial de la entidad

Empresa Departamental de Servicios Públicos de Boyacá S.A E.S.P.
Dirección: Cr 11 N° 20-54 Tel. 7445126-7449389-7441216
Web: www.espb.gov.co, correo institucional: empresa@espb.gov.co

IV - Análisis de cierre de brechas

Nombre del Indicador: Aspectos organizativos de la seguridad de la información

Analisis Situacional: Las normas y políticas de seguridad de la información existente, no ha sido socializadas con todo el personal, razón por la cual, el incumplimiento de reglas básicas del cuidado tanto de equipos informáticos como de la información tanto digital como física.

Linea Base	Meta	Cant. a Realizar
0	1	1

Esfuerzo BAJO O DE MANTENIMIENTO

Impacto Medio

Tipo de meta Meta de Incremento

Nombre del Indicador: Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información

Analisis Situacional: La red de internet implementada no es la más adecuada teniendo en cuenta que la mayor parte de la empresa cuenta con conexión WIFI y la señal se torna débil o inoperante en algunas oficinas. La lentitud del servicio de internet y la perdida de señal afecta de manera directa la productividad.

Linea Base	Meta	Cant. a Realizar
0	100	100

Esfuerzo BAJO O DE MANTENIMIENTO

Impacto Alto

Tipo de meta Meta de Incremento

Nombre del Indicador: Elaboración de matriz de riesgos

Analisis Situacional: Los documentos físicos que se administran en la Empresa no se han digitalizado en su totalidad, por lo tanto, están expuestos a pérdidas y daños físicos, entre otras cosas, dado que los sitios de almacenamiento en las oficinas no son lo suficientemente adecuados.
Los procedimientos de copias de seguridad en la Empresa no son lo suficientemente efectivos.
No existe un plan de continuidad del negocio que permita reanudar las operaciones normales durante o después de interrupciones significativas a las actividades de la Empresa (En caso de incendio o desastres naturales existen altas probabilidades de perder la información de los servidores).

Linea Base	Meta	Cant. a Realizar
1	1	1

Esfuerzo BAJO O DE MANTENIMIENTO

Impacto Alto

Tipo de meta Meta de Mantenimiento

Empresa Departamental de Servicios Públicos de Boyacá S.A E.S.P.
Dirección: Cr 11 N° 20-54 Tel. 7445126-7449389-7441216
Web: www.espb.gov.co, correo institucional: empresa@espb.gov.co

Nombre del Indicador: Seguridad en las telecomunicaciones

Analisis Situacional: No existe un historial de reportes de los procesos y/o mitigaciones de vulnerabilidad realizados por el personal de sistemas de la Empresa.

Linea Base	Meta	Cant. a Realizar
0	1	1

Esfuerzo BAJO O DE MANTENIMIENTO

Impacto Medio

Tipo de meta Meta de Incremento

Empresa Departamental de Servicios Públicos de Boyacá S.A E.S.P.
Dirección: Cr 11 N° 20-54 Tel. 7445126-7449389-7441216
Web: www.espb.gov.co, correo institucional: empresa@espb.gov.co

V. - Parte estrategica del plan

Sector	Acción	Trim 1	Trim 2	Trim 3	Trim 4	Ttl Prog.	Dependencia
Realizar inventario de activos de información	Actualizar, socializar e implementar un Manual depolíticas y normas de seguridad de la información en la Empresa.			1	1	2	SECRETARIA GENERAL
Elaborar alcance del Plan del Tratamiento de Riesgos de Seguridad y Privacidad de la información	Mejorar y mantener la capacidad en el cableado Estructurado.			1	1	2	SECRETARIA GENERAL
Realizar identificación de riesgos con los líderes de proceso	Realizar socialización, y capacitación a los servidores públicos vinculados a la Empresa respecto de las políticas y normas de seguridad.		1		1	2	SECRETARIA GENERAL
Matriz de Valoración de Activos y Análisis de Riesgos de Seguridad de la Información	Apoyo en la seguridad de la información digitalizada por parte de archivo			1	1	2	SECRETARIA GENERAL
Valoración del riesgo residual	Crear un instructivo de Copias de seguridad.			1		1	SECRETARIA GENERAL
Valoración del riesgo residual	Capacitar al personal de la Empresa para el dominio de este tema.		1		1	2	SECRETARIA GENERAL
Valoración del riesgo residual	Adquirir un servidor para almacenar las copias deseguridad.				1	1	SECRETARIA GENERAL
Valoración del riesgo residual	Adquisición de una nube para almacenamiento deinformación				1	1	SECRETARIA GENERAL
Valoración del riesgo residual	Crear cuentas de usuario con claves.	1	1			2	SECRETARIA GENERAL
Valoración del riesgo residual	Implementar acciones para controlar y proteger la información que transite dentro y fuera de la entidad.			1	1	2	SECRETARIA GENERAL

Valoración del riesgo residual	Contratar servicios profesionales para actualización, antivirus y seguridad para los equipos informáticos de la entidad.	1	1			2	SECRETARIA GENERAL

Elaboró DIEGO ALEJANDRO MORENO MANCILLA
Revisó ELIS ALEXANDER MORENO SALAMANCA
Aprobó LUZ MARIETHA AVILA FERNANDEZ

Empresa Departamental de Servicios Públicos de Boyacá S.A E.S.P.
Dirección: Cr 11 N° 20-54 Tel. 7445126-7449389-7441216
Web: www.espb.gov.co, correo institucional: empresa@espb.gov.co