Código			Política	
09-09.2-P-001-v.1			Política de Seguridad de la Información	
Fecha de emisión				
17	07	2015		

Elaborado por:	Revisado por:	Aprobado por:
Yezid Ospina Piñeros – Líder de Seguridad de la Información (E) – Gerencia Implementación de la Estrategia	Katerine Llanos Orozco – Líder SIG (E) – Gerencia Implementación de la Estrategia	Natalia Gutiérrez Leal – Gerente Implementación de la Estrategia Yezid Ospina Piñeros – Líder de Seguridad de la Información (E) – Gerencia Implementación de la Estrategia Jenny Elizabeth Caipe Balcazar – Oficial de Seguridad – Vicepresidencia de Infraestructura Oscar Javier Malaver Olmos – Oficial de Seguridad (E) – Vicepresidencia de Informática

Objetivo: Definir las intenciones globales y orientación de ETB relativas a la seguridad de la información tal y como se expresan formalmente por la alta dirección.

Alcance: Dirigida a todos los empleados, contratistas y proveedores de ETB

Definiciones:

Acceso: Es la capacidad de disponer de una información que ya existe dentro de un sistema informático (fichero, memoria, etc.) y que es posible acceder a ésta, continuando una secuencia fija y predeterminada de operaciones como también a partir de una clave, independientemente de las anteriores operaciones.

Activo de información: Para ETB los activos corresponden a los objetos materiales o intangibles asociados con la información y que son requeridos para la operación de las actividades de los negocios.

Alteración: Es un tipo de delito informático mediante el cual se puede realizar fraude introduciendo, cambiando o borrando datos informáticos o la interferencia de sistemas informáticos.

Archivo: Es uno o más conjuntos de documentos, sea cual fuere su fecha, su forma y soporte material, acumulados en un proceso natural por una persona o institución pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información para la persona o institución que los produce, para los ciudadanos, o para servir como fuentes de historia.

USO INTERNO

Bases de datos: Es una colección de información organizada de forma que un programa de ordenador pueda seleccionar rápidamente los fragmentos de datos que necesite. Una base de datos es un sistema de archivos electrónico. Las bases de datos tradicionales se organizan por campos, registros y archivos. Un campo es una pieza única de información; un registro es un sistema completo de campos; y un archivo es una colección de registros.

Cifrar: Es la codificación del contenido de un mensaje o archivo para que llegue solamente a la persona autorizada a recibirlo.

Código malicioso: Programas potencialmente peligrosos diseñados para dañar los sistemas y los datos, o modificarlos para que funcionen de manera incorrecta.

Confidencialidad de la Información: Se refiere a la preservación de las restricciones o limitantes que ETB, sus entes reguladores y sus obligaciones con los clientes han fijado para autorizar el acceso y la divulgación, así como los medios para la protección de la intimidad personal y propiedad de la información.

Continuidad de negocio: (Inglés: Business Continuity). Incluye la planificación para asegurar la continuidad de las funciones críticas de un negocio en la eventualidad de una falla o desastre. Este tipo de planificación abarca aspectos claves de la operación tales como personal, facilidades, comunicaciones, y cambio de controles. Un plan de continuidad de negocio es inclusive de un Plan de Recuperación de Desastre para la recuperación de infraestructura tecnológica.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Correo electrónico: Es una herramienta de comunicación que permite intercambiar mensajes de texto y archivos adjuntos entre los equipos de la red de datos y entre estos e Internet.

Cuenta de usuario de una aplicación: Se asigna a un usuario para tener acceso a un sistema de aplicación (aplicativo). Tiene un nombre de usuario,una contraseña y atributos.

USO INTERNO

Declaración de aplicabilidad: (Inglés: Statement of Applicability; SOA). Documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.

Derechos de autor: Entendida en este contexto como Propiedad Industrial, hace referencia a la protección de los intereses de los creadores al ofrecerles ventajas en relación con sus creaciones. La entidad nacional delegada para la administración de la Propiedad Industrial en Colombia es la Superintendencia de Industria y Comercio a través de la Delegatura para la Propiedad Industrial. Esta entidad cuenta con la Oficina de Servicio al Consumidor y Apoyo Empresarial, OSCAE, quien administra y coordina las actividades de divulgación y formación en temas de Propiedad Industrial. La Oficina tiene entre sus funciones diseñar y promover los mecanismos y herramientas para la divulgación, promoción y fomento de las funciones, trámites y servicios institucionales.

