LA SEGURIDAD DE LAS BASES DE DATOS

A continuación, algunas recomendaciones sobre seguridad en bases de datos, instaladas en servidores propios de la organización.

ETAPA 1. Identificación del flujo de los datos personales Los responsables y encargados deberán contestar cada una de las preguntas de esta etapa para identificar con claridad el uso que dan a los datos personales, desde que los recaban hasta que los eliminan en sus organizaciones o empresas.

Pregunta 1. ¿Qué tipos de datos personales recabo? El objetivo es identificar qué tipo de datos personales se recaban en los distintos formatos que se utilizan y lo más importante, si es necesario recabarlos o no, con el fin de utilizar sólo los tipos de datos necesarios para la finalidad del servicio. La respuesta a esta pregunta debe ser un listado de todos los tipos de datos personales que son necesarios para que la empresa pueda ofrecer productos y/o brindar servicios.

Pregunta 2. ¿Cómo recabo los datos personales? El objetivo es identificar en qué tipo de formatos se recaban y almacenan los datos personales por el responsable. La respuesta a esta pregunta debe ser un listado de todos los documentos, plantillas, formularios, físicos o electrónicos en los que se registran los datos personales.

Pregunta 3. ¿Dónde se almacenan los datos personales? Cada formato identificado puede estar almacenado en una o más ubicaciones, físicas o electrónicas. La respuesta a esta pregunta debe ser un listado de los lugares, gabinetes, archiveros, carpetas, computadoras, etc. donde se almacenen los medios.

Pregunta 4. ¿Quién tiene permiso para acceder o manejar los datos personales? Diferentes personas en una empresa u organización pueden tener acceso a los sitios donde se almacenan los datos personales. Las personas identificadas y autorizadas para acceder podrían manejar la información personal con permisos específicos de uso, esto es conocido comúnmente como un esquema de privilegios. La respuesta a esta pregunta es una relación de las personas que tienen acceso autorizado a los sitios identificados o permisos para manejar los medios que contienen datos personales.

ETAPA 2. Evaluación de las medidas de seguridad básicas

Para una organización, no es posible implementar un programa de seguridad de la información que reduzca el riesgo a cero, sin embargo, se pueden poner en marcha medidas de seguridad básicas para minimizar las vulneraciones a la seguridad de los datos personales y sistemas de tratamiento.

Las medidas de seguridad pueden abordarse bajo las siguientes categorías generales: **A)** Medidas de seguridad basadas en la cultura del personal. **B)** Medidas de seguridad en el entorno de trabajo físico. **C)** Medidas de seguridad en el entorno de trabajo digital.

A. Medidas de seguridad basadas en la cultura del personal

Una de las principales causas por las que ocurre robo o extravío de datos personales e incluso de cualquier información relevante para la organización, es simplemente porque los datos no se cuidan adecuadamente. El siguiente grupo de preguntas tienen como objetivo identificar las prácticas inadecuadas más comunes, que podrían provocar una vulneración a la seguridad.

A.1. ¿Pones atención en no dejar a la vista información personal y llevas registro de su manejo? Cuando se dejan datos personales sin supervisión o por descuido, éstos corren el riesgo de ser sustraídos por alguien más (interno o externo a la organización). Por ello es importante considerar controles como:

A.1.1. Política de escritorio limpio: No dejar a simple vista documentos importantes, equipo de cómputo, contraseñas en “post-it”, llaves, identificaciones, entre otros.

A.1.2. Hábitos de cierre y resguardo: Esto debe incluir conductas como: que cada empleado cierre sus cajones, que las cosas importantes siempre se mantengan bajo llave si no están en uso y/o que el último en salir de las oficinas cierre los archiveros y las puertas con llave, y active las alarmas.

A.1.3. Impresoras, escáneres, copiadoras y buzones limpios: Nunca se deben dejar abandonados documentos en áreas de uso común como las mencionadas.

