1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 29 de noviembre de 2016 por el Comité de Calidad y Seguridad. Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

Este texto anula el anterior, que fue aprobado el día 15 de noviembre de 2010 por el Comité de Dirección.

2. INTRODUCCIÓN

TREVENQUE depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos dentro del alcance deben aplicar las medidas mínimas de seguridad exigidas tanto por la norma ISO 27001:2014 como por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los departamentos dentro del alcance deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del Esquema Nacional de Seguridad (ENS) y con el apartado 16.1 de la norma ISO 27002:2015.

2.1. PREVENCIÓN

Todo TREVENQUE y muy en particular los departamentos dentro del alcance deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello los departamentos deben implementar las medidas mínimas de seguridad determinadas por el ENS y por las normas ISO 27001 e ISO 27002, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos dentro del alcance deben:

- Autorizar los activos antes de entrar en operación.

- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

2.2. DETECCIÓN

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS y en los controles sobre Seguridad de las Operaciones de la norma ISO 27002.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

2.3. RESPUESTA

Los departamentos dentro del alcance deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar puntos de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos.
- Establecer protocolos para el intercambio de información relacionada con el incidente.

2.4. RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, los departamentos dentro del alcance deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

3. ALCANCE

En el caso de la norma ISO 27001, esta política se aplica a los sistemas de información que soportan los servicios de:

a) Alojamiento físico de servidores de terceros;
b) Provisión y mantenimiento de servidores privados virtuales;
c) Provisión y mantenimiento de servidores dedicados;
d) Gestión de back up
e) Coubicación de antenas de telecomunicación

de acuerdo a la declaración de aplicabilidad vigente.

Por otro lado, de cara al Esquema Nacional de Seguridad el alcance es: Los sistemas de información que soportan los servicios de provisión y mantenimiento de máquinas virtuales y alojamiento de servidores de terceros.

El alcance de la norma ISO 27001 engloba por lo tanto el alcance del ENS.

4. MISIÓN

La misión de TREVENQUE es acercar la tecnología a la empresa, entendida esta en un sentido amplio (empresa como cualquier organización prestadora de servicios, sean privados o públicos).

5. MARCO NORMATIVO

TREVENQUE se esfuerza en cumplir con toda la legislación aplicable a su actividad, ya sea de carácter general (Código de Comercio, Código Civil, etc.) o específico, como por ejemplo la siguiente:

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

6. ORGANIZACIÓN DE LA SEGURIDAD

6.1. COMITÉS: FUNCIONES Y RESPONSABILIDADES

El Comité de Calidad y Seguridad estará formado por el Director Financiero y por el Coordinador del CCA, que podrán estar auxiliados de manera permanente o esporádica por consultores externos.

El Secretario del Comité de Calidad y Seguridad será el Coordinador del CCA (o persona en quien delegue) y tendrá como funciones la preparación de las reuniones, la difusión de sus resultados y el seguimiento de los acuerdos alcanzados.

El Comité de Calidad y Seguridad reportará al Comité de Dirección.

El Comité de Calidad y Seguridad, por lo que se refiere al SGSI de Trevenque y al cumplimiento de lo dispuesto en el ENS, tendrá las siguientes funciones:

a) Coordinar y aprobar las acciones en materia de seguridad de la información;

b) Impulsar la cultura en seguridad de la información;
c) Participar en la categorización de los sistemas y el análisis de riesgos;
d) Revisar y aprobar la documentación relacionada con la seguridad del sistema;
e) Resolver discrepancias y problemas que puedan surgir en la gestión de la seguridad.

6.2. ROLES: FUNCIONES Y RESPONSABILIDADES

El Director Financiero de Trevenque asume la función de Responsable del Sistema de Seguridad.

Las funciones del Responsable de Seguridad de la Información son las siguientes:

- Mantener el nivel adecuado de seguridad de la información manejada y de los servicios prestados por los sistemas.
- Realizar o promover las auditorías periódicas a las que obliga la norma ISO 27001 y el ENS para verificar el cumplimiento de los requisitos del mismo.
- Gestionar o promover la formación y concienciación en materia de seguridad TIC.
- Comprobar que las medidas de seguridad existente son las adecuadas para las necesidades de la entidad, con la colaboración del Coordinador del CCA.
- Revisar, completar y aprobar toda la documentación relacionada con la seguridad del sistema, con el auxilio del resto del Comité de Calidad y Seguridad.

Por su parte, las responsabilidades del Coordinador del CCA son estas:

- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución, emitiendo informes periódicos sobre los más relevantes al Comité.
- Coordinar el Comité de Seguridad Técnica.
- Auxiliar al Responsable del SGSI en el desarrollo de su función.

6.3. PROCEDIMIENTOS DE DESIGNACIÓN

El Responsable de Seguridad de la Información será nombrado por el Comité de Dirección a propuesta del Comité de Calidad y Seguridad. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

A su vez, la designación del Coordinador del CCA es competencia del Director Técnico.

6.4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Calidad y Seguridad la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será

aprobada por el Comité de Dirección y difundida para que la conozcan todas las partes afectadas.

7. DATOS DE CARÁCTER PERSONAL

TREVENQUE trata datos de carácter personal. El documento de seguridad, al que tendrán acceso sólo las personas autorizadas, recoge los ficheros afectados y los responsables correspondientes. Todos los sistemas de información de TREVENQUE se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

8. GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se revisará:

- regularmente, al menos una vez al año;
- cuando cambie sustancialmente la información manejada;
- cuando cambien los servicios prestados dentro del alcance;
- cuando ocurra un incidente muy grave de seguridad;
- cuando se reporten vulnerabilidades muy graves.

Los análisis de riesgos se llevarán a cabo siguiendo siempre una misma metodología, que estará procedimentada.

9. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información complementa las políticas de TREVENQUE en materia de Calidad y Medio Ambiente.

La Política de Seguridad se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La normativa de seguridad estará disponible en la web de TREVENQUE.

10. OBLIGACIONES DEL PERSONAL

Todos los trabajadores de TREVENQUE tienen la obligación de conocer esta Política de Seguridad de la Información, que es de obligado cumplimiento dentro del alcance identificado, siendo responsabilidad del Comité de Calidad y Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Se establecerá un programa de concienciación continua para atender a todos los miembros de TREVENQUE, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC dentro del alcance recibirán formación para el manejo seguro de los sistemas en la medida en que la

necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

11. TERCERAS PARTES

Las terceras partes relacionadas con TREVENQUE, dentro del alcance, firman con la empresa un acuerdo que protege la información intercambiada.

Cuando TREVENQUE utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha Política, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.