Información acerca de la Seguridad de la información

Política de seguridad de la información

CIRION cuenta con una política de seguridad de la información que proporciona activamente administración y supervisión de la efectividad del programa de cumplimiento con una amplia gama de organizaciones, complejidad organizativa, recursos y programas de cumplimiento. Estándares, políticas y procedimientos. Administración del programa de cumplimiento. Detección y evaluación de empleados, proveedores y otros agentes. Comunicación, educación y capacitación sobre cuestiones de cumplimiento. Sistemas de seguimiento, auditoría y presentación de informes internos. Acciones disciplinarias por incumplimiento. Investigaciones y medidas correctivas.

CIRION se somete a auditorías realizadas por firmas externas de prestigio regional y global. Las revisiones independientes del proceso de gestión de riesgos permiten a CIRION identificar, comprender y remediar los riesgos de seguridad de la información que podrían afectar las operaciones.

El momento de la incorporación de nuevo personal o provedores se realizan capacitaciones de seguridad las cuáles se repiten para todos los empreados y contratistas de forma anual.

Nuestro centros de datos cuentan con certificación ISO27001 y en general nuestros servicios están sometidos a políticas de administración de modificaciones, ventanas de mantenimiento, mentenimiento emergente, acuerdos de nivel de servicio, entre otros.

Los sistemas de CIRION cuentan con controles internos de auditoría, seguimiento y responabilidad personal. Los administradores deben asegurarse de que cada sistema pueda vincular la información de registro pertinente con las actividades efetuadas por personas o procesos; así como , los procedimientos o estándares para

el análisis de los registros para determinar actividades inapropiadas. Los controles de resposnabilidad deben ser suficientes para detetar y disuadir los intentos de violar la seguridad del sistema de manera oportuna.

Sobre su cuenta de Internet:

CIRION al ser un proveedor de Servicios de Acceso a Internet, a continuación emite recomendaciones para usuarios a manera de guía para un uso adecuado y beneficioso del servicio de Internet en cuanto a la Seguridad de la Información.

Así, las recomendaciones que se manifiestan son las siguientes:

- El usuario principal del servicio de Internet que paga y administra el contrato del servicio en mención debe procurar un manejo adecuado de los usuarios (hijos, conyugue, usuarios empresariales, etc.) mediante controles parentales o políticas de seguridad para el acceso a estos servicios.
- El usuario que haga uso del servicio de Internet puede efectuar pruebas de capacidad contratada conectando su computadora directo al dispositivo de red del proveedor sin equipos intermedios y hacer pruebas de envío y recepción de información.

Uso de claves:

- El uso de claves para servicios de Internet debe manejarse de manera secreta. No se la debe mencionar ni escribir para evitar divulgación de dicha información, y a su vez evitar correos que solicitan información sensible (número de tarjeta o número de cuentas, etc.) ya que pueden ser correos falsos que utilizan tácticas de ingeniería social para obtener información y realizar fraudes.
- La clave del usuarios (password) debe de ser conocido solo por el usuario que es dueño de la cuenta de correo, que incluyan mínimo 8 caracteres

incluyendo mayúsculas, minúsculas, números y caracteres especiales, esto es por su seguridad.

- Se recomienda cambiar la clave periódicamente, de preferencia cada 3 meses.

Sobre el uso del correo electrónico:

- Evite renviar correos masivos, los cuales son diseñados para generar SPAM lo cual congestiona la red de internet, además que es una forma para obtener direcciones de correos, que luego son utilizadas para enviar propaganda publicitaria que no se ha solicitado. Si considera conveniente renviar un correo masivo, sugerimos primero verificar la fuente o validar si dicho correo no es un engaño (Hoax), para lo cual puede consultar en su buscador de internet la palabra HOAX y parte del texto recibido en el correo con lo cual se enterará si dicho correo ha sido generado para engañar al público.
- No responder ningún correo por confiable que este parezca ante la solicitud de su clave. Las empresas que tienen un manejo responsable de la información, no solicita las claves por correo.
- Es conveniente usar de forma adecuada la dirección de correo electrónico evitando informar o publicar la dirección y clave en páginas web, dado que esto se presta para la copia de listas de correo electrónico para distribución de propaganda y correo no deseado (SPAM).
- En el caso de que se publique información en Internet, tenga cuidado de que estas publicaciones no tengan efectos ilícitos o dolosos. Esto a fin de preservar una adecuada conducta con la información publicada.