A.1.4. Gestión de bitácoras, usuarios y acceso: Para controlar el acceso a los sitios, medios de almacenamiento, formatos y equipo de cómputo, se puede hacer con bitácoras tan simples como una lista donde se anote el nombre, fecha y hora de la persona que accede a un archivero para consultar un expediente, o bien, llevar bitácoras automatizadas para el uso de medios electrónicos. Es importante habilitar los mecanismos de registro en los equipos de cómputo y su software para

identificar la actividad de los usuarios. Así como revisar que las credenciales y permisos de los usuarios estén bien definidos.

A.2. ¿Tienes mecanismos para eliminar de manera segura la información? Si cualquier documento es depositado simplemente en la basura, éste puede ser recuperado y visto por cualquier persona malintencionada, y así ocurrir una fuga de información importante. Por otra parte, en los medios electrónicos, la simple acción de "borrado" no elimina de forma definitiva la información, y ésta puede ser recuperada desde los dispositivos desechados, con ciertas herramientas. Por ello se deben tomar en cuenta controles como:

A.2.1. Destrucción segura de documentos: Los documentos y otros medios físicos no deben simplemente desecharse una vez que ya no se utilizan, sino destruirse por ejemplo con triturado o incinerado. Cuando se adquiere equipo para estas tareas se debe evaluar que tan difícil sería para una persona recuperar la información, por ejemplo, hay trituradoras que hacen tiras el papel y otras que lo hacen pequeños trozos. Con tiempo y esfuerzo es posible recuperar un documento hecho tiras, pero es muy difícil recuperar uno hecho "confeti" o cenizas. Otra opción es almacenar en un sitio seguro los documentos a triturar y entregarlos periódicamente a alguien que preste el servicio de destrucción de documentos, sin olvidar que debe existir un contrato que estipule claramente el deber de confidencialidad del prestador de servicio.

A.2.2. Destrucción segura de información en equipo de cómputo y medios de almacenamiento electrónico: Es conocido que en los equipos de cómputo se puede "borrar" o "eliminar" la información de forma simple o con un clic, pero debido a la naturaleza del almacenamiento electrónico, lo que ocurre en realidad, es que ésta deja de ser fácilmente accesible pero sigue ahí hasta que nueva información la "sobrescribe". Para la eliminación definitiva de información existen herramientas de software que borran archivos electrónicos específicos o dispositivos de almacenamiento completos. Cuando la vida útil de un equipo de cómputo o medio de almacenamiento electrónico ha terminado, es recomendable destruirlo físicamente. Esto lo puede hacer la misma organización o contratar a un tercero para este servicio, cuando la cantidad de equipo de cómputo es mayor.

A.2.3. Fijar periodos de retención y destrucción de información: Es importante identificar de manera regular toda la información que ya no es de utilidad para la organización y que no requiere almacenarse para cumplir con alguna responsabilidad legal o contractual. Los procedimientos de

eliminación de información de gran valor o a gran escala deben ser formales y se deben registrar en bitácoras.

A.2.4. Tomar precauciones con los procedimientos de re-utilización: Por diversas razones, las organizaciones pueden optar por diferentes mecanismos de reciclado para minimizar costos, pero se debe ser cuidadoso en la posible exposición de datos personales. Por ejemplo, es común el uso de “bandejas de papel reciclado”, pero bajo ninguna circunstancia deberían utilizarse documentos con datos personales como “papel de reúso”. Cuando el equipo de cómputo tenga que cambiar de dueño por ejemplo, de un empleado a otro, es importante respaldar la información relevante para la organización y borrar completamente los datos que resguarda el equipo.

