POLÍTICA DE INCIEDENTES DE SEGURIDAD INFORMÁTICA CONJUNTO INMOBILIARIO CITY PLAZA P.H.

Dando cumplimiento a lo dispuesto en la ley estatutaria 1581 de 2012, a su Decreto Reglamentario 1377 de 2013 y lo consignado en el artículo 15 de la Constitución Política y a las recomendaciones hechas por la Delegatura de Protección de Datos Personales de la Superintendencia de Industria y Comercio, **EL CONJUNTO INMOBILIARIO CITY PLAZA P.H.** ha adopta el presente manual para la regulación de los eventuales incidentes de seguridad informática que lleguen a ocurrir en **EL CONJUNTO INMOBILIARIO CITY PLAZA P.H.** en su condición de responsable del tratamiento de datos personales. La necesidad de la implementación de la presente política obedece al cumplimiento estricto de un mandato legal, el cual establece el deber parte el responsable del tratamiento de datos de llevar a cabo acciones frente a los incidentes de seguridad en el manejo de la información que se presenten:

> "*ARTI□CULO17. DEBERES DE LOS RESPONSABLES DEL TRATAMIENTO. Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:* (...)
> "*n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.* (...)
>
> *ARTI□CULO 18. DEBERES DE LOS ENCARGADOS DEL TRATAMIENTO. Los Encargados del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:* (...)
> "*k) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares;* (...)"

OBJETO.- El presente manual se expide para determinar los parámetros bajo los cuales deben tratarse y manejarse los eventuales incidentes de seguridad informática que se presente. De esta manera se pretende edificar un plan dirigido a afrontar los incidentes de seguridad que afecten los Datos Personales bajo la custodia o posesión de la copropiedad y la mitigación potencial de su impacto sobre los Titulares de la información y sus datos.

FINALIDAD.- Este manual permite instrumentar los procedimientos que se llevarán a cabo frente a la sospecha o consumación real de un incidente de seguridad informática que afecte o pueda llegar a afectar los datos de la copropiedad. El manual pretende generar un esquema organizado para salvaguardar los datos privados, semiprivados, públicos y sensibles de sus titulares.

CONSULTA DE LA POLÍTICA.- Esta política debe ser presentada y dispuesta en un acceso visible en los sitios oficiales de **EL CONJUNTO INMOBILIARIO CITY PLAZA P.H.** para su fácil consulta y acceso por parte del público en general.

CLASIFICACIÓN DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.- Los incidentes de seguridad pueden clasificarse dependiendo del grado de pérdida de las siguientes características de la información:

- Confidencialidad: se presenta cuando existe una revelación indebida de información privilegiada o una vulneración voluntaria de información confidencial.

- Integridad: Consiste en la adulteración o alteración de la información física o digital efectuada por un tercero o por un empleado de la entidad.

- Disponibilidad: se presenta cuando se deja de tener la disponibilidad y control pleno de la información

PROTOCOLO PARA EL MANEJO DE INCIDENTES DE SEGURIDAD INFORMÁTICA.- De acuerdo con lo contemplado por la normatividad vigente aplicable en materia de protección de datos, incidentes que se presente sobre datos personales tratados por la copropiedad se manejarán de la siguiente forma:

- Protocolo de respuesta en el manejo de incidentes de seguridad: una vez se tenga conocimiento un reporte de cualquier tipo de incidente de seguridad informática o que afecte los datos personales de sus titulares, se pondrá conocimiento a más tardar dentro del día hábil siguiente al superior jerárquico y a la persona encargada del tratamiento de datos en la empresa de administración de la copropiedad.

- Posteriormente se analizará el impacto que pueda llegar a tener el incidente y se efectuará una consulta con el abogado externo de la entidad para verificar los alcances implicaciones legales que pueda llegar a tener el incidente de seguridad de la información. Para esto se tendrá un plazo máximo de cinco días hábiles contados a partir del momento en que se tuvo conocimiento del incidente de seguridad informática.

- Posteriormente se radicará el incidente de seguridad informática en el sitio web https://www.sic.gov.co/content/reporte-de-incidentes-de-seguridad. La presentación del incidente se deberá efectuar dentro de los cinco días hábiles posteriores al momento en que se tenga el dictamen del abogado externo de la entidad.

- En el momento en que se tuvo conocimiento del incidente y hasta la radicación del incidente de seguridad informática en la página de la superintendencia no podrán pasar más de 15 días hábiles.

- Se analizará si dentro del incidente de la seguridad se encuentran datos sensibles, para efectos de dar el mejor manejo posible a la contingencia.

- En todo momento la persona que tuvo conocimiento del incidente debe llevar la trazabilidad de las gestiones encaminadas para el control del riesgo y la presentación y radicación del incidente de seguridad de la información ante la autoridad competente.

