Política de Seguridad de la Información

La información de la propiedad horizontal es un elemento valioso por lo que su integridad, disponibilidad, autenticidad, trazabilidad, protección, legalidad, fiabilidad y confidencialidad debe preservarse a lo largo de su tratamiento. El objetivo del presente documento es el de evitar o controlar daños o pérdidas de información relacionados con amenazas o incidentes.

1. Alcance. Esta política aplica a todo tipo de información y es de obligatoria observancia por parte del personal vinculado directa o indirectamente con la propiedad. Las violaciones a la seguridad comprometen al infractor con quien se podrán emprender acciones disciplinarias, civiles o penales, según corresponda.

2. Funcionario de Privacidad. Le corresponde al Administrador de la propiedad horizontal, salvo que se designe a otra persona, adelantar los siguientes procesos:

- Designar a las personas que pueden tratar información y definir niveles de acceso.
- Informar al personal a su cargo o a terceros sobre la política de seguridad.
- Si es del caso, asignar o solicitar activación o desactivación de claves de acceso para correos y/o documentos, procurar el correcto manejo de internet.

3. Comité de Seguridad de la Información. La propiedad horizontal podrá integrar el Comité con el Funcionario de Privacidad, quien lo presidirá, y los miembros del Consejo de Administración. Al Comité le compete tratar todos los asuntos relacionados con temas seguridad de la información y decidir sobre el curso de las acciones a tomar.

4. Objetivos Principales. Los principales objetivos en materia de seguridad:

- Proteger, preservar y administrar adecuadamente la información y los elementos a físicos y tecnológicos para el tratamiento de la información.
- Mantener la Política de Seguridad de la Información actualizada.
- Establecer directrices para la correcta identificación, análisis y evaluación de los riesgos y establecer responsabilidades para usuarios.

5. Seguridad Física y Tecnológica.

- El acceso a las instalaciones y equipos es controlado, restringido y seguro.

- Los archivos físicos, computadores y/o servidores que contengan información, así como otros elementos de comunicación se mantendrán en un ambiente seguro y protegidos con controles de acceso.

- Los computadores deben estar protegidos contra códigos maliciosos y se crearán copias de seguridad de manera periódica.

- Las personas vinculadas a la propiedad horizontal tienen la obligación de reportar al Funcionario de Privacidad cualquier incidente de seguridad a la mayor brevedad posible, con el fin de controlar la situación de forma eficaz.

- Todo incidente de seguridad debe tratarse en el Comité de Seguridad de la Información, si se integra, para que lo analice y tome las acciones pertinentes.

- El intercambio de Información con agentes externos debe estar aprobado por el administrador o quien la copropiedad designe.

- El uso responsable del internet y del correo electrónico es una obligación

- Se controlará la información a la que nuevos empleados pueden tener acceso. Cuando se desvinculen, se les solicitará la entrega de los elementos informáticos, copias de seguridad y, en todo caso, se asegurará de que no dispongan para su beneficio o el de terceros de información que conocieron en razón de sus labores.

- En caso de mantenimiento de equipos informáticos o cambio de los mismos, previamente se asegurará la información (mediante copias de respaldo) y, cuando se cambien o desechen equipos, se eliminará toda la información.

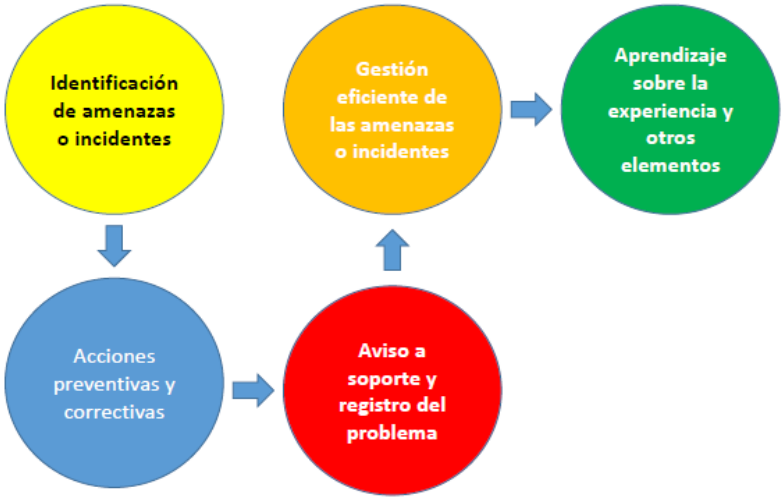
- El Funcionario de Privacidad realizará auditorías de los sistemas de información para revisar sus condiciones físicas y de desempeño.

- Cada usuario que trate datos tiene la obligación de verificar y asegurar que la información de la que hace uso sea confiable, veraz, certera, pertinente y se adapte a los formatos o lineamientos proporcionados por la propiedad horizontal.

- Cuando la información haya cumplido su vida útil o deba ser descartada o destruida, se seguirán los siguientes parámetros: (i) si se trata de documentos físicos, se debe romper o pasar por máquinas rasgadoras de papel y botarse en canecas dispuestas para tal fin; (ii) Si se trata de documentos electrónicos, se deben borrar dichos documentos de los respecticos archivos y eliminarlos también de la papelera. Así mismo, se deben eliminar de toda copia de respaldo.

- La presente política podrá actualizarse o mejorarse a partir de los incidentes o vulnerabilidades de seguridad que sean detectados.

