CÓMO AYUDAR A PREPARAR LA ENTIDAD, ANTE LA POSIBLE PÉRDIDA DE INFORMACIÓN

Rubiano Gomez Christian Fabian
Christian.rubiano10@gmail.com
Universidad Piloto de Colombia

Abstract— There are many news that can be read in some media related to security incidents in which theft or theft of confidential information occurs. This has very serious consequences, not only in the economic or legal, with fines or sanctions for breach of legislation on data protection; but in terms of image and loss of reputation and that several clients withdraw from the entity.
Is that the information, without a doubt, is one of the most important assets of the entity, regardless of whether it is small, medium or large, public or private sector.
Citizens often hear rumors, where it is exposed, that the information of people who are registered in a certain company, has been violated and on several occasions that was stolen and is offered on the Internet, causing panic, confusion or often fear among the citizenship in general.

Resumen— Son muchas las noticias que se pueden leer en algunos medios de comunicación relacionados con incidentes de seguridad en las que se producen robos o sustracciones de información confidencial. Esto tiene consecuencias muy graves, no solamente en lo económico o legal, con multas o sanciones por incumplimiento de legislación en materia de protección de datos; sino en cuanto a imagen y pérdida de reputación y que varios clientes se retiren de la entidad.
Es que la información, sin duda alguna, constituye uno de los activos más importantes de la entidad, independientemente de que esta sea pequeña, mediana o grande, del sector público o privado.
Los ciudadanos muchas veces escuchan rumores, donde se expone, que la información de las personas que están inscritas en determinada empresa, ha sido vulnerada y en varias ocasiones que fue hurtada y es ofrecida en Internet, causando pánico, confusión o muchas veces temor entre la ciudadanía en general.

Índice de Términos— Seguridad, información, concienciación, colaboradores, disponibilidad, privacidad, integridad.

I. INTRODUCCIÓN

En los últimos años, las tecnologías de la información y las comunicaciones se han convertido en la herramienta comúnmente más utilizada para optimizar los procesos y el mejoramiento hacia el eficaz funcionamiento en una entidad.
Por tal motivo, surgen a su vez amenazas y vulnerabilidades asociadas que pueden poner el riesgo los pilares fundamentales de la información, como lo son la disponibilidad, privacidad e integridad; estas amenazas y vulnerabilidades se encuentran disponible en las diferentes plataformas tecnológicas de la entidad, afectando de esta manera el desempeño normal de la entidad.
Los modelos de seguridad y privacidad indican pautas específicas para guiar a las entidades a robustecer sus plataformas y mitigar amenazas que traen consigo las tecnologías implementadas, sin embargo, un programa robusto de seguridad y privacidad de la información, no se debe centrar únicamente en el aseguramiento y robustecimiento de las plataformas y procesos, sino también debe involucrar los factores humanos (las personas).
Se ha venido argumentando entre el gremio de los profesionales de la seguridad informática y de la información que el eslabón más débil dentro de la cadena de seguridad, es el ser humano, que en muchos casos, son la principal causa de incidentes de seguridad dentro de un sistema determinado, esto, debido a que muchas veces no conocen sobre seguridad de la información o no son conscientes de su rol dentro de la entidad, por tal motivo, se mostrará una guía del contenido en los planes de concienciación que deben tener las entidades con sus colaboradores, para evitar la fuga de información sensible y confidencial o secreta de la entidad y a su vez puede ser utilizada para la información personal de los colaboradores, por lo que es necesario sensibilizarlos y capacitarlos sobre la importancia de la perseverancia de la disponibilidad, integridad y confidencialidad de la información.

II. LAS PREOCUPACIONES EN LAS EMPRESAS

En el informe presentado por ESET Security Report Latinoamérica 2012 del resultado de la participación del Technology Day que se realiza en Centroamérica, en Segurinfo de Sudamérica y su participación en varios eventos de seguridad de la información en países de toda la región; de acuerdo a datos revelados, se pueden observar que las mayores preocupaciones por parte de los equipos de TI y seguridad de la información de empresas de la región, los tres factores de mayor

relevancia son: el malware, la fuga de información (tema central de este artículo) y las vulnerabilidades en las aplicaciones.

Figura 1 Porcentajes Preocupaciones en la SI [8].

Con respecto a los incidentes sufridos, las personas responsables del área de TI afirman con amplio margen sobre las demás opciones que el malware continúa a la vanguardia entre los incidentes que más afectan a las organizaciones en la región latinoamericana.

Por otra parte, el robo de información, que representa la mayor preocupación para las empresas, afecta a menos del 10% de ellas.

Esto podría llevar a que muchas empresas no estén concentrando sus esfuerzos en la amenaza que más atenta contra sus organizaciones.

Otros números, sin embargo, no reflejan graves incidentes a pesar de la gran preocupación que representan para las empresas. Por ejemplo, el fraude interno y externo, es una preocupación que alcanza el 40 por ciento de los encuestados, no obstante solo afecta al 6% de ellos.

En esta temática, muchos de los encuestados coinciden que el fraude interno es más nocivo, ya que es más difícil de prever y el impacto puede ser muchas veces mayor. Además, muchos ejecutivos manifiestan que se trata de empleados desleales a la organización y por lo tanto consideran que la falta de confianza agrava los hechos en una cuestión de esta índole.

El porcentaje de pérdida de datos luego de analizar los datos recopilados arroja un 60.88% de preocupación en la seguridad de la información, "Figura 1"; lo que indica la necesidad de tomar acciones correctivas para mitigar estos casos y se observa la importancia de la educación y concienciación de los colaboradores como un pilar fundamental con el trato de la fuga de información dentro del plan de seguridad de la información de las entidades y su política de seguridad [1].