A.3. ¿Has establecido y documentado los compromisos respecto a la protección de datos? Todos aquellos involucrados en el tratamiento de datos personales deben actuar con relación a los principios que establece la Ley. No se deben obviar o dejar como reglas implícitas todas aquéllas relacionadas a la privacidad y protección de datos personales de las personas. De manera adicional, se debe fomentar la cultura de la seguridad y la noción del valor intrínseco de la información. Por ello, se deben considerar estrategias como:

A.3.1. Informar al personal sobre sus deberes mínimos de seguridad y protección de datos: El personal involucrado en el tratamiento de datos personales debe estar informado de manera explícita que tiene un compromiso y responsabilidad sobre la información en su custodia, y en su caso tareas específicas a realizar. Esto incluye por ejemplo, informar al personal de nuevo ingreso sobre sus funciones y obligaciones para la protección de datos e incluir cláusulas al respecto cuando se hace una contratación. En su caso, también se debe informar a los empleados de las posibles consecuencias y medidas disciplinarias relacionadas, en caso de no cumplir con sus deberes.

A.3.2. Fomentar la cultura de la seguridad de la información: En el trabajo diario, es común que a todas las personas que manejan información personal de manera continua, se les vuelva una actividad rutinaria, esto puede provocar que sean descuidados con la gestión de la información. Por lo que es necesario permear la seguridad de la información como una práctica cotidiana, recordando la importancia de este deber e incentivando a los empleados, para que entre ellos se recuerden el uso de medidas de seguridad y buenos hábitos de tratamiento.

A.3.3. Difundir noticias en temas de seguridad: Mantener informado al personal respecto a las últimas noticias en seguridad puede parecer complejo, sin embargo existen muchos medios de

comunicación, como las redes sociales, por los cuales las organizaciones se pueden mantener al tanto de las historias más relevantes en seguridad.

A.3.4. Prevenir al personal sobre la Ingeniería Social: De manera general se considera a la ingeniería social como un conjunto de técnicas para influenciar a una persona a tomar acciones que pueden estar o no dentro de sus intereses o responsabilidades. Estas técnicas pueden ser utilizadas por criminales para engañar a personas desprevenidas en línea, por teléfono o personalmente. Se debe invitar al empleado a que sea "cauto y cortés" es decir, que se cuestione en todo momento si alguna solicitud tiene sentido y si está dentro de sus responsabilidades cumplirla, de lo contrario negarse educadamente a entregar la información o a realizar la acción solicitada e informar de este hecho a su jefe inmediato.

A.3.5. Asegurar la protección de datos personales en subcontrataciones: La organización no debe asumir que un proveedor o cualquier externo tomará las medidas de seguridad necesarias para proteger la información personal y que la tratará como confidencial, sin que esto se manifieste explícitamente. Por ejemplo, a través de cláusulas que especifiquen claramente el tratamiento legítimo y las medidas de seguridad implementadas para la protección de los datos personales. Otros tipos de convenio que deben revisarse son los relacionados a la compra, venta o intercambio de datos de titulares, revisando a detalle que los datos sean utilizados con el consentimiento del titular. Además, en el uso de servicios de almacenamiento en línea o de cómputo en la nube, por ejemplo, el correo electrónico, se debe revisar y evaluar si el contrato de adhesión garantiza seguridad y confidencialidad de los datos que se almacenen.

A.4. ¿Tienes procedimientos para actuar ante vulneraciones a la seguridad de los datos personales? Para las organizaciones, incluso para aquéllas con gran madurez en el tema de seguridad de la información, el tema de vulneraciones a la seguridad de los datos personales puede resultar particularmente complicado, la idea básica es disminuir la afectación a los titulares de los datos personales y a la organización. Por eso, se requiere tomar medidas como:

A.4.1. Tener un procedimiento de notificación: Se debe tener establecida una cadena de avisos dentro de la empresa u organización en caso de que ocurra una vulneración a la seguridad. Cuando un empleado sufra o identifique un incidente de seguridad, éste debe tener muy claro a quién debe avisar en la empresa u organización. El responsable debe evaluar qué información se afectó y los medios para notificar a los titulares de lo ocurrido, esto con el fin de alertarlos y que tomen

precauciones. Adicionalmente, se podrá diagnosticar el posible impacto a las operaciones y tomar acciones que mitiguen el incidente, por ejemplo actualizando sus procedimientos y medidas de seguridad.