6. Proceso en torno a la seguridad de la información. A continuación, se describe de manera gráfica el proceso en torno a la seguridad de la información



7. Herramientas de seguridad de la información. La propiedad horizontal ha identificado las posibles amenazas y el nivel daño impacto que las mismas podrían tener en caso de presentarse. Estos aspectos los ha decantado en dos matrices que, de manera gráfica, los describe. En la primera matriz se establecen los grados de posibilidad de ocurrencia de las amenazas y los niveles de daño, siendo 1 la calificación menos grave y 9 la más crítica, según se muestra a continuación:

Nivel De Daño	3	6	9
	2	4	6
	1	2	3
	Posibilidad de ocurrencia		

Lo anterior permite establecer los grados de alerta que se identifican en la siguiente Matriz de Riesgo de la Información.

MATRIZ DE RIESGO DE LA INFORMACIÓN								
	Actos Criminales				Eventos físicos			Negligencia
Amenazas	Virus	Hackeo	Hurto	Vandalismo	Incendio	Inundación	Corriente	imprudencia
Nivel de Daño	6	6	9	4	9	4	2	3
Unidades	Posibilidad de ocurrencia							
Portátiles	9	9	6	2	2	2	4	2
Computadores	9	9	3	1	1	1	3	2
Archivo físico	1	1	3	1	1	1	1	4
Administración	1	1	2	1	1	1	2	1
Finanzas	1	2	2	1	1	1	2	1
Personal	3	3	2	1	1	1	3	2

8. Acciones preventivas y correctivas. A continuación se indican las medidas preventivas que aplicarán para cada caso.

8.1. Virus informáticos. Los portátiles y computadores de escritorio estarán protegidos con software antivirus. Ante un evento de virus, la persona que lo detecte debe dar aviso inmediato al Funcionario de Privacidad y tomar las medidas correctivas del caso para contener el daño o potencial daño.

8.2. *Hackeo*. Los portátiles y computadores de escritorio destinados contarán con claves de acceso y estarán debidamente resguardados. Ante un evento de *Hackeo*, la persona que lo detecte avisará de inmediato al Funcionario de Privacidad y tomará las medidas para contener el daño real o potencial.

8.3. Hurto. Las instalaciones de la propiedad horizontal cuentan con niveles adecuados de seguridad en sus accesos de entrada. Así mismo, la recepción sirve de filtro de seguridad y limita el acceso de las personas. Cuando se saquen los computadores de la propiedad horizontal se incrementa el nivel de exposición de estos elementos a hurtos, extravíos y daños materiales, entre otros. En estos casos, el personal debe ser especialmente diligente en resguardar los equipos y responder por la integridad de los mismos. Ante un evento de hurto, la persona que lo detecte avisará de

inmediato al Funcionario de Privacidad. Si hay lugar a ello, se efectuará la respectiva denuncia ante las autoridades y se contactará a la compañía de seguros.

8.4. **Vandalismo.** Los equipos están resguardados en las instalaciones de la propiedad horizontal. Sin embargo, ante un evento de vandalismo, la persona que lo detecte avisará de inmediato al Funcionario de Privacidad para tomar las medidas correctivas del caso para contener el daño real o potencial. Así mimo, cuando haya lugar a ello, se debe efectuar la respectiva denuncia ante las autoridades y, si del caso, contactar a la compañía de seguros.

8.5. **Incendio.** Dada la naturaleza de las actividades de la propiedad horizontal y el lugar desde donde opera y /o realiza sus actividades, no se corre mayor riesgo por causa de incendio. Sin embargo, el lugar donde las instalaciones se encuentran ubicadas podrá tener sistemas de alarmas y equipos de prevención y extinción de fuego. En todo caso, el personal debe ser especialmente diligente en la prevención de cualquier tipo de incidentes. Ante un evento de incendio, la persona que lo detecte debe dar aviso inmediato al área de soporte correspondiente y tomar las medidas correctivas del caso para contener el daño o potencial daño. Así mimo, se debe contactar a los bomberos y a otras autoridades cuando corresponda.

8.6. **Inundación.** El riesgo de inundación es muy bajo. En todo caso, el personal debe ser diligente en la prevención de cualquier tipo de incidentes. Ante un evento de inundación, la persona que lo detecte debe dar aviso inmediato al área de soporte correspondiente y tomar las medidas correctivas del caso para contener el daño real o potencial. Así mimo, se debe contactar a los bomberos y a otras autoridades cuando corresponda.

8.7. **Corriente eléctrica.** Los equipos electrónicos pueden sufrir daños por cuenta de fluctuaciones en fluido eléctrico. En la medida de lo aconsejable se utilizarán reguladores de corriente para evitar incidentes. Ante un evento relacionado con el fluido eléctrico, la persona que lo detecte debe dar aviso inmediato al área de soporte correspondiente y tomar las medidas correctivas del caso para contener el daño o potencial daño.

8.8. **Imprudencia.** El personal debe dar el tratamiento adecuado a los equipos y utilizarlos según sus particulares propiedades y usos dentro de sus límites racionales. Ante un evento de imprudencia, la persona que lo cometa o detecte debe dar aviso inmediato al área de soporte correspondiente y tomar las medidas correctivas del caso para contener el daño o potencial daño.

9. **Confidencialidad.** Todo el personal vinculado directa o indirectamente a la propiedad horizontal debe ser instruido acerca del compromiso expreso de tratar de manera confidencial la información, especialmente la relativa a datos personales.

----------o----------