III. EDUCACIÓN Y CONCIENCIACIÓN

Para el 2016 ESET participó en diversos eventos relacionados con la seguridad de la información en toda Latinoamérica, donde aprovechó su presencia para encuestar a ejecutivos, gerentes y administradores de IT de las empresas asistentes, con toda la información recolectada se elaboró el ESET Security Report Latinoamérica 2017, en uno de sus apartes se habla sobre educación y concienciación; se evidencia que resulta difícil para los colaboradores de las entidades asumir que también son parte del sistema y que sus acciones pueden derivar en posibles incidentes.

Suelen delegar la seguridad únicamente a los componentes informáticos, sin ver su verdadero valor o el de la información que tratan a diario.

Por ello es importante capacitar a los diferentes estratos de las entidades, respecto a las amenazas informáticas que buscan atacar el factor humano mediante las técnicas de ingeniería social.

El porcentaje de las entidades que promueven actividades de concienciación periódicamente disminuye con los años, mientras que aumenta la cantidad de entidades que lo hace ocasionalmente o planea hacerlo, lo cual proyecta un mejor escenario.

Comparativa de realización de actividad de concientización en seguridad de la información

2014	2015	2016	
40,7%	33,2%	35,3%	Sí, periódicamente
38,1%	37,0%	39,3%	Sí, ocasionalmente
11,9%	13,6%	13,4%	No
9,3%	16,2%	12,0%	No, pero planean hacerlo a corto plazo

Figura 2 Comparativa Concienciación [9]

Además de realizar actividades de concienciación y orientar los procesos de seguridad hacia la usabilidad, se debe prestar atención a que tales actividades educativas resulten efectivas.

Muchas organizaciones ostentan un único programa de capacitación en seguridad de la información, cuando existe un universo de usuarios con diferentes aptitudes técnicas.

En consecuencia, el principal problema en la capacitación suele ser la falta de motivación de los usuarios.

Es importante, entonces, diseñar planes para audiencias específicas, construirlos sobre los resultados esperados y pensarlos para ganar la atención de su público buscando mantener a los distintos actores interesados en aprender.

Además, es necesario estipular mecanismos para mantenerlos al tanto de los cambios que sufre la política de la organización, puesto que estas se deben actualizar y modificar periódicamente.

Finalmente, el abordaje práctico de este tema requerirá un conocimiento extenso de la organización, una estrategia estructural, las herramientas correctas y mucha paciencia.

La asignación de responsabilidades referidas a las tareas de seguridad cibernética es un asunto más delicado de lo que parece.

Las mejores prácticas establecen que los roles en este ámbito deben ser independientes para brindar objetividad e imparcialidad; de lo contrario, el reporte de incidentes puede ser alterado o pasado por alto.

Desafortunadamente, un gran porcentaje de empresas no cuentan con los recursos para seguir estos lineamientos.

En 2016 más del 50% de los encuestados afirmó que el área de seguridad de la información de sus empresas depende de la gerencia de TI, mientras que solo el 12% ha establecido un área dedicada exclusivamente a tareas de seguridad informática.

La cantidad de empresas que no poseen ningún área dedicada a dichas tareas ha decrecido un 1% con respecto a 2015, llegando al 9% en 2016.

Esto nos indica que la mayoría de las organizaciones latinoamericanas se preocupan por la seguridad de sus activos, al punto de reflejarlo en su estructura organizacional.

La concesión de recursos para la protección de los datos suelen generar conflictos entre técnicos y gerentes ya que, a diferencia de inversiones en instalaciones o maquinaria, el beneficio es más difícil de percibir: las herramientas de seguridad no busca aumentar las ganancias, sino disminuir posibles pérdidas.

Es por esto que, a pesar de la abrumadora evidencia respecto a la evolución de amenazas informáticas, el número de empresas que no cuenta con un presupuesto para la seguridad supera año tras año a aquellas que sí lo hacen.

En 2016, solo el 37% de las empresas latinoamericanas destinó parte de sus ganancias a incorporar herramientas de control, lo cual supone un aumento del 1% respecto a 2015.

El concepto de "potencial pérdida" es, quizá, lo que desalienta a los administradores de empresas a invertir en minimizar el riesgo de ver sus activos digitales comprometidos. No obstante, deben entender que los ataques informáticos no pertenecen al campo del azar, sino al de la probabilidad; y hoy son casi una certeza. Estos indicadores demuestran la importancia de una correcta capacitación en seguridad de la información que se extienda incluso hacia los altos mandos de la jerarquía organizacional [2].

IV. CÓMO VALIDAR EL ESTADO DE RIESGO DE LA ENTIDAD

Uno de los principales activos en cualquier empresa o para muchas entidades el más importante es la información, se gestiona a través de diferentes dispositivos conectados a Internet, es por esto, que la seguridad informática se ha convertido en uno de los mayores retos que afrontan las entidades, sea cual sea su tamaño.

Una mala gestión de la seguridad informática puede tener tanto impacto económico como afectar a la reputación y la confianza de socios y clientes.

Muchas entidades depende para su funcionamiento de la información y de la tecnología que es usada para gestionarla, como los equipo portátiles, computadoras de escritorio, teléfonos inteligentes, tabletas, servidores, bases de datos, canales de comunicación y dispositivos de almacenamiento, entre los más usuales; al ser manipulados a diario, nunca nos detenemos a observar qué tan vulnerables pueden ser y si estamos manipulado correctamente estos equipos tecnológicos en el trabajo o en la vida diaria.

Una cita muy famosa dice que: "**Lo que no se define no se puede medir. Lo que no se mide, no se puede mejorar. Lo que no se mejora, se degrada siempre**."

La seguridad de la información no es una excepción y es por eso que es necesaria una aproximación seria y objetiva a los colaboradores de las entidades, que les permita determinar de manera fiable los riesgos a los que están expuestos y sus consecuencias.

Las entidades deben evaluar su estado de seguridad y avanzar a mayores niveles de protección de la información, es necesario hacer un análisis de riesgos para determinar la amenazas en el funcionamiento de la entidad y los aspectos a mejorar, con el fin de iniciar una medición y así poder llegar a una mejora continua de los procesos de la entidad.

