INTRODUCCIÓN

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración de Inspectoría Santa María Mazzarello con respecto a la protección de los activos de información (los empleados, contratistas, terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

OBJETIVO

Inspectoría Santa María Mazzarello, para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Minimizar el riesgo de los procesos misionales de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los empleados, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información a los empleados, terceros, practicantes y clientes de la INSPECTORÍA SANTA MARÍA MAZZARELLO.
- Garantizar la continuidad del negocio frente a incidentes.

ALCANCE/APLICABILIDAD

Esta política aplica a toda la sede administrativa, sus empleados, contratistas y terceros de la Inspectoría Santa María Mazzarello.

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

Las excepciones al cumplimiento de las políticas de seguridad de la información serán autorizadas única y exclusivamente por la ecónoma inspectorial del momento, cuando se considere que su impacto es negativo para la continuidad de los procesos o logro de los objetivos institucionales, y deberán ser documentadas formalmente.

Las políticas de seguridad informática serán objeto de evaluación anual, aplicando mecanismos de autocontrol y autoevaluación, para garantizar el mejoramiento continuo.

POLÍTICAS

A continuación, se establecen las políticas de seguridad que soportan el SGSI de la Inspectoría Santa María Mazzarello

1. **Política Confidencialidad de la información**

Todos los miembros de la organización que manipulen información en cumplimiento de sus funciones, y terceros tales como proveedores de redes y servicios de telecomunicaciones, personal de entes de control entre otros, deben aceptar acuerdos de uso y manejo de la información reservada o confidencial definida por la Entidad*, donde se comprometen a no revelar, modificar, dañar, eliminar o usar inapropiadamente la información confidencial a la que tengan acceso, so pena de las investigaciones penales y disciplinarias a las que haya lugar.

Controles

La Entidad identificará la información considerada clasificada o reservada, índice que deberá ser divulgada de conformidad con la normatividad vigente.

La Entidad establecerá controles para el intercambio de información con terceros para asegurar la reserva e integridad de la misma y que se respeten los derechos de autor.

La información clasificada reservada/confidencial solo se debe almacenar en las unidades de red de la Entidad con las respectivas restricciones para que su acceso exclusivo a personal específico.

2. **Política Usuarios, roles y permisos.**

Las tareas realizadas por los usuarios en cada uno de los sistemas de información de la Inspectoría Santa María Mazzarello, serán controladas por medio de la creación de cuentas de usuario a los cuales se les controlarán los privilegios de acceso, modificación y eliminación, de conformidad con los roles y perfiles que requiera el usuario.

En el caso de retiro de personal, se deberá notificar de forma inmediata a través de un ticket para deshabilitar dicha cuenta el mismo día en que termina sus funciones. La cuenta estará deshabilitada durante 30 días, tiempo que una vez cumplido se procederá a la eliminación definitiva del usuario.

Controles

Cuando se requiera el acceso para un nuevo usuario en la red, deberá realizarse una solicitud a través de ticket, especificando: Nombre completo, rol, accesos a carpetas compartidas y privilegios de navegación a internet que deberá tener.

3. **Política de gestión de contraseñas.**

La vigencia del usuario y contraseñas a personal de contrato estará sujeta a la fecha de finalización del mismo, siendo responsabilidad de los jefes inmediatos reportar a la empresa encargada de la gestión de las cuentas, la novedad de retiro.

Se precisa que el control de acceso al sistema, se debe realizar por medio de Usuario único.

Se debe tener en la longitud de las contraseñas un mínimo de ocho caracteres y una longitud máxima de cuatrocientos cincuenta y seis (456) caracteres, siendo esta una combinación de Mayúsculas y minúsculas.

En caso de asignación contraseñas, no se divulgarán por medio de líneas telefónicas, se envían por correo electrónico, y el usuario debe cambiarla de manera inmediata al ingresar por primera vez al aplicativo.

Se precisa que las contraseñas nunca deben ser compartidas o reveladas a nadie más que al usuario autorizado. Hacerlo expone al usuario a responsabilizarse de acciones que otras personas hagan con su cuenta. Los usuarios serán responsables de la confidencialidad de las contraseñas y bajo ninguna circunstancia la darán a conocer a otras personas, o harán uso de contraseñas ajenas, ni de la opción de autoguardado de contraseñas.

Ante la posibilidad o sospecha de la pérdida de confidencialidad de la contraseña, esta debe ser cambiada de manera inmediata y reportado el evento al correo **asistencia@tcservices.co**.

Se precisa que todos los usuarios cambien periódicamente la contraseña en el sistema, mínimo cada 60 días.

