POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

CLASIFICACIÓN Y CONTROL DE LA INFORMACIÓN
La información de negocio de 3SM S.A. y todos los recursos TIC relacionados se encontrarán inventariados, tendrán asignados un propietario y estarán clasificados según su nivel de confidencialidad y criticidad para el negocio de 3SM S.A.

ADMINISTRACIÓN DE RIESGOS:
Se evaluarán los riesgos a los que están sometidos los activos TIC de 3SM S.A. El departamento de seguridad de la información en conjunto con el propietario del recurso TIC establecerán los riesgos que pueden afectar a dicho recurso, las implicancias de su exposición, modificación o acceso no autorizado y cuáles son las medidas de protección que se implementarán de acuerdo con el análisis de riesgo efectuado.

SEGURIDAD DEL PERSONAL:
Se informará al personal de 3SM S.A., ya sea efectivo o contratado, o perteneciente a empresas proveedoras de 3SM S.A., desde el momento de su ingreso de las responsabilidades y derechos en materia de uso y protección de los recursos TIC de la Compañía. Se capacitará con el fin de crear conciencia acerca de la importancia que adquiere este aspecto para la Compañía. Se realizará un seguimiento del uso que se hace de los recursos TIC para impedir daños e interferencias, evitando así, interrupciones en las actividades de 3SM S.A.

SEGURIDAD FÍSICA Y DE ENTORNO:
Se protegerán adecuadamente todos los recursos TIC y las áreas donde estos residen para evitar accesos no autorizados y daño intencional o fortuito, a través de medidas de protección acorde con la clasificación de criticidad, confidencialidad y riesgo otorgado a cada recurso.

ADMINISTRACIÓN DE COMUNICACIONES Y OPERACIONES:
Se asegurará la integridad y disponibilidad de los servicios y comunicaciones para garantizar un correcto procesamiento de la información, resguardando la confidencialidad de la misma.

CONTROLES DE ACCESO:
El acceso a los recursos TIC será restringido de acuerdo con los requerimientos de control establecidos por sus propietarios y con la necesidad de saber a fin de utilizarlos. Dicho acceso se asegurará a través de procesos de autenticación, autorización, monitoreo y posterior auditoria.

DESARROLLO Y MANTENIMIENTO DE SISTEMAS:
Los principios de seguridad de la información serán incorporados a los sistemas aplicativos en todo el ciclo de vida de los mismos, incluyendo los procesos de desarrollo, prueba, mantenimiento y puesta en producción de los sistemas aplicativos. Se prevendrán pérdidas, modificaciones o uso inadecuado de los datos, proyectos y sistemas aplicativos de 3SM S.A.

ADMINISTRACIÓN DE LA CONTINUIDAD DE NEGOCIO:
Se desarrollarán y mantendrán los planes de recuperación tecnológica y continuidad de negocio, de forma tal de poder responder a eventos no deseados que impacten de manera negativa sobre los procesos de negocio críticos para 3SM S.A.

CONFORMIDAD CON LEYES, REGULACIONES Y NORMAS INTERNAS:
Se garantizará que la utilización de los recursos TIC no provoque infracciones o violaciones de leyes, regulaciones, ni de las obligaciones establecidas por estatutos, normas, reglamentos o contratos vigentes en cada ámbito de actuación. Asimismo, se evaluará y asegurará el cumplimiento de las normas internas (políticas, estándares, procedimientos) relativos a la seguridad de la información.