Un análisis de riesgos es una evaluación inicial de los posibles riesgos de seguridad de la entidad en función de cómo son utilizados los elementos tecnológicos, como los equipos portátiles, computadoras de escritorio, teléfonos inteligentes, tabletas, servidores, bases de datos, canales de comunicación y dispositivos de almacenamiento.

Con preguntas como:

1. ¿Qué tecnologías utilizan en la entidad?
   - A. Correo electrónico
   - B. Página Web
   - C. Servidores Propios
   - D. Teletrabajo
   - E. Dispositivos Móviles.
2. ¿Cómo se mantienen sus sistemas tecnológicos al día?
   - A. Tratan de mantenerlos como se puedan
   - B. Los mantiene un amigo
   - C. Tiene ingeniero a cargo
   - D. Subcontratan el mantenimiento.
3. ¿Tiene algún sistema de protección en sus equipos de cómputo, portátiles y equipos de escritorio; estos se utilizan?
   - A. No lo sé
   - B. No, ninguno
   - C. Todos equipos tienen antivirus
   - D. Además de antivirus se tiene firewall
4. ¿Ha formado recientemente a sus colaboradores en seguridad informática?
   - A. Considera que no es necesario
   - B. Les dan información para leer
   - C. Reciben charlas
   - D. Al contratar colaboradores se requiere que tengan cursos de seguridad de la información.
5. ¿Controla el acceso al área segura o restringida de la entidad?
   - A. No, el acceso es libre
   - B. Se usan llaves y tarjetas de acceso
   - C. Se tiene elementos físicos que bloquean las puertas
   - D. Se tiene cámaras de seguridad
   - E. Hay guardias de seguridad que controlan el acceso.
6. ¿Se ha definido una política de gestión de contraseñas entre sus colaboradores?
   - A. No
   - B. Si. El usuario selecciona su contraseña

C. Los servidores obligan a cambiar la contraseña periódicamente
D. Sí, tenemos una política de gestión de contraseñas de obligatorio cumplimiento.

7. ¿Cuándo una información aparentemente ya no es útil, como se deshace de esta información, los soportes y sistemas que ya no utiliza?
   A. Se tiran a la basura
   B. Se tiene, una destructora de papel y el resto a la basura
   C. Subcontratan destrucción
   D. Se definió una política de destrucción de papel y soportes; según la norma vigente.
8. ¿La entidad tiene presencia en las redes sociales?
   A. Sí, tienen cuenta en Twitter o Facebook, no estoy seguro
   B. Se Tiene un par de redes sociales y se actualizan cuando hay algo importante que comunicar
   C. Se tiene presencia en varias redes sociales y una persona que actualiza la información
   D. No, en ninguna
9. ¿Tiene cuenta de correo corporativa; si es así; cuánto tiempo podrían estar sin acceso al correo electrónico sin que esto genere un problema con los clientes y colaboradores?
   A. No
   B. Menos de 4 horas
   C. Menos de un día
   D. Entre 1 y 5 días
   E. Más de 5 días, no es fundamental para la entidad.
10. ¿Con qué frecuencia realiza copias de seguridad de sus dispositivos de almacenamiento y su correo electrónico?
   A Cuando me acuerdo
   B. Nunca / no lo sé
   C. Una vez al mes
   D. Cada semana
   E. Todos los días.
11. ¿Existen conexiones remotas desde fuera hacia algún sistema de la entidad?
   A. Empleados y Clientes a través de la página Web
   B. Los empleados acceden a través de una aplicación Web/Intranet
   C. Solo el administrador de forma segura
   D. Los empleados acceden a través de escritorio remoto
   E. No, nunca
12. ¿Sus servidores y equipos de comunicación donde se encuentran en la entidad?
   A. Están en una zona donde circula personal externo e interno
   B. En un cuarto compartido
   C. En un cuarto con acceso restringido
   D. En las instalaciones del proveedor
13. ¿Si ocurriera un desastre catastrófico, tiene algún plan B para utilizar los sistemas de información de la entidad?
   A. No
   B. Algo pero no se ha probado
   C. Si, está definido pero no lo hemos comprobado
   D. Sí, bien definido y comprobado; con copias de seguridad
   E. Sí, bien definido y comprobado; con copias de seguridad en otra ubicación fuera de la empresa
   F. Sí, tenemos incluso servidores redundantes
14. ¿El personal técnico de la entidad tiene conocimiento específico sobre seguridad de la información?
   A. No/No estoy seguro
   B. Creo que sí, pero con conocimientos básicos
   C. Si, han recibido información técnica
   D. Sí, todos los colaboradores están certificados en seguridad de la información.
15. ¿Con qué frecuencia actualiza el software de los sistemas de información y equipos de cómputo de la entidad?
   A. Nunca
   B. De vez en cuanto
   C. Se actualiza cuando se informa por parte del fabricante o proveedor
   D. Están al día en las actualizaciones [3].

Las respuestas que se dan en este artículo son de referencia y pueden ser utilizadas para una encuesta en la entidad.

Una vez terminada la evaluación con este formulario de preguntas como base, y teniendo en cuenta que cada pregunta tiene una opción de respuesta entre las que se seleccionen para poder tabularlas y tener una medición del estado inicial, se procede a tomar una acción ante los resultados.

Para este artículo y a manera de ejemplo, el riesgo generado después de la tabulación de las respuestas indica un riesgo “alto” en el ámbito de los colaboradores; ahora se debe crear una cultura de seguridad en la entidad entre los colaboradores.

V. CÓMO ESTABLECER UNA CULTURA DE SEGURIDAD EN LA ENTIDAD

«Una cadena es tan fuerte como su eslabón más débil»

Esta frase tan popular dentro del gremio de la seguridad de la información significa que aunque las entidades inviertan mucho en dispositivos tecnológicos y en soluciones técnicas para proteger de manera adecuada los sistemas de información, si alguno de ellos falla, toda la seguridad se ve comprometida.

Los colaboradores y los usuarios en general son un eslabón más de la cadena,... Y la experiencia ha ido demostrando que es uno de los eslabones más débiles, por donde esta cadena de seguridad se rompe.

