CIRCULAR ASUNTO: POLÍTICAS NORMAS DE SEGURIDAD FÍSICA			PREVISORA SEGUROS
CÓDIGO: CIR-380	**ÁREA EMISORA:** GERENCIA DE RIESGOS	**FECHA:** 25/Abr/2018	
VERSIÓN: 1	**CREA** ☐ **MODIFICA** ☑ **MANUAL** ☑ **NORMA** ☐ **PROCEDIMIENTO** ☐		
Documento de Uso Interno			

PARA: TODOS LOS PROCESOS DE LA COMPAÑÍA

OBJETIVO:

Establecer lineamientos que contribuyan con la prevención del daño físico ya sea a las instalaciones, a los activos o a la información de la organización, usando medidas de control para el acceso físico, previniendo la afectación de los recursos y la afectación de las actividades de la organización que se puedan generar por amenazas físicas de origen natural o humano.

ALCANCE:

Esta política aplica a todos los procesos de la Compañía, sus funcionarios, contratistas y terceros que accedan, copien, modifiquen o procesen la información.

POLÍTICA

a) Generalidades:

I. La Previsora debe dar tratamiento a amenazas de seguridad física que puedan afectar los activos de información críticos, así como las instalaciones donde éstos se encuentren.

II. Todas las instalaciones deben contar con protecciones físicas y ambientales acordes con la clasificación de los activos que protegen, incluyendo áreas seguras para la gestión, almacenamiento y procesamiento de información, perímetros de seguridad, controles de acceso físicos, controles especiales en áreas de mayor sensibilidad que se hayan identificado, seguridad de los equipos, seguridad en el suministro eléctrico y cableado, condiciones ambientales de operación y sistemas de contención, detección y extinción de incendios adecuados.

III. La Previsora debe identificar y tratar a los riesgos que puedan ocurrir, en relación a la seguridad física, ambiental y del entorno que podría afectar la Seguridad de la Información.

b) Protección Contra Amenazas Externas Y Ambientales

I. Se deben almacenar adecuadamente elementos que puedan ser combustibles o que contribuyan a una conflagración.

II. La Compañía, en cabeza de la Subgerencia de Recursos Físicos, debe realizar inspecciones para validar y analizar los riesgos (amenazas y vulnerabilidades) de las instalaciones, especialmente de aquellas donde se realicen actividades de control y monitoreo de infraestructura, de procesamiento de información y comunicaciones, y aquellas donde se soporten servicios de apoyo a las operaciones organizacionales.

III. Las instalaciones de control de la infraestructura de procesamiento de datos deben ubicarse en lugares a los cuales no pueda acceder el público en general.

IV. Aquellas áreas que se encuentren vacías deben ser controladas, revisadas y monitoreadas de manera periódica.

c) Roles y responsabilidades

I. Todos los colaboradores y terceros son responsables de acatar los controles de acceso físico y por ningún motivo deben tratar de sobrepasarlos. De igual forma deben informar en caso de hallar personal ajeno a Previsora en áreas no permitidas, así como cualquier violación de las medidas de seguridad física.

II. Los líderes de proceso son los responsables de autorizar o no el ingreso a las áreas delimitadas como de acceso restringido, que se encuentran bajo su custodia.

III. Los responsables de cada área deben mantener un registro protegido que permita auditar todos los accesos a la información y a las áreas de acceso limitado y restringido.

IV. Los lineamientos para el control de acceso de los visitantes y empleados a las instalaciones de la compañía se definen en las circulares y manuales documentados por la Subgerencia de Recursos Físicos, dentro del proceso de Infraestructura Física.

d) Recursos

I. La Previsora debe ofrecer recursos y asesoría para el control de los activos de acuerdo a su tratamiento y mantener áreas seguras para la gestión, almacenamiento y procesamiento de información. Estas áreas deben contar con protecciones físicas, ambientales acordes con los activos que protegen, incluyendo perímetros de seguridad, controles de acceso físicos entre otros.

e) Revisión

I. Esta política se encuentra inmersa en el proceso de mejora continua del Sistema de Gestión de Seguridad de la Información, por tal razón se revisará cuando sea requerido conforme los cambios organizacionales que se den en el transcurso del tiempo o en su defecto una vez cada dos años.

f) Manejo de Excepciones

I. Las excepciones a cualquiera de las directrices de la Política de Seguridad General o sus políticas derivadas serán admitidas únicamente cuando el Oficial de Seguridad de la Información avale y divulgue su aceptación. Las excepciones a los lineamientos existentes deben estar sustentadas sobre la base de un análisis de riesgos aplicable.

CIRCULAR(ES) DEROGADAS(S):	

CONTROL DE CAMBIOS		
VERSIÓN	**FECHA**	**JUSTIFICACIÓN Y DESCRIPCIÓN DEL CAMBIO**
0	23/Dic/2014	Se crea documento.
1	06/Feb/2018	Se actualiza este documento (Caso 3562)

FLUJO DOCUMENTAL		
ELABORÓ	**REVISÓ**	**APROBÓ**
Nombre: ADMONCALIDAD **Cargo:** ADMINISTRADOR DOCUMENTAL **Fecha:** 09/Abr/2018	**Nombre:** SANDRA PATRICIA CEDIEL BRAVO **Cargo:** Especialista **Fecha:** 09/Abr/2018	**Nombre:** RENATO YESID MUNOZ RODRIGUEZ **Cargo:** GERENTE CASA MATRIZ **Fecha:** 25/Abr/2018