A.4.2. Realizar revisiones y auditorías: Se debe considerar la revisión periódica a la empresa u organización por un especialista en temas de seguridad para que éste realice evaluaciones y recomendaciones. Por la naturaleza técnica de algunas amenazas, este tipo de revisiones podrían ayudar a revelar malas prácticas en el tratamiento de datos personales o la existencia de vulneraciones a la seguridad no detectadas, por ejemplo a través de las llamadas pruebas de penetración o pentest. Los resultados de cualquier evaluación deben informarse a los empleados involucrados en el tratamiento de datos personales.

A.5. ¿Realizas respaldos periódicos de los datos personales? En la medida de lo posible se deben almacenar los documentos físicos en medio electrónico, es decir, capturar, digitalizar o escanear la información en papel para almacenarla, de forma tal que se resguarde el mínimo de información en papel y sólo se imprima cuando sea estrictamente necesario. Esto debido a que es más práctico respaldar información copiando un archivo de un medio electrónico a otro, comparado con fotocopiar, organizar y almacenar documentos en papel. Los datos personales almacenados en equipo de cómputo pueden dañarse de manera parcial o total debido a fallas en los sistemas o aplicaciones, por errores de operación de las personas, o bien por interrupciones de energía eléctrica, si se realizan respaldos de la información importante de manera periódica pueden mitigarse las consecuencias de estos incidentes. Es importante que los respaldos se realicen de manera regular y también cada vez que haya una actualización importante de los datos que están siendo almacenados en la organización. Se pueden realizar respaldos parciales sólo de la información crítica, diario o cada semana, y respaldos de toda la información, cada quince días o mensualmente. Es importante que los respaldos no se encuentren en la misma ubicación física que la información que se están respaldando y hacer pruebas de recuperación de las copias de respaldo para asegurarnos de que la información se encuentra íntegra.

B. Medidas de seguridad en el entorno de trabajo físico

Conforme los equipos de cómputo son cada vez más pequeños, ligeros y convenientes se vuelve muy fácil para las personas llevar información con ellos, por otro lado para muchas organizaciones es común revisar información en lugares públicos como un restaurante, cafetería o en el transporte

público. La seguridad del entorno de trabajo físico es un elemento básico para mitigar vulneraciones a la seguridad de los datos personales.

B.1. ¿Tienes medidas de seguridad para acceder al entorno de trabajo físico? El acceso al entorno de trabajo físico debe ser sólo para personal autorizado, si no existen restricciones para el acceso, se corre el riesgo de que los datos personales sean robados o manipulados. De manera particular, ninguna persona sin autorización debería poder acercarse al equipo de cómputo, archiveros con datos personales, o a cualquier otro medio de almacenamiento. Para esto se deben considerar medidas como:

B.1.1. Alerta del entorno de trabajo: No se debe permitir que alguien sin motivos relacionados al funcionamiento del negocio ingrese al entorno de trabajo. Se debe tener precaución con las personas no autorizadas al entorno, por ejemplo, en las oficinas de la empresa u organización debería haber áreas como un mostrador de recepción o si se está trabajando en un café se debería evitar que alguna persona extraña esté muy cerca de los elementos donde se tengan datos personales. Siempre se debe cuestionar la presencia de un extraño sin acompañamiento o que se encuentre cerca del entorno de trabajo.

B.1.2. Mantener bitácoras del personal con acceso al entorno de trabajo: En entornos como oficinas es importante mantener un registro de todos los que ingresan y salen y acordar que aquéllos que salen al final del entorno de trabajo deben poner especial atención, dicho de manera coloquial el "último en salir cierra".