Es necesario que las entidades inviertan en la formación en seguridad de la información a los colaboradores y usuarios; se tiene que ser consciente de que a la hora de hablar de seguridad de la información, la tecnología nunca es suficiente.

Es importante, pero a la hora de la verdad los auténticos protagonistas de la seguridad en las entidades son los colaboradores que son los que gestionan y utilizan los sistemas de información de la entidad.

Uno de los primeros pasos y el más complejo de alcanzar es desarrollar e integrar una cultura de seguridad dentro de la entidad; en primer lugar, por el tiempo que se requiere y sus

acciones de mejora continua y en segundo lugar, y muy importante, es porque se habla de personas y lograr que interioricen en sus actividades diarias, una manera de trabajar que garantice hacer bien las cosas en materia de seguridad de la información, no es tarea sencilla.

Al implementar protocolos de seguridad en las entidades, los colaboradores los ven como una complicación y hasta una molestia; su percepción de la seguridad de la información es incómoda y lo ven como una demora en sus actividades diarias imponiendo limitaciones.

Es necesario revertir la visión negativa y concienciar a los colaboradores sobre los beneficios que esto conlleva y crear una auténtica cultura de la seguridad de la información en la entidad.

Un adecuado nivel de seguridad debe contar como mínimo con los siguientes aspectos:

1. Realizar acciones de formación en seguridad de acuerdo al perfil de los colaboradores.
2. Establecer políticas, normativas y procedimientos de seguridad.
3. Supervisar que se cumplan las buenas prácticas en seguridad.
4. Realizar acciones de sensibilización y concienciación en seguridad para los colaboradores [4], [5].

Un programa efectivo de capacitación y sensibilización de la seguridad de la información, debe explicar de manera apropiada las reglas de comportamiento adecuadas para el uso de los sistemas y la gestión de la información, que generalmente está definido en la política de seguridad y procedimientos de seguridad de la información que la entidad requiere que sean cumplidos por parte de todos los colaboradores y usuarios del sistema de información.

Si alguna de las políticas de la información no se cumple en su totalidad, debe existir una sanción, siempre y cuando el colaborador haya sido adecuadamente informado y capacitado sobre el contenido de la seguridad de la información que le corresponde, teniendo en cuenta su rol dentro de la entidad y las responsabilidades sobre su gestión con la información.

Con base en lo anterior, un plan de capacitación, sensibilización y comunicación efectivo, debe contener las siguientes fases en su contenido:

1. **Diseño**: Identificar las actividades a ser realizadas para cumplir con las metas de entrenamiento de la entidad.
2. **Desarrollo**: Esta fase se enfoca en las fuentes de información disponible, alcance y contenidos del material de entrenamiento.
3. **Implementación**: Es la definición de la manera efectiva en la comunicación del material diseñado y del cómo hacer llegar a los colaboradores de manera amena y sensible, el mensaje de la implementación de la seguridad de la información.
4. **Mejoramiento**: Esta fase indica cómo mantener el programa actualizado, monitorear su efectividad y saber qué complementos pueden adicionar para mejorar su funcionamiento.

Es importante definir los términos sensibilización, entrenamiento y educación.

Sensibilización: Es un proceso que tiene como objetivo principal, impactar sobre el comportamiento de una población o reforzar buenas prácticas sobre algún tema en particular. Ejemplo: Uso correcto de contraseñas, consecuencias reales sobre prestar una contraseña y qué hacer si no recuerdo mi contraseña.

El éxito de la sensibilización es lo práctico y su simplicidad en que esta información es entregada, para captar la atención del aprendiz.

Entrenamiento: Busca enseñar habilidades, que permitan a una persona ejecutar funciones específicas asignadas su cargo.

Un programa de entrenamiento no busca certificar (aunque puede llegar a hacerlo), pero puede tener mucha temática relacionada con un curso de certificación.

Ejemplo: Un curso de seguridad de la información, enfocado a administración de riesgos, ciclo de vida del servicio de seguridad y controles operacionales.

Un curso sobre administración de plataformas de verificación de registros (Log).

Educación Formal: Se define como todos los niveles y habilidades de seguridad envueltos en un único cuerpo de conocimiento.

Ejemplo: Programa de estudios de educación superior, postgrados, etc.

No Formal: Busca asegurar que los usuarios desde el más principiante hasta el más experimentado, tengan los conocimientos suficientes para desempeñar sus roles.

Esto se logra a través de certificaciones, que ofrecen proveedores de plataformas específicas, sistemas operativos etc. O algunas otras relacionadas con conceptos de seguridad informática (gestión, planeación etc.).

Esta parte de desarrollo profesional, depende de cada institución, si requiere de certificaciones para desempeñar bien sus roles o si son motivo para brindar algún tipo de bonificación adicional al empleado por su preparación. [6]

Para ello se tienen que implementar medidas preventivas y reactivas en la entidad, destinadas a preservar y proteger los pilares fundamentales de la información, la confidencialidad, la disponibilidad y la integridad.

1. **Confidencialidad**: es la garantía de acceso a la información de los usuarios que se encuentran autorizados para tal fin.
2. **Integridad**: es la preservación de la información completa y exacta.
3. **Disponibilidad**: es la garantía de que el usuario accede a la información que necesita en ese preciso momento [7].

Se debe tener en cuenta que la mejor metodología para elaborar el plan de capacitación es el ciclo PH VA (planear, hacer, verificar y actuar).

Ahora se procede a describir todas las actividades que realizan en cada una de las cuatro fases del ciclo Deming (PH VA):

1. **Planificar**: durante esta fase tiene lugar la creación de un sistema de gestión de seguridad de la Información, con la definición del alcance y la política de seguridad. Para comenzar se debe realizar un análisis de riesgos que refleje la situación actual de la entidad. Una vez realizado el análisis, se obtienen unos resultados que definirán el plan de tratamiento de riesgos, que conlleva la implementación en la empresa de unos controles de seguridad con el objetivo de mitigar los diferentes riesgos no asumidos por la dirección.

