Resumen Política General de Seguridad de la Información

Blumar y Filiales

Política

La Política General de Seguridad de la Información, tiene como objetivo establecer las directrices generales para la protección de los activos de información utilizados en los procesos de Blumar.

Objetivo General

Otorgar continuidad a los procesos operativos de Blumar, protegiendo los activos de información frente a amenazas internas y externas que atenten contra la confidencialidad, integridad y la disponibilidad.

Seguridad de la información

Es el conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información (física o digital) de ataques maliciosos buscando mantener la confidencialidad, integridad y disponibilidad de la información.

LOS TRES PILARES FUNDAMENTALES DE LA SEGURIDAD DE LA INFORMACIÓN

Confidencialidad: Nivel o clasificación de la información de acuerdo con la capacidad de accesibilidad para las personas autorizadas.

Integridad: Nivel de protección de la totalidad y la exactitud de la información.

Disponibilidad: Nivel de aseguramiento de los accesos de los usuarios autorizados a la información y a los activos asociados.

RESPONSABILIDADES

Responsabilidad de los Colaboradores

Cumplir con lo formalizado en la política y aplicarlo tanto en su entorno laboral, como fuera de este, además, tiene la obligación de alertar de manera oportuna y adecuada a su supervisor y/o comité de seguridad de la información, cualquier incidente que afecte la confidencialidad, integridad y disponibilidad de la información.

Responsabilidad de los Proveedores

Cumplir las exigencias de seguridad de la información que Blumar define tales como:

- Dar cumplimiento de los niveles de servicio establecidos.
- Contar con mecanismos de continuidad de negocios para asegurar la disponibilidad de los servicios.
- Se deben cumplir las condiciones de confidencialidad y no divulgación de información incluso al finalizar el contrato por los servicios.
- Se debe notificar a Blumar sobre cualquier emergencia de seguridad de la información que se presente.

RECOMENDACIONES

Aun que cada día pueden aparecer nuevas amenazas siempre se deben seguir estas recomendaciones para trabajadores y proveedores.

- Mantener software antivirus instalado y actualizado
- Ser precavido a la hora de visitar sitios web fijándose siempre en que sean sitios seguros y cuenten con el protocolo https.
- Nunca abrir links enviados por correo electrónico de origen desconocido
- Nunca abrir archivos adjuntos en correos electrónicos de fuentes desconocidas
- Si viajas con un computador, siempre llévalo como equipaje de mano, y no dejarlo a la vista en automóviles o lugares públicos.
- Mantener las fuentes de información confidencial con mecanismos de control de acceso y fuera del alcance de quienes no deban acceder.
- Bloquear el computador cuando quede desatendido.
- No guardar contraseñas escritas en lugares visibles o de fácil acceso como agendas, bajo el teclado etc.
- Solo utilizar software autorizado por la compañía
- No utilizar dispositivos de almacenamiento externos como pendrive, discos duros externos etc. en computadores conectados a la red de Blumar que no cumplan con los requisitos mínimos de seguridad o, que no se sepa la procedencia del dispositivo o, que fue utilizado en algún computador que no cuente con las medidas de seguridad necesarias.
- La información física o digital que ya no se necesite debe ser destruida mediante trituradoras o borrado seguro de información.

BLUMAR