B.2. ¿Tienes medidas de seguridad para evitar el robo? Se deben establecer medidas con las cuales se minimice el riesgo de que alguien robe información fácilmente. Por ejemplo:

B.2.1. Cerraduras y candados: En las oficinas de la empresa u organización o en casa se debe contar como mínimo con gavetas, escritorios, o archiveros que se puedan cerrar con llave. El mismo principio aplica para otros entornos, usando candados para laptops o maletas con cierre de combinación.

B.2.2. Elementos disuasorios: Existen medidas de seguridad que reducen de manera significativa el interés de un atacante, por ejemplo, alarmas (tanto para el entorno como para los dispositivos), guardias de seguridad, rejas, maletines de seguridad, entre otros.

B.2.3. Minimizar el riesgo oportunista: Es necesario limitar el número de entornos de trabajo donde se realice tratamiento de datos personales (por ejemplo, sólo en casa o en la oficina), si es necesario trabajar constantemente en otros entornos (como aeropuertos u oficinas de otros clientes) se debe permanecer especialmente cauto del entorno y nunca dejar un elemento con datos personales sin supervisión.

B.3. ¿Cuidas el movimiento de información en entornos de trabajo físicos? Al realizar envío de información siempre se corre el riesgo de que ésta se pierda o sea robada. Por ello, es importante tener controles de seguridad que minimicen el impacto del extravío, como:

B.3.1. Aprobación de salida de documentos, equipo de cómputo y/o medios de almacenamiento electrónico: Se debe registrar el permiso o la acción relacionada a la salida de los elementos mencionados en una bitácora, esto con el fin de que, en caso de pérdida, robo, daño o extravío se tenga control del posible impacto.

B.3.2. Mantener en movimiento sólo copias de la información, no el elemento original: Un incidente común en las organizaciones de cualquier tamaño es que la información que se pierde es la única información disponible. La información que sale de los entornos de trabajo usuales debería ser una copia, y no la información original.

B.3.3. Usar mensajería certificada: Es importante que el envío físico de medios que contienen datos personales se realice con mensajería segura/certificada, o en su defecto con personal de confianza, y siempre se debe recabar el acuse de recibo del envío.

C. Medidas de seguridad en el entorno de trabajo digital

Muchas de las operaciones de las organizaciones y de los mismos titulares están siendo llevadas a entornos digitales, por lo que se vuelve primordial proteger equipos de cómputo y dispositivos de almacenamiento contra el acceso no autorizado, de igual forma, contra amenazas informáticas como software malicioso (malware, virus, entre otros).

C.1. ¿Realizas actualizaciones al equipo de cómputo? Si una deficiencia en la seguridad de un equipo de cómputo (llamada vulnerabilidad o agujero) no es atendida, el equipo puede infectarse con malware o tener algún malfuncionamiento. Los productos de software como sistemas operativos, programas y aplicaciones deben encontrarse en sus versiones más recientes y/o debidamente actualizadas. La mayoría del equipo de cómputo de uso común y su software está configurado para

actualizarse de manera periódica, sin embargo debe verificarse que efectivamente esté habilitada esta funcionalidad, de lo contrario se debe programar al menos una vez al mes un espacio para realizar las actualizaciones correspondientes.

C.2. ¿Revisas periódicamente el software instalado en el equipo de cómputo? Es importante revisar periódicamente qué tipos de programas se encuentran instalados en el equipo de cómputo, para verificar que se esté utilizando sólo software autorizado y evitar la instalación de software no deseado. Es de especial importancia evitar el uso de software para "bajar" o compartir archivos en equipos de cómputo de la organización, o con otros dispositivos personales, como tabletas o celulares, no sólo para evitar infringir la ley de derechos de autor, sino porque este software puede dar acceso a la información de un equipo a personas malintencionadas. También se debe vigilar que no se tenga instalado software sin licencia o "pirata", ya que éste podría estar infectado o simplemente no operar como el original y causar pérdida de información.