2. **Hacer**: durante esta fase de la implementación se debe centrar en el plan de tratamiento de riesgos, es decir, su ejecución. Se debe incluir la formación y la concienciación de los trabajadores de la organización en materia de seguridad y se deben conocer, la definición de métricas e indicadores que se utilizarán para evaluar la eficacia de los diferentes controles implementados.
3. **Verificar**: esta fase conlleva la realización de diferentes tipos de revisión en los que se comprobarán, la correcta implementación del sistema de gestión de seguridad de la información según ISO 27001. Para ello, se deben realizar auditorías internas independientes y objetivas, además de llevar a cabo una revisión global del sistema de gestión de seguridad de la información por la alta dirección de la empresa, persiguiendo el fin de marcarse nuevas metas a cumplir durante el próximo ciclo del sistema de gestión de seguridad de la información.
4. **Actuar**: El resultado obtenido de las revisiones, debe quedar reflejado en la definición e implementación de las diferentes acciones correctivas, preventivas o de mejora con las que se consigue avanzar en la consecución del sistema de gestión de seguridad de la información, siendo un sistema eficaz y eficiente [8].

Con estos conceptos bien interiorizados se procede a realizar la formación en seguridad de la información de los colaboradores.
Se debe ser consciente de la importancia de formar a los colaboradores en seguridad de la información, no solo desde el punto de vista de protección de datos personales, sino también, en materia de toda la información que trata la entidad: datos de clientes, tarifas, proveedores, constructoras, créditos entregados, etc.
No todos los colaboradores de la entidad requieren el mismo grado de formación en materia de la seguridad de la información.
La formación de un colaborador técnico que gestiona los servidores, no debe ser la misma, que la de un colaborador o usuario final que solamente dispone de un acceso limitado a un parte de los dispositivos informáticos, donde puede acceder a la información de la entidad y solo es fundamental para sus actividades diarias.

A Personal técnico

El personal técnico del departamento de informática, es quien precisa más formación en materia de seguridad y con un mayor grado de especialización.
Se deben poner a disposición de los administradores de sistemas, los recursos y mecanismos adecuados para formarse o auto formarse en aspectos relacionados con la seguridad de los sistemas y aplicaciones que dan soporte a los procesos de negocio de nuestra entidad.
Dentro de estos aspectos, se pueden señalar algunos tan críticos como:
Un punto clave para tener en cuenta, es que, gracias al cambio constante que sufre la tecnología, el personal técnico debe estar en continuo proceso de formación, ya que en muchos casos, estos colaboradores se convierten en el soporte y asesoría de los colaboradores o usuarios finales, en el uso de la tecnología y sus necesidades de seguridad, en cuanto a la información, tanto personal, como de la entidad.

B Colaboradores o usuarios finales

Requieren de un alto grado de sensibilización sobre la seguridad y las reglas de comportamiento adecuadas con los sistemas que tienen a disposición.
Actualmente en las entidades, la gran mayoría de sus colaboradores trabajan con equipos portátiles o de escritorio y

Figura 3 Aspectos Clave [10]

con los dispositivos móviles, que les permiten conectarse a los sistemas de información de la entidad.
La seguridad hoy en día no se debe limitar únicamente a los aspectos técnicos, también deben incorporar otros ámbitos, como el organizativo y el legal, rebasando así las competencias del departamento de informática o sistemas.
Es necesario tener en cuenta, que existen departamentos como el de recursos humanos o el comercial, que por su gestión con los clientes, deben conocer aspectos vitales en la gestión de la seguridad de la información, como la ley de el Habeas Data, que trata del derecho fundamental que tiene toda persona para conocer, actualizar y rectificar, toda aquella información que se relacione con ella y que se recopile o almacene en bancos de datos [9].
El no hacerlo, puede provocar que la entidad incurra en situaciones de riesgo, tanto a nivel de protección de datos, como a nivel de infracciones legislativas.
En este caso, es necesario que algunos colaboradores de la entidad reciban formación específica e incluso contar con el asesoramiento de algún experto en legislación, aplicada a la protección de datos en un entorno de empresa estatal; puesto que la entidad tiene como principales clientes, personas naturales y resulta fundamental, la formación en el ámbito de

protección de datos personales, ya que el nivel de riesgo asociado puede ser muy alto.

El tratamiento de los datos personales de los clientes, debe realizarse partiendo de unas determinadas condiciones, tanto a nivel técnico como legal, que son establecidas en la ley de protección de datos personales Habeas Data.

Por ejemplo, los colaboradores de atención al cliente deben estar perfectamente capacitados para saber cómo atender una petición ejercicio de los derechos de conocer, actualizar y rectificar, pues existen unos tiempos muy ajustados para atender este tipo de peticiones.

Otros aspectos a considerar en la formación de los colaboradores de la entidad en cuanto a seguridad de la información son:

Figura 4 Otros Aspectos [11]

Todos los colaboradores de la entidad con acceso a los sistemas de información corporativos, deben recibir formación relacionada con buenas prácticas en materia de seguridad de la información, en su puesto de trabajo y en el desempeño de sus actividades diarias.

VI. MATERIAL SENSIBILIZACIÓN

El plan de sensibilización impacta a todos los colaboradores de la entidad, todos deben ver la información socializada como una responsabilidad compartida en seguridad de la información y, a su vez, saber que todos son igualmente importantes en esta labor.

A Política de seguridad

Para realizar una efectiva implementación de las políticas de seguridad de la información, se necesita cumplir con una serie de fases que son sugeridas en este artículo y las cuales tienen como objetivo, que la entidad desarrolle, apruebe, implemente, socialice e interiorice, las políticas para un uso correcto por parte de los colaboradores, proveedores y usuarios de la entidad.

