Logo de la empresa

Políticas de seguridad de la información

Empresa

Mes – Año

Aviso legal

Control de versiones del documento

Versión	Fecha	Creada por	Descripción
1.0	Abril 10 de 2014	Héctor Vargas	Creación del documento

Contenido

Introducción

La política de seguridad es una declaración ética, responsables y de estricto cumplimiento en toda la organización, la cual es desplegada a través de las diferentes guías y procedimientos, procurando que los riesgos sean tratados adecuadamente.

Objetivo general

Entender que la información en toda la organización debe ser protegida, manteniendo los niveles óptimos de seguridad, permitiendo velar porque dicha información (sea propia y/o de terceros) se le conserve la confidencialidad, integridad y disponibilidad.

Objetivo específico

1. *Indicar que la información propia o de terceros sobre las redes de telecomunicaciones y sistemas de información es uno de los activos más importantes a proteger, la cual debe resguardarse con los mecanismos más óptimos que preserven la confidencialidad, integridad y disponibilidad de la información.*
2. *Desplegar la política y todos sus lineamientos de seguridad a través del Sistema de Gestión de Seguridad de la Información.*
3. *Definir los roles y responsabilidades de todos las personas y grupos de interés, así mismo realizar la respectiva comunicación y divulgación.*
4. *Adoptar, promover e implementar una metodología para la gestión de riesgos para las plataformas tecnológicas como mecanismo único de la empresa para la toma de decisiones, con ello, ejecutar la implementación de contramedida, mitigando los riesgos en las redes y sistemas de información hasta un nivel aceptable por la alta dirección.*
5. *Establecer los mecanismos legales y/o sancionatorios frente a la violación de alguna política de seguridad.*

Alcance

La política de seguridad de la información aplica a cualquier información de la empresa y que esté sobre las redes de comunicaciones y sistemas de información que apoyan los servicios al segmento de hogares, que sea propia o de terceros (clientes, proveedores y contratistas) y que esté en custodia (almacenada o en tránsito).

Ésta política va dirigida hacia los empleados y contratistas que tengan contacto o uso de las tecnologías de información y comunicaciones que hacen parte del SGSI.

Sanción y Cumplimiento

Tanto la política de seguridad, sus lineamientos, guías y procedimientos son de estricto cumplimiento, cada empleado y tercero debe reconocer los riesgos a que está expuesta la

información, así mismo conocer, interiorizar y cumplir su rol dentro del Sistema de Gestión de Seguridad de la Información limitado por el alcance.

Cualquier incumplimiento de la política de seguridad y el modelo que la despliega, podrá generar sanciones administrativas, disciplinarias y/o penales (en términos de la ley Colombiana).

Descripción de políticas

Las políticas son una descripción del "que", el cual se despliega a través de los lineamientos, guías y procedimientos. A continuación se entregan las diferentes políticas de seguridad:

Política 1: Sobre el SGSI

El Sistema de Gestión de Seguridad de la información – SGSI debe ser mantenido y actualizado de manera periódica, considerando:

- *Cumpla con los requisitos del negocio, obligaciones con los socios y las legales.*
- *Establezca una metodología donde se evalué, califique y traten periódicamente los riesgos.*
- *Se debe hacer revisión periódica de las políticas de seguridad y declaración de aplicabilidad, como mínimo cada año.*
- *Revisiones periódicas (al menos cada año) por parte de los auditores internos de manera independiente, validando las acciones preventivas, correctivas y de mejora que surjan para los sistemas de información y elementos tecnológicos.*
- *Conformación del comité de seguridad y/o de riesgos, declarando sus funciones y responsabilidades.*
- *Asegurar la capacitación, sensibilización, formación y toma de conciencia para los empleados, jefes y oficiales de seguridad.*
- *Participar en diferentes grupos de interés, así como establecer contactos con las autoridades.*

Política 2: Control de Acceso

Todos y cada uno de los sistemas informáticos y plataformas tecnológicas debe contar con un adecuado control de acceso, en la medida que:

- *Se tengan procedimientos para autorizar y revocar privilegios.*
- *Se tenga separación de funciones en el acceso*
- *Se tengan auditorios y registros de seguimientos en los sistemas de información y comunicaciones.*
- *Se cuente con control para el acceso remoto y redes inalámbricas.*
- *Se cuente con controles de acceso hacia los sistemas de información, que surtan la identificación y autorización respectiva.*
- *Se protejan las contraseñas y sistemas de autenticación.*

- *Se haga gestión sobre todos los privilegios de usuarios y la respectiva actualización de procedimientos.*
- *Todos los usuarios deben tener una identificación única, se prohíbe el préstamo de cualquier elemento de identificación y autenticación.*

Política 3: Gestión de los activos

Todos los activos de información que hagan parte del alcance de implementación, deben ser identificados, etiquetados e inventariados, para ello:

- *Se debe definir la propiedad de los activos.*
- *Se debe contar con mecanismos para la clasificación.*

Política 4: Seguridad sobre el talento humano

La organización debe tener procedimientos para el reclutamiento, selección y desvinculación del personal, para lo cual:

- *Se deben definir y mantener los roles y responsabilidades.*
- *Definir claramente las condiciones contractuales y de seguridad, incluyendo los acuerdos de confidencialidad.*
- *Entregar la debida identificación para el ingreso a los sistemas de información y revocar éstos cuando ya no se usen o la persona esté por fuera de la empresa.*
- *Se tengan procesos o un control disciplinario y/o administrativo que evalúen las faltas y den sanciones.*

Política 5: Capacitación y entrenamiento

Se deben tener planes de capacitación anual para los empleados y oficiales de seguridad, de modo que se eleven los niveles de sensibilización frente a la protección de la información.