- Frente a posibles riesgos en los datos de los titulares, se podrá advertir a los mismos para efectos de generar recomendaciones en causadas a la mitigación y prevención de manejos indebidos de datos por parte de terceros.

- Llevar a cabo un análisis de las causas que generaron el incidente de seguridad de la información, para efectos de tomar correctivos inmediatos y resguardar el excedente de información o datos que no hayan entrado en el incidente.

- Verificar la necesidad de presentar una denuncia penal o querella frente al incidente ocurrido.

- El análisis, seguimiento y resolución de un incidente de seguridad comportará la máxima prioridad para todo el personal de la entidad.

- Se deberá hacer una graduación del riesgo por parte del oficial de tratamiento, quien deberá catalogar el incidente de seguridad informática mediante los siguientes niveles de riesgo: nivel bajo, nivel medio, nivel alto y nivel grave. La división de los niveles de riesgo obedecerá a la afectación de los titulares de los datos, el impacto patrimonial que tuvo el incidente y la naturaleza de los datos afectados. Esta división se puede explicar de la siguiente manera:

  Bajo riesgo: es improbable que el incidente de seguridad tenga un impacto en las personas, y de generarlo, este sería mínimo.

  Riesgo medio: el incidente de seguridad puede tener un impacto en las personas, pero es poco probable que el impacto sea sustancial.

  Riesgo alto: el incidente de seguridad puede tener un impacto considerable en las personas afectadas.

  Riesgo grave: el incidente de seguridad puede tener un impacto crítico, extenso o peligroso en las personas afectadas.

- Tiempos de ejecución frente a la puesta en conocimiento de un incidente de seguridad en la información serán los siguientes:

PROCEDIMIENTO	TÉRMINO
Análisis preliminar del incidente	5 días
Evaluación con el abogado externo de la entidad sobre el manejo impacto del incidente	5 días
Radicación del incidente de seguridad de información ante la autoridad competente	5 días

Independientemente del incidente de seguridad informática, éste debe ser radicado dentro de los 15 días hábiles siguientes a su ocurrencia.

REGISTROS INTERNOS DEL INCIDENTE DE SEGURIDAD EN LA INFORMACIÓN.- Para efectos del presente manual, **EL CONJUNTO INMOBILIARIO CITY PLAZA P.H.** efectuará los siguientes registros documentales de cara a los incidentes de seguridad de la información que ocurran:

1. El oficial del tratamiento de la entidad efectuará una descripción general de las circunstancias del incidente de seguridad (incluidas las Bases de Datos y las clases de datos -sensibles, privados, etc- comprometidos). Para lograr este cometido, se podrá emplear el siguiente catálogo de preguntas que deberán ser objeto de esclarecimiento:

    1.1. ¿Cómo se produjo?

    1.2. ¿Cuándo y dónde tuvo lugar?

    1.3. ¿Cuál fue la naturaleza y quién lo detecto?

    1.4. ¿Se continúa compartiendo o divulgando información personal sin Autorización?

    1.5. ¿Quién tiene acceso a la información personal?

    1.6. ¿Es este un problema sistémico o aislado?

    1.7. ¿Cuál fue el alcance del incidente de seguridad?

    1.8. ¿Que se puede hacer para asegurar la información o detener el acceso, divulgación o disponibilidad no autorizada y reducir el riesgo de daños a los afectados?

    1.9. ¿Es un incidente de seguridad relacionado con Datos Personales que requiere la notificación a las personas tan pronto como sea posible?

    1.10. ¿Los datos comprometidos afectarán las transacciones que debe realizar la entidad con terceros externos?

2. El oficial del tratamiento debe segmentar dentro del informe las categorías de Titulares de la información afectados con el incidente de seguridad en la información.

3. La fecha y hora del incidente de seguridad y del descubrimiento del mismo.

4. Las indagaciones preliminares e investigaciones realizadas por la organización.

5. Los Responsables del manejo del incidente de seguridad.

6. La evaluación del nivel de riesgo derivado del incidente de seguridad en los Titulares y los factores tenidos en cuenta.