Es importante contar con una política de seguridad de la información, ya que son ellas, las que guiarán el comportamiento profesional y personal de los colaboradores, proveedores y usuarios sobre la información obtenida, generada o procesada en la entidad, las políticas permiten a la entidad establecer mejores prácticas de seguridad y asegurar el cumplimiento de los requisitos legales a los cuales están obligados como entidad.

Como primera fase, está el desarrollo de las políticas, donde la entidad debe responsabilizar las áreas para la creación, la estructuración, escribirlas, revisarlas y aprobarlas; para llevar a buen término esta fase, se requiere verificar los siguientes aspectos:

Justificación de la creación de política: Debe identificarse el por qué, la entidad requiere la creación de la política de seguridad de información y determinar el control al cual hace referencia su implementación.

Alcance: Debe determinarse el alcance, ¿A qué población, áreas, procesos o departamentos aplica la política?, ¿Quién debe cumplir la política?

Roles y Responsabilidades: Se debe definir los responsables y los roles para la implementación, aplicación, seguimiento y autorizaciones de la política.

Revisión de la política: Es la actividad, mediante la cual la política una vez haya sido redactada, pasa a un procedimiento de evaluación por parte de otros colaboradores o grupo de colaboradores, que evalúan la aplicabilidad, la redacción y se realizan sugerencias sobre el desarrollo y creación de la misma.

Aprobación de la Política: Se debe determinar al interior de la entidad, el colaborador o rol de la alta dirección, que tiene la competencia de formalizar las políticas de seguridad de la información, mediante la firma y publicación de las mismas.

Es importante que la alta gerencia de la entidad, muestre el interés y apoyo, en la implementación de dichas políticas.

Como segunda fase, está el cumplimiento de la política de seguridad de la información, donde todas aquellas políticas escritas deben estar implementadas y relacionadas a los controles de seguridad de la Información, esto con el fin de que exista consistencia entre lo escrito en las políticas versus los controles de seguridad implementados y documentados.

La fase de comunicación, mediante la cual se da a conocer las políticas de seguridad de la información a los colaboradores, proveedores y/o clientes de la entidad.

Esta fase es muy importante, toda vez que, del conocimiento del contenido de las políticas de seguridad de la información, depende gran parte del cumplimiento de las mismas; esta fase, de la implementación, también, permitirá obtener retro alimentación de la efectividad de las políticas, permitiendo así realizar excepciones, correcciones y ajustes pertinentes.

Todos los colaboradores, proveedores y/o clientes de la entidad, deben conocer la existencia de las políticas, la obligatoriedad de su cumplimiento y la ubicación física de tal documento o documentos, para que sean consultados en el momento que se requieran.

La fase de monitoreo, en esta fase, es importante que las políticas de seguridad de la información, sean monitoreadas para determinar la efectividad y cumplimiento de las mismas, deben crearse indicadores, para verificar de forma periódica y con evidencias, que la política funciona, y si debe, o no, ajustarse.

Una fase de mantenimiento es la encargada de asegurar que la política de seguridad de la información, se encuentra

actualizada, integra y que contiene los ajustes necesarios y obtenidos de las retroalimentaciones.

Una última fase, es la de retiro, donde se hace la eliminación de una política de seguridad de la información, en cuanto esta, ha cumplido su finalidad o la política, ya no es necesaria en la entidad.

Esta es la última fase, para completar el ciclo de vida de las políticas de seguridad de la información y requiere que este retiro, sea documentado, con el objetivo de tener referencias y antecedentes sobre el tema.

B Temas para la sensibilización de los funcionarios.

Los siguientes son temas que pueden ser desarrollados con todos los colaboradores de la entidad:

1. Clasificación de la información.

La clasificación de activos de información, tiene como objetivo asegurar que la información recibe los niveles de protección adecuados, ya que, con base, en su valor y de acuerdo a otras características particulares, requiere un tipo de manejo especial.

El sistema de clasificación de la información, que podría definirse en la entidad, se debe basar, en las características particulares de la información, contempla la cultura y el funcionamiento interno y busca dar cumplimiento a los requerimientos estipulados en los estándares 27001:2013, ISO 27002, e ISO 27005.

2. Uso seguro del correo electrónico.

Se deben dar las pautas generales para asegurar una adecuada protección de la información de la entidad, en el servicio y uso del servicio de correo electrónico por parte de los colaboradores autorizados.

El personal del área de tecnologías y sistemas de la información no debe dar a conocer su clave de usuario a terceros de los sistemas de información, sin previa autorización del jefe del área de tecnologías y sistemas de la información.

Los usuarios y claves de los administradores de sistemas y del personal del área de tecnologías de la información y sistemas de la información son de uso personal e intransferible.

Los colaboradores de la entidad deben emplear obligatoriamente las claves o contraseñas con un alto nivel de complejidad y utilizar los servicios de autenticación fuerte que posea la entidad de acuerdo al rol asignado.

3. Prácticas de navegación segura.

Se deben establecer unos lineamientos, que garanticen la navegación segura y el uso adecuado de la red por parte de los colaboradores y usuarios finales, evitando errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones Web.

4. Uso de los activos.

En esta política, se debe lograr y mantener la protección adecuada de los activos de la información, mediante la asignación a los colaboradores, que deban administrarlos, de acuerdo a sus roles y actividades.

5. Gestión de contraseñas.

Se debe concienciar y controlar a los colaboradores, para que apliquen buenas prácticas de seguridad en la selección, uso y protección de claves o contraseñas, las cuales constituyen un medio de validación de la identidad de un colaborador y consecuentemente, un medio para establecer derechos de acceso a las instalaciones, equipos o servicios informáticos.

Se debe seguir una política de cambio de clave o contraseña y utilizar el procedimiento de salvaguarda o custodia de las claves o contraseñas en un sitio seguro. A este lugar solo debe tener acceso el jefe del área de tecnologías de la información y sistemas de información o el quien cumpla este rol en la entidad.

6. Borrado seguro de la información.

Se debe asegurar, una perfecta disposición final de la información, realizando un borrado o formateo del dispositivo de almacenamiento; garantizando una copia de seguridad de la información para la entidad.