Política 6: Manejo del riesgo

Se debe contar con una metodología de riesgos, para la identificación, análisis y evaluación, así como los mecanismos de tratamiento, para lo cual es necesario:

- *Formalizar la metodología general de riesgos para sistemas de información y plataformas tecnológicas.*
- *Definir los niveles aceptables de los riesgos por parte de la alta dirección.*
- *Definir los roles y responsabilidades frente al riesgos.*
- *General mapas de riesgos de manera periódica, al menos cada año.*

Política 7: Seguridad física y ambiental

Se deben tener elementos de protección física que resguardes los centros de datos y las redes en general:

- *Se debe tener control de acceso físico a las instalaciones, que proteja contra amenazas internas y externas.*

- *Identificación del personal propio, proveedores y contratistas.*
- *Se debe medir las variables ambientales de los centros de cómputo como humedad y temperatura.*
- *Seguridad para los equipos informáticos que estén por fuera de las instalaciones.*
- *Implementar y mantener sistemas de video vigilancia en todas las zonas.*

Política 8: Gestión de las redes y los sistemas informáticos

Todas las redes de computadores, de telecomunicaciones, sistemas informáticos, dispositivos móviles y sistemas de información deben contar con la protección adecuada ante ataques, fuga de información y accesos no autorizados:

- *Se debe contar con sistemas antivirus, anti-spam y anti-espías en todos los sistemas.*
- *Se debe tener ambientes de procesamientos como desarrollo, testing y producción.*
- *Se debe tener un sistema de monitoreo de alertas de seguridad en toda la red y sistemas.*
- *Todos los servicios y acceso a la red deben estar controlados, para lo cual se debe implementar control de acceso en la red y sistemas de información.*
- *Los sistemas de red deben tener las configuraciones de seguridad (hardening) antes de estar en producción y tener servicio.*

Política 9: Sistemas de respaldo y recuperación

Se deben tener sistemas de respaldo y procedimientos de recuperación, protección de medios de almacenamiento y control de acceso hacia las librerías y cintas. Todos los medios removibles o de almacenamiento que no se usen se les debe eliminar sus información de modo seguro (sin recuperación).

- *Tanto las bases de datos, aplicaciones como medios de almacenamiento deben ser respaldados de forma periódica.*
- *Se debe programar al menos una vez al año una prueba de recuperación de información.*

Política 10: Comercio electrónico

Para todos los sistemas de comercio electrónico (transporte, bases de datos y aplicaciones Web) se debe proveer mecanismos de autenticación, autorización, identificación y no repudio a través de cifrado (criptografía):

- *Se debe implementar y mantener un sistema PKI (infraestructura de clave pública).*
- *Las firmas digitales y certificados deben estar resguardados de manera óptima, así como las llaves de cifrado.*
- *Los datos en las bases de datos acorde a su nivel de criticidad deben estar cifrados.*

- *Se debe hacer pruebas de seguridad (penetration testing y análisis de vulnerabilidades) de manera periódica, al menos 2 veces al año, para las Bases de datos y aplicaciones Web.*
- *Se debe configurar los diferentes registros de auditoría y monitoreo de transacciones en línea.*

Política 11: Desarrollo de software y soluciones

Se debe tener un proceso de desarrollo de software que de garantía que las diferentes aplicaciones tienen todos los elementos de seguridad que eviten ataques informáticos, tales como SQL Injection y Cross-site-scripting (XSS).

- *Todas las soluciones deben pasar por los ambientes de pruebas, testing y producción.*
- *Se deben hacer pruebas funcionales y de seguridad.*
- *Se debe tener protección contra modificación no autorizada del código fuente.*

Política 12: Gestión de los incidentes de seguridad

Se debe contar con un proceso para la atención, detección, control, tratamiento y respuesta de incidentes de seguridad:

- *Cada incidente debe alimentar las fuentes de los riesgos, con sus respectivos tratamientos.*
- *Se debe tener un equipo de respuesta a incidentes y/o un CSIRT.*
- *Todos los eventos de seguridad deben ser registrados y monitoreados hasta la solución final.*
- *Se debe contar con un procedimiento para la investigación forense.*

Política 13: Planes de recuperación ante desastres

Se debe contar con planes para la recuperación ante desastres documentados, oficializados, divulgados y aprobados, de modo que todo el personal este enterado de las acciones técnicas a realizar en caso de fallo de la red, bases de datos, sistema operativo y aplicaciones en general. Todos los planes de recuperación ante desastres deben tener un análisis de riesgos previo (BIA- Business Impact Análisis).

Política 14: Sobre la documentación

Toda la documentación y registros en general deben protegerse acorde a su criticidad:

- *Se debe emplear las metodologías para la clasificación de información.*
- *Si la información es crítica, ésta se debe proteger a través de elementos criptográficos.*
- *Los registros y documentos digitales deben tener control de acceso.*

1. *Todos los documentos deben tener control de cambios y versiones.*