Directiva o directriz: Una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

Disponibilidad de la información: Acceso oportuno y confiable del uso de la información de cada una de las unidades organizacionales de ETB autorizadas.

Divulgación: En este contexto, hace referencia a la distribución no autorizada de datos a personas no autorizadas.

Documento: Es cualquier unidad en la cual se registra información, independiente del tipo de soporte en el que se encuentre (papel, cintas y discos magnéticos, películas, fotografías, etc.) el cual puede ser modificado y controlado por técnica de versiones.

File Server: Repositorio de información asignado a un área o proceso para guardar información, este sitio debe tener controles de ingreso de escritura, modificación o eliminación.

Gestión de claves: (Inglés: Key management). Controles referidos a la gestión de claves criptográficas.

Gestión de incidentes de seguridad de la información: (Inglés: Information security incident management). Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

USO INTERNO

Gestión documental: Son las actividades administrativas y técnicas que propenden por la planificación, manejo y organización de la información producida y recibida por las entidades desde que se produce o recibe hasta su disposición final.

Incidente de seguridad de la información: (Inglés: Information security incident). Evento único o serie de eventos de seguridad de la información inesperados o no deseados que comprometen o poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Infraestructura: Es el conjunto de recursos tecnológicos, hardware y software que permite la optimización de los procesos que soportan los servicios ofrecidos a nuestros clientes.

Integridad de la Información: La protección contra la modificación no autorizada, exactitud o completitud de toda información que pertenezca a los negocios de ETB o sus transversales.

Internet: Internet es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial. Los dispositivos que crean o reciben una solicitud o mensaje a través de ella son identificados por direcciones IP. Cada dirección IP utiliza un único conjunto de caracteres hexadecimales para identificar una red, una subred (si procede) y un dispositivo dentro de la red. Estos dispositivos pueden ser altamente vulnerados si no se cuentan con los controles pertinentes.

Intranet: Es una red de computadores limitada al interior de una organización o área específica la cual presta servicios similares a los de Internet. Para ETB, es un sistema de comunicación interactivo mediante el cual se puede emitir, recibir y compartir información de interés general para los trabajadores.

Medios de almacenamiento extraíbles: Medios para guardar y portar información de forma electrónica tales como disquetes, CD's, DVD's, discos ZIP, discos ópticos, discos duros externos, memoria digital USB, etc.

Periférico: Elemento o dispositivo del computador que no hace parte de la unidad central, tales como el monitor, mouse, teclado, parlantes, impresora, escáner, unidades de almacenamiento, etc.

USO INTERNO

Plan de recuperación de desastres: (Inglés: Disaster Recovery Plan - DRP). Es parte de un plan mayor de Continuidad de Negocios que incluye los procesos y soluciones con miras a restaurar aplicaciones críticas, información, hardware, comunicaciones y redes y otras infraestructuras propias de sistemas de información y tecnología.

Propietario del riesgo: (Inglés: Risk owner). Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.

Pruebas de penetración: Su principal propósito detectar vulnerabilidades que resultan de fallas de software, configuraciones inapropiadas, etc. Se puede realizar de forma remota o local y se ejecutan las pruebas tal y como lo intentaría un intruso con propósitos adversos para la organización.

Publicar: Es el acto mediante el cual se publica información, esta puede ser pública, interna, restringida y reservada.

Red: Es un sistema complejo soportado por una infraestructura tecnológica tal que permite ofrecer los servicios de telecomunicaciones a nuestros clientes. Se caracteriza porque puede ser gestionado y monitoreado de manera que pueda operar bajo las necesidades requeridas para el servicio.

Seguridad de la Información: La seguridad de la información significa la protección de la información y los sistemas de información del acceso, la divulgación, la alteración y la modificación o destrucción no autorizados. La gestión de la seguridad de la información se apoya en el cumplimiento de tres criterios:

1. La confidencialidad
2. La integridad y
3. La disponibilidad.

Sistema operativo: Programa de computador que organiza y gestiona todas las actividades que sobre él se ejecutan. Algunos sistemas operativos son Windows, Unix y Linux.