7. La inclusión de detalles personales, cuando deban establecerse.

8. Análisis e identificación de los daños que pueda causar el incidente. Para la correcta identificación de los daños se podrá verificar si el incidente ha causado alguno de los siguientes perjuicios:

    8.1. Riesgo en su seguridad física o psicológica
    8.2. Extorsión económica o sexual
    8.3. Hurto de identidad
    8.4. Suplantación de identidad
    8.5. Pérdida financiera
    8.6. Negación de un crédito o seguro
    8.7. Perfilamiento con fines ilícitos
    8.8. Pérdida de negocios u oportunidades de empleo
    8.9. Discriminación
    8.10. Humillación significativa o pérdida de dignidad y daño a la reputación
    8.11. Pérdida reputacional
    8.12. Pérdida de clientes o usuarios
    8.13. Pérdida de confianza en la organización
    8.14. Honorarios de consultores e ingenieros forenses
    8.15. Pérdida de activos
    8.16. Sanciones, órdenes e instrucciones administrativas
    8.17. Exposición financiera
    8.18. Órdenes judiciales
    8.19. Demandas judiciales
    8.20. Riesgo para la salud pública
    8.21. Riesgo para la seguridad pública
    8.22. Pánico económico
    8.23. Alteración de los pilares constitucionales de un país

9. Las medidas correctivas que se llevarán a cabo.

10. La prueba del reporte efectuado ante la SIC, así como la comunicación realizada a los Titulares de la información, si fue necesario.

11. Determinación e individualización de los titulares de los datos que fueron afectados con el incidente.

PARÁMETROS QUE DEBE CUMPLIR LA INFORMACIÓN PARA EL REGISTRO.- la información almacenada por la copropiedad para efectos de registro deberá contar con lo siguiente:

- Contener suficientes detalles para que la autoridad evalúe si se actuó diligentemente en el manejo del incidente de seguridad.

- Conservarse con las medidas de seguridad y confidencialidad necesarias para protegerla de cualquier amenaza.

- Estar sujeta a los plazos de conservación establecidos para la entidad (10 años), en concordancia con los principios de finalidad, necesidad y proporcionalidad.

- Garantizar la originalidad e integridad de la prueba técnica en los términos de la Ley 527 de 1999.

POSIBLES CAUSAS DE INCIDENTES DE SEGURIDAD DE LA INOFRMACIÓN. - la siguiente lista enuncia múltiples ejemplos de incidentes de seguridad la información que pueden servir para efectos de identificar la existencia del incidente:

- Alteración; destrucción; robo o pérdida de archivos físicos
- Deficiencias o defectos en las operaciones
- Actos maliciosos o criminales
- Fallas en los sistemas de la organización
- Virus, malwares o similares
- La revelación involuntaria o fortuita de información confidencial o privilegiada.

MONITOREO POSTERIOR AL INCIDENTE.- Con posterioridad a la ocurrencia del incidente de seguridad informática, el responsable del tratamiento deberá realizar un monitoreo consiste en realizar un seguimiento constante para velar porque las medidas que se hayan establecido al interior de la entidad se apliquen y funcionen en la práctica.

COMUNICACIÓN DEL INCIDENTE DE SEGURIDAD.- Según la naturaleza del incidente de seguridad ha ocurrido, se designará una persona para que realice la respectiva comunicación a los titulares de los datos, en el evento en que esto sea pertinente.

CANAL DE COMUNICACIÓN FRENTE A UN INCIDENTE DE SEGURIDAD.- Cualquier tipo de solicitud producto del ejercicio de los deberes y derechos consagrados en este manual podrá dirigirse a los siguientes canales de comunicación habilitados para la recepción de quejas, reclamos, peticiones y/o solicitudes relacionadas con el tratamiento de datos personales: mercadeo@cityplaza.com.co. No se consideran canales de comunicación para este efecto ningún otro que no haya sido descrito anteriormente, los portales web ni las redes sociales de propiedad de la institución.

MEDIDAS A IMPLEMENTAR CON POSTERIORIDAD A LA OCURRENCIA DE UN INCIDENTE.- con posterioridad a la ocurrencia del incidente, se debe tomar correctivos para la prevención y mitigación del riesgo causado con ocasión al incidente de seguridad informática, para lo cual se analizarán las siguientes alternativas:

• Reforzar los programas de capacitación y educación del personal.

• Identificar y mejorar los controles internos que no tuvieron el efecto esperado en la contención de la brecha de seguridad.

• Identificar y eliminar malware o desactivar cuentas de usuarios vulnerables.

• Realizar un contraste con las medidas adoptadas para solucionar el incidente de seguridad en cuestión, y garantizar un análisis pormenorizado de las soluciones que pudieron haberse adoptado.

• Actualizar el antivirus de la organización.

• Analizar con el antivirus todo el sistema operativo, incluidas aquellas secciones que no se vieron afectadas.

• Garantizar que la estrategia adoptada encuentre un balance entre la continuidad del negocio y el riesgo intrínseco en los activos que se hayan visto afectados por el incidente de seguridad.

• Elaborar un informe final tendiente a recopilar la información, plazos de actuación y medidas adoptadas, de cara a una revisión por terceras personas

ACTUALIZACIÓN.- La Presenta Política de Incidentes de Seguridad Informática del **EL CONJUNTO INMOBILIARIO CITY PLAZA P.H.** fue actualizada por última vez en septiembre de 2023.