C.3. ¿Tienes medidas de seguridad para acceder al entorno de trabajo electrónico? El equipo de cómputo es susceptible a que cualquiera lo pueda utilizar, incluso personal no autorizado. Se deben tomar medidas de seguridad para evitar que alguien use un equipo de cómputo, medio de almacenamiento electrónico o acceda a un entorno de trabajo digital sin autorización, por ejemplo mediante el uso de contraseñas y/o cifrado, o de aplicaciones o dispositivos para la verificación de identidad del usuario.

C.3.1. Uso de contraseñas y/o cifrado: Toda información personal en medio digital debería estar protegida con bloqueos por contraseña y/o cifrado, para evitar su acceso no autorizado y posibles eventos de robo o pérdida de información.

C.3.2. Uso de contraseñas sólidas: Una contraseña débil es susceptible a ser "crakeada" es decir, averiguar la contraseña con herramientas de software o simplemente adivinando. Se debe evitar el uso de información personal o palabras simples en las contraseñas. Aunque es una recomendación usual el crear contraseñas mezclando caracteres especiales y números para hacerlas difícil de adivinar, también puede ser difícil para los usuarios memorizarlas, y provocar que recaigan en malas prácticas como tenerlas escritas a la vista. Una mejor alternativa puede ser el uso de "passphrases", es decir, frases o ideas completas por ejemplo, "me gusta la pizza de jamón", esta es una contraseña segura por ser muy larga y difícil de adivinar, pero es fácil de aprender. Otra opción es usar software de administración de contraseñas.

C.3.3. Bloqueo y cierre de sesiones: Cuando no se utilice el equipo de cómputo se debe bloquear o cerrar la sesión de usuario. Si un equipo no se va a utilizar por un periodo largo, se debe optar por apagarlo. Todo inicio de sesión debe requerir el uso de una contraseña, token, u otro mecanismo de autenticación. También se pueden considerar mecanismos de bloqueo y borrado remoto para los dispositivos móviles, de forma tal que se pueda restringir o eliminar la información aun cuando un equipo haya sido robado o extraviado.

C.3.4. Administrar usuarios y accesos: Se debe minimizar el uso de credenciales compartidas, es decir, que más de una persona tenga acceso al mismo servicio con el mismo usuario y contraseña por ejemplo, que dos personas distintas usen la misma identificación para usar la misma cuenta de correo. En su caso, cuando se implementan sistemas de tratamiento más complejos, por ejemplo bases de datos, se debe tener una correcta administración de los usuarios, contraseñas y privilegios de acceso (permisos para leer y modificar un archivo).

C.4. ¿Revisas la configuración de seguridad del equipo de cómputo? El equipo de cómputo, el software y en algunas ocasiones los medios de almacenamiento electrónico tienen configuraciones que permiten incrementar su nivel de seguridad. Los responsables deben habilitar las opciones de seguridad que permita a sus equipos estar más seguros por ejemplo, encender el firewall o habilitar las actualizaciones automáticas del antivirus, esta práctica, conocida como hardening o endurecimiento, puede requerir de cierto estudio y dedicación. Sin embargo, gracias a lo amigable de las nuevas herramientas así como a la información disponible en los sitios de Internet para soporte en línea del fabricante o proveedor, esta tarea es más fácil y podemos incrementar el nivel de seguridad significativamente. Es conveniente que todos los equipos de la organización, ya sean fijos o portátiles, mantengan un mismo nivel de configuración de seguridad.

C.5. ¿Tienes medidas de seguridad para navegar en entornos digitales? El uso cotidiano de los equipos de cómputo y de los entornos digitales hace que se den por obvias algunas conductas que podrían representar riesgo a los datos personales, por ello se deben implementar medidas de seguridad como:

C.5.1. Instalar herramientas antimalware y de filtrado de tráfico: el software malicioso o malware comprende diferentes tipos como virus, troyanos, gusanos, entre otros, que tiene por objetivo extraer datos de los usuarios como sus contraseñas o números de cuenta bancaria. Se debe instalar al menos, software antivirus y habilitar el filtrado de tráfico (como un firewall).