Los intentos fallidos de acceso al sistema de información antes del límite de cinco intentos, despliegan un mensaje de advertencia indicando que el usuario no ha podido iniciar sesión debido a los datos de usuario o *password* son incorrectos. Cuando los intentos fallidos superan el máximo de cinco, se desplegará un mensaje de bloqueo de usuario, lo que implica que debe comunicarse con el administrador del sistema para el desbloqueo respectivo.

Controles

Para el cumplimiento de esto, las estaciones de trabajo del personal estarán bajo el dominio corporativo y se tendrán GPOs aplicadas para cada perfil que permita aplicar dichas restricciones.

4. **Política de recursos y herramientas tecnológicas.**

El personal nuevo que ingrese a la organización se le asignará un equipo con las características de hardware y software legal instalado, dependiendo a sus funciones; el cual al momento de la entrega el usuario deberá aceptar la responsabilidad del correcto manejo del mismo.

Cuando un usuario se retire de la Entidad, deberá devolver el equipo en las mismas condiciones que fue entregado una vez ingresado a la organización.

Controles

Cada usuario deberá diligenciar y firmar el documento “Acta entrega equipos” cuando reciba el equipo, aceptando y validando el estado del mismo. Este documento será digitalizado y almacenado en el servidor de red de la Entidad.

Una vez el usuario se retire de la organización diligenciará nuevamente el documento “Acta entrega equipos”, donde se corroborará el estado del dispositivo. Este documento será digitalizado y almacenado en el servidor de red de la Entidad.

5. **Política acceso a internet**

Los canales de acceso a internet de la Entidad no podrán ser usados para fines diferentes a los requeridos en el desarrollo de las actividades propias de los cargos. Esta restricción incluye el acceso a páginas con contenido pornográfico, terrorismo, juegos en línea y demás cuyo contenido no sea obligatorio para desarrollar las labores encomendadas al cargo.

No es permitido el uso de Internet para actividades ilegales o que atenten contra la ética y el buen nombre de la Inspectoría o de las personas.

Controles

Mediante el sistema de FlashStart se restringe en el router de internet el acceso a este tipo de contenido.

6. **Política de Antivirus**

Todos los equipos de la entidad deben tener instalado, en funcionamiento, actualizado y debidamente licenciado un antivirus, el cual será gestionado a través de una consola centralizada.

Controles

El antivirus se debe instalar con opción de actualización automática.

Está prohibido que los usuarios desinstalen el antivirus de su equipo, modifiquen o eliminen las configuraciones de seguridad que previenen la propagación de virus, ya que esta acción puede ocasionar riesgo total de contaminación de virus.

Los usuarios deben asegurarse que todos los medios de almacenamiento tanto internos como externos están libres de virus o software malicioso, mediante la ejecución del software antivirus autorizado.

Los usuarios que tengan conocimiento del alojamiento de un virus en su PC deben comunicar de manera inmediata a través del canal de Telegram o al correo **asistencia@tcservices.co**. para que le brinden el soporte técnico de erradicación del virus.

Todos los archivos anexos a los mensajes recibidos en el correo institucional, estarán sujetos al análisis del antivirus, y el destinatario final recibirá solo los que hayan sido exitosos.

7. **Pruebas de vulnerabilidad de la red**

En el año se deberán realizar una prueba de vulnerabilidad de la red externa o "*pentesting*" durante el mes de diciembre, a través de las cual se puedan identificar posibles fallas de seguridad, que correspondan a un riesgo de acceso a la red interna y a la información de la organización.

Controles

Se deberá contar con un informe ejecutivo y técnico de cada una de las pruebas de vulnerabilidad, con los resultados exitosos o no de intrusión y las mejoras a implementar.

8. **Política Acceso a Centro de Cómputo**

El acceso a esta área, donde se encuentran los servidores y equipos de infraestructura de conectividad y red estará limitado al personal técnico, y solo en los casos que sea estrictamente necesarios, como la revisión de problemas, mantenimientos o implementaciones nuevas.

Controles

El área del centro de cómputo debe estar cerrada bajo llave, la cual solo será prestada bajo autorización directa de la ecónoma inspectoral o contadora.

9. **Mantenimiento de la infraestructura**

Durante dos veces al año se realizará mantenimiento preventivo en los servidores.

Durante una vez al año se realizará mantenimiento preventivo en las estaciones de trabajo de la Entidad.

Controles

Se tendrá una hoja de vida de cada uno de los equipos, con un formato firmado por el usuario responsable del dispositivo una vez realizado el mantenimiento.

10. Política de Copias de respaldo

Se realizará una copia de seguridad diaria de las carpetas de Datos (que sirve de unidad de red) y las correspondientes al aplicativo SIIGO.

Controles

Se tienen notificaciones automáticas del estado de la copia de seguridad y se realizará cada dos meses una prueba de restauración de datos, aplicaciones o archivos.