Sobre las redes sociales:

- Cuando acceda a una sesión de chat (chat room), nunca se deben de escribir número de tarjetas de crédito, contraseñas o información personal que pueda ser utilizada por terceros para hacer mal uso de ella.
- Tener siempre la certeza de a quien se acepta como supuesto amigo o contacto en las conocidas redes sociales. Se recuerda que estos

contactos pueden tener puerta abierta a que conozcan toda la información que se publica en el portal personal, incluidas fotos familiares, amigos, información personal, actividades diarias, entre otros.

- Se recomienda que la publicación de información personal sea la mínima posible y el manejo de la privacidad sea configurado para que su información no esté abierta o se preste para el uso doloso o nocivo.
- La pérdida de la privacidad se produce cuando se proporciona, a través de Internet, información sobre la vida personal del usuario, o imagen personal, esto para poder entrar en determinados espacios comunes o para la utilización “gratuita” de servicios. Muchas páginas solicitan datos personales para un uso fraudulento de los mismos. Para evitar esto, se recomienda no usar siempre el mismo nombre de usuario y contraseña en todos los servicios que utilice (si se desea conservar una misma contraseña, se le puede ir agregando algún número a la misma para que sea distinta según distintos servicios que se usen en Internet). No proporcionar, por principio, datos personales como nombre, dirección, número de cédula, número de teléfono o fotografías/vídeos suyas o de su familia.

El Internet y el entorno familiar:

- En el caso de entornos familiares. Los padres de familia deben animar a sus hijos a dialogar sobre los contenidos desplegados en Internet y sobretodo acerca del contenido que sea desagradable para el uso de Internet. Procure mantener momentos adecuados para la reflexión de la información publicada en Internet y de los efectos que esta puede causar si no se tiene la precaución y cuidado del caso.
- Se recomienda a los padres de familia aprender sobre computación y sobre conceptos de web tales como los “wikis”, los blogs, las redes sociales, los podcast, con la finalidad de conocer el mundo cibernético en el que están sus hijos y ser sus guías y orientadores.
- Para los padres de familia, se recomienda que tengan esquemas de control parental básico para que hijos y usuarios de la red del hogar eviten el acceso

a páginas de contenido nocivo o falso. Así también, para el uso de sistemas de conversación (chats), se recomienda que los padres de familia tengan conocimiento de dichos sistemas y orienten a sus hijos respecto del uso y riesgos que existen.

El Internet y el entorno empresarial:

- En entornos empresariales, las políticas de uso de Internet se deben normar a fin de que la información que el usuario final tenga prevención en el uso de Internet y se establezca una política de cambio periódico de claves.
- Nunca deje el computador prendido con sesiones activas de banco o de compras en Internet. Para esto procure usar protectores de pantalla con clave.

Otros temas generales:

- Para el uso de compras por Internet, tener la prevención de que la publicidad colocada en dichas páginas no siempre tiene resultados beneficiosos ni necesarios para el usuario que accede a dicho contenido. Por otra parte, procure manejar sistemas de pago seguro y tenga sus tarjetas de crédito debidamente controladas. Consulte con su entidad de servicios bancarios para el uso adecuado y recomendaciones de seguridad de la tarjeta de crédito para compras en Internet.
- El “PISHING” es un método para el intento de adquirir fraudulentamente información de una persona, como la identidad y código secreto de una tarjeta electrónica o del acceso a los datos bancarios. Actúa a través de la recepción de un correo electrónico en el que en nombre de una entidad bancaria, se pide al usuario esta información. El mensaje suele imitar con mucha exactitud la imagen y textos habituales de la entidad bancaria o comercial. Para evitar caer en este tipo de fraudes, haga caso omiso de dichos correos y NO proporcione nunca información sobre su cuenta bancaria, su identidad o el código de acceso. Informe a su entidad bancaria o comercial de la recepción de cualquier correo sospechoso.

- En el caso de servicios de Telefonía IP por Internet, se debe leer las condiciones de servicio que se prestan por dicho servicio. A su vez, tener la precaución de usar usuarios con claves seguras y sistemas de control para evitar los fraudes de tipo telefónico.