C.5.2. Reglas de navegación segura: Sólo se deben revisar sitios web esenciales para el negocio, evitando navegar en sitios no relacionados y mucho menos en sitios de riesgo como son los de descarga de contenido que violan los derechos de autor o pornográficos. Todos los empleados deben estar informados de los riesgos a los que se exponen por visitar sitios web que no son relevantes para sus funciones, también se les debe informar del peligro relacionado a la descarga de contenido, y la ventaja de verificar que el protocolo de conexión a los sitios web sea seguro es decir, verificar que en la dirección web aparezca https y la imagen de un candado, en lugar de que sólo sea http. Además, se puede optar por herramientas de cifrado de las comunicaciones como las redes virtuales privadas (o VPN, Virtual Private Network).

C.5.3. Reglas para la divulgación de información: Antes de enviar información a un tercero, almacenarla en cuentas de cómputo en la nube, publicarla en un sitio web, o compartirla en redes sociales, se debe evaluar si esta acción no está poniendo en riesgo a titulares o a personal de la organización.

C.5.4. Uso de conexiones seguras: Además de verificar que los protocolos de navegación sean seguros, se debe cuidar que la conexión también sea confiable. Cuando se trate de redes inalámbricas, éstas deberán contar con contraseñas y configuración segura (por ejemplo WPA o WPA2, evitando conectarse o configurar redes WEP o abiertas, susceptibles a que un externo malintencionado intercepte las comunicaciones). Asimismo es preferible evitar el uso de redes públicas, particularmente en los casos en que sea necesario llevar a cabo una transacción que implique el uso de información personal o contraseñas (por ejemplo, acceder a un portal bancario mediante un dispositivo portátil, utilizando una red WiFi provista por un sitio público, como un aeropuerto o una cafetería). De manera general, si no se puede asegurar la conexión, se deberá evitar cualquier tratamiento que involucre datos personales en línea.

C.6. ¿Cuidas el movimiento de información en entornos de trabajo digitales? El envío erróneo o intercepción de mensajes electrónicos (ya sea correo, mensajería instantánea, redes sociales, mensajes de texto a celular, entre otros) representa una grave fuga de información que puede perjudicar seriamente a los titulares. Es por esto que se debe considerar:

C.6.1. Validación del destinatario de una comunicación: Se han registrado muchos incidentes en los cuales la información personal se ha fugado a terceros debido a la transmisión errónea de mensajes electrónicos como correos, faxes, redes 33 sociales, entre otros. Antes de enviar un mensaje se debe

asegurar que el envío se realiza al destinatario correcto. Cuando se envíe un mensaje electrónico a varios destinatarios se debe revisar el método de envío y designación (por ejemplo en correo electrónico, CC o con copia, CCO o con copia oculta).

C.6.2. Seguridad de la información enviada y recibida: Cuando se envía información importante a través de mensajes electrónicos, ésta no se debería incluir bajo ninguna circunstancia en el cuerpo del mensaje, sino en un archivo individual protegido por contraseña/cifrado, la contraseña no debe estar contenida en el cuerpo del mensaje del que se envía la información, sino en un mensaje distinto o comunicarse por otro medio (por ejemplo, por teléfono). Cuando se recibe información en un mensaje electrónico, sin importar quien lo haya enviado, se debe ser cuidadoso con los archivos y ligas adjuntas cuando éstas no son esperadas, por ejemplo, un mensaje de un proveedor que pide revisar una cotización no solicitada abriendo un archivo adjunto o dando clic a una liga específica. En tal caso hay que verificar, (por ejemplo, por teléfono) con el remitente del mensaje y/o utilizar herramientas antimalware para verificar el contenido.