Software libre: Es software donde los usuarios tienen la libertad para ejecutar, copiar, distribuir, estudiar, modificar o mejorar el software. Este tipo de software debe ser autorizado por las áreas de Tecnología e Infraestructura.

Spam: Se denomina correo electrónico basura (en inglés también conocido como *junk-mail* o s*pam*) a una cierta forma de inundar la Internet con muchas copias (incluso millones) del mismo mensaje.

USO INTERNO

Teletrabajo: Una forma de organización laboral, consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información para el contacto entre el trabajador y ETB, sin requerirse la presencia física del trabajador en un sitio específico.

Transversales: Son los procesos que se encargan de apoyar al negocio en temas estratégicos, administrativos y de operación.

USB (Universal Serial Bus): Puerto Serial Universal del computador al cual se pueden conectar los periféricos.

Unidad de Conservación: Medio utilizado para archivar la documentación.

VPN: Es una tecnología que permite la extensión de una red privada como la de ETB en un espacio de red publico pero protegido por un canal virtual. Para los negocios es de vital importancia debido a las tareas adicionales que se tienen que hacer fuera del horario laboral, para teletrabajo y zonas en las que no hay un canal asignado.

Vulnerabilidad: (Inglés: Vulnerability). Debilidad de un activo o control que puede ser explotada por una o más amenazas.

USO INTERNO

Política:

ETB gestiona la integridad, disponibilidad y confidencialidad requerida de la información y sus procesos relacionados, los sistemas, redes y el personal involucrado en su operación, manipulación y protección, debido a que son activos productivos esenciales e imprescindibles para el desarrollo del objeto central del negocio. En ese sentido da prioridad a la protección de los activos de la información crítica del negocio en general y en particular a la de los servicios soportados por los Data Center.

Todos los empleados, contratistas y proveedores son responsables del cumplimiento de las políticas y procedimientos de seguridad establecidos en la organización y de postular riesgos, ejecutar controles y gestionar incidentes de seguridad de la información sobre los activos de información que les sean pertinentes de acuerdo a su responsabilidad. Todo lo anterior bajo la orientación metodológica y seguimiento del equipo de gestión de seguridad de la información corporativo.

Para lograr la coordinación, ejecución y control de las actividades mencionadas, ETB se organiza en los siguientes frentes de seguridad de la información, para los cuales se deben planear las inversiones necesarias y desarrollar las competencias de las personas claves y de quienes los sustituirán en caso de ausencia:

- Responsabilidad de la alta dirección

- Necesidades y expectativas de partes interesadas

- Recursos humanos

- Operación tecnológica

- Seguridad física y ambiental

- Continuidad del negocio

- Obligaciones legales y contractuales

Estos frentes deben responder prioritariamente y según corresponda, por:

- La protección de activos de información que intervienen en la efectividad de las ventas, la gestión de la facturación, el aseguramiento de los ingresos, la experiencia del cliente, el retorno de las inversiones y la gestión de programas y proyectos.

- La protección de los intereses de la organización preservando la seguridad de la información antes, duarte y al finalizar los contratos de trabajo con los empleados, y

USO INTERNO

- La comunicación efectiva a nuestros clientes corporativos actuales y potenciales sobre los beneficios que les genera una ETB con un SGSI implementado

Las acciones señaladas deben ser continuamente mantenidas y mejoradas sobre la base metodológica de las normas ISO 27001:2013 e ISO 27002:2013, aplicable bajo los lineamientos del Modelo Integrado de Gestión Empresarial, la Política del Sistema Integrado de Gestión de la organización y los acuerdos interinstitucionales e interempresariales pactados por ETB y en línea con las disposiciones vigentes respecto a delitos informáticos, bancos de datos, bases de datos, datos personales y demás obligaciones legales y regulatorias aplicables.

Control de Cambios:

Versión	Descripción del Cambio	Fecha del Cambio
1.0	Documento inicial	17/07/2015

USO INTERNO