Para los documentos físicos, se debe proceder a una destrucción segura de los documentos y una correcta eliminación.

Los temas a tratar no solamente están relacionados con el uso de la tecnología, sino que abarcan otros ámbitos:

7. Escritorio limpio.

Definir las pautas generales para reducir el riesgo de acceso no autorizado, pérdida y daño de la información, durante y fuera del horario de trabajo normal de los usuarios y colaboradores.

Dejar un equipo sin protección durante el almuerzo, la comida, o incluso por la noche, es equivalente a no utilizar contraseña de acceso.

Debe enseñarse al colaborador, cómo pueden bloquear su equipo de manera sencilla.

Asimismo, se debe indicar al empleado, que es necesario apagar su equipo al acabar la jornada laboral.

Además, se deben establecer las políticas de seguridad, técnicas adecuadas para que el bloqueo del puesto de trabajo, se realice de manera automática tras un tiempo prudencial, sin actividad en el equipo.

También, se pueden establecer medidas, para que se apaguen automáticamente los equipos, cuando finalice la jornada laboral.

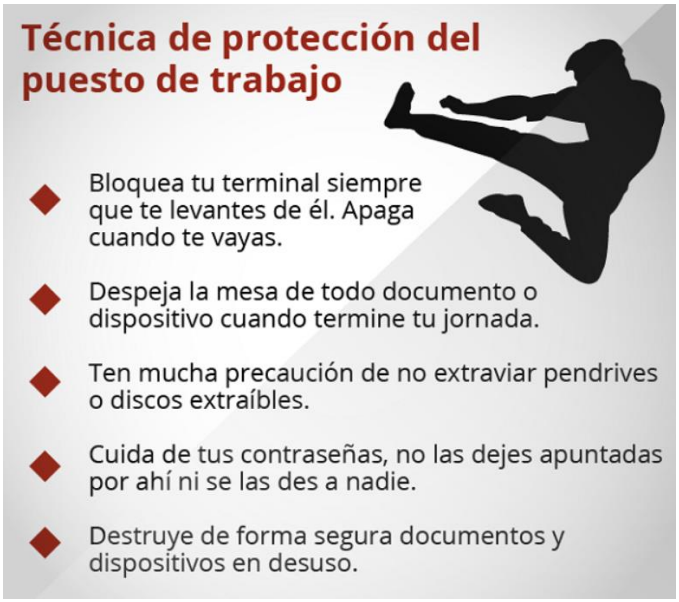

Figura 5 Protección puesto de trabajo. [10]

8. Copias de seguridad.

Una copia de seguridad, también conocida como backup, es un duplicado que se realiza sobre archivos o aplicaciones contenidas en un computador de escritorio o portátil, con la finalidad de recuperar los datos, en el caso, de que el sistema de información sufra daños o pérdidas accidentales de los datos almacenados [10].

Todo plan de contingencia de una empresa, requiere contar con una planificación adecuada de las copias de seguridad, que se realizan, ya que la pérdida de datos, puede poner en peligro la continuidad del negocio.

Guardar información relacionada con la actividad de la entidad o sus clientes en el disco duro del computador es, por lo general, una mala idea.

Los equipos de escritorio están expuestos a fallos o ataques que pueden suponer la pérdida de datos valiosos, los portátiles también, y además, pueden ser robados o perderse.

Una buena práctica, es pedir a los colaboradores que almacenen los archivos, en los servidores de la entidad o en algún servicio en la nube, proporcionado por la entidad.

Si de todos modos deben conservar información en el disco duro de sus equipos de trabajo, es fundamental que realicen copias de seguridad a menudo, para poder recuperar el material, si surge algún inconveniente.

La entidad al mantener copias de seguridad periódicas de su información, es capaz de recuperarse más rápido, lo ideal es que se cuente con una alternativa, que haga estas copias de manera automática y periódica; también, pueden cifrar estas copias, como una medida de seguridad adicional y resguardarlas en un sitio diferente a la entidad misma; una correcta gestión de las copias de seguridad, permite mantener en todo momento, la integridad, confidencialidad y disponibilidad de la información.

9. Posibles escenarios de fuga de información.

Este tema es el más importante para la sensibilización, y objetivo del artículo, es llegar a todos los colaboradores de la entidad, para que interioricen y hagan parte de la seguridad de la información; vamos a ver, los temas que deben tener mayor recordación entre los colaboradores de la entidad.

Confirma la identidad de todo aquel que solicite información.

Un consejo especialmente útil para recepcionistas, colaboradores de 'call center' o soporte técnico, personal de recursos humanos y otros profesionales cuyo trabajo, de una u otra forma, requiere proporcionar datos en determinadas ocasiones.

Los atacantes, se aprovechan en muchas ocasiones, de la ingenuidad o la buena fe de estos colaboradores, para recabar información de la manera más sencilla y obvia: pidiéndola.

Figura 6 Defensa ingeniería social. [10]

Para ello, se hacen pasar por proveedores, clientes u otros colaboradores de la entidad que tienen una excusa, aparentemente legítima.

Es muy importante que los colaboradores de la entidad, conozcan estas tácticas y se aseguren, de que la persona, al otro lado del teléfono o el correo electrónico, es quien dice ser, antes de proporcionar información alguna.

Las contraseñas, siempre seguras.

Si, con las claves que utilizamos para nuestras cuentas personales, hay que tener ciertas precauciones presentes, con las que dan acceso a información de la entidad, todavía más.

Lo primero, seguir las recomendaciones habituales para crear una buena contraseña: no usar la misma en varios sitios (y menos si uno es personal y otro de empresa), evitar que contenga detalles sobre el colaborador demasiado evidentes (fecha de cumpleaños, nombre de su perro, su equipo de fútbol favorito, etc.) y procurar que esté compuesta por números y símbolos, además de letras, combinando, mayúsculas y minúsculas.

Además, en el contexto empresarial, es importante pedir a los colaboradores que se abstengan de apuntar la clave en un post-it (algo por desgracia bastante habitual) o en una nota debajo del teclado.

Por último, y volviendo al punto anterior, jamás reveles tu contraseña a alguien que la solicita por teléfono o correo electrónico, aunque asegure que trabaja en la entidad, en el área técnica o finge ser un proveedor o cliente habitual de la entidad.

Correo electrónico.

Una de las principales herramientas que utilizan los delincuentes cibernéticos para colarse en una entidad y robar datos, sigue siendo el correo electrónico. Si los colaboradores tienen una cuenta corporativa, lo primero que deben procurar, es no utilizarla para fines personales, ni proporcionarla en sitios de acceso público (por ejemplo, en un foro o una página web a la que todo el mundo puede acceder). De lo contrario, podría acabar en una lista de envío de spam y recibir correos que, además de molestos, pueden resultar peligrosos.

En general, el mejor consejo que se les puede dar a los colaboradores, respecto al correo electrónico, es que jamás respondan al correo que proviene de un remitente sospechoso o desconocido, ni mucho menos, abran o descarguen sus adjuntos.

Podrían esconder malware, capaz no solo de afectar a su ordenador sino, en algunos casos, a toda la red de la entidad. Cuando hablamos de amenazas de seguridad a los sistemas de información, hay una entre todas ellas que es recurrente y que ha logrado sobrevivir a más de tres décadas. Ha crecido, evolucionado y se ha adaptado conforme ha ido avanzando la tecnología: es el código malicioso (malware) o, en lenguaje coloquial más conocido como los «virus».

Actualmente, la variedad es tal, que referirse a estos como «virus» es hablar únicamente de una de las formas que pueden adoptar estos programas. Es más, el término «virus» hace referencia a una característica muy particular, la capacidad para copiarse a sí mismos, de forma similar a como lo hacen los que atacan a organismos biológicos, como es el caso de los virus humanos. Esta analogía con los virus biológicos va más allá de la capacidad de auto replicarse en el sistema atacado, ya que ambos causan daños al sistema que los alberga, se pueden

prevenir o incluso eliminar, pero también pueden mutar y evolucionar, adaptándose al medio.

La tipología es muy extensa, tanto como lo son las actividades para las cuales son diseñados. Algunos de los más conocidos son los siguientes:

Virus. Son programas capaces de crear copias de sí mismos, de forma que anexan estas copias a otros programas legítimos o en zonas especiales de soportes de almacenamiento, como en el caso de los discos duros o los sistemas de almacenamiento externo. Necesitan de la intervención del usuario para propagarse, utilizando diversas vías para conseguirlo como ingeniería social, descarga de ficheros, visita a páginas web de dudosa reputación, utilización incorrecta de dispositivos externos de memoria, correo electrónico, etc. Los virus suelen diseñarse para producir todo tipo de problemas en un ordenador, como volverlo más lento, bloquearlo o impedir el acceso a la información.

Gusanos. Son un tipo de código malicioso que se diseñó originalmente para su propagación a través de redes de comunicaciones, mediante el uso de servicios como el correo electrónico. En la actualidad, son capaces de replicarse y propagarse a través de la red sin necesidad de la intervención del usuario, a través de servicios de mensajería instantánea o de redes de intercambio de ficheros (P2P). Suelen aprovechar las vulnerabilidades de los sistemas operativos o de las aplicaciones instaladas (sobre todo en las que no están debidamente actualizadas), y su velocidad de propagación es muy alta en comparación con los virus, alcanzando además, zonas geográficas muy amplias. En realidad las técnicas de propagación de los gusanos son usadas por otros tipos de código malicioso.

Troyanos. Son programas que se ocultan o esconden en programas legítimos, como aplicaciones de ofimática, facturación, documentos de trabajo, fotos, etc. para proporcionar acceso no autorizado al sistema infectado.

Su propagación requiere de la acción directa del usuario para su descarga e instalación. Los troyanos se han especializado en el robo de credenciales bancarias y son una de las mayores amenazas en la actualidad, por la proliferación de este tipo de código malicioso, muy utilizado por los delincuentes cibernéticos.

Existen diferentes tipos, en función de la forma en que afectan el comportamiento del equipo infectado:

Backdoors, o troyanos de acceso remoto, que proporcionan un acceso total del equipo para que el atacante pueda realizar cualquier tarea en él.

Keyloggers, o malware que registra las pulsaciones que realizamos con el teclado, permitiendo averiguar las contraseñas o cualquier otro tipo de información privada que hayamos tecleado.

Stealers, que acceden y roban información privada almacenada en los equipos para enviárselas al atacante. Información como las contraseñas que se almacenan o memorizan en los diversos programas como navegadores, mensajería instantánea, correo electrónico, etc.

Ransonware, que tiene como objetivo bloquear y secuestrar el acceso a un equipo de trabajo o a la información que contiene -cifrando el contenido bloqueado-, con el fin de pedir un rescate económico a cambio de su desbloqueo.

Spyware. Son programas destinados a la recolección de información sobre la actividad de un usuario. Están diseñados para pasar inadvertidos, de forma que el usuario no perciba ningún tipo de actividad fuera de lo normal. Cuanto más tiempo pasen sin ser detectados, más información será capaz de recopilar, que luego es enviada a servidores o direcciones de correo que la recogen y la usan para todo tipo de fines.

Adware. Son programas diseñados para mostrar publicidad al usuario. Suelen ser instalados junto con otros programas legítimos. Estos programas pueden recopilar información sobre la actividad del usuario con objeto de mostrar publicidad dirigida y específica. En general este tipo de aplicaciones son más bien una molestia, pero su instalación puede suponer un peor funcionamiento del ordenador y también, el acceso a sitios y páginas web que pueden contener a su vez código malicioso.

Hoy en día, el malware se ha vuelto muy complejo, hasta el punto de que es difícil clasificarlo o saber cómo actúa, puesto que existen algunos tipos que incorporan características de los virus, pudiendo actuar como un troyano, con las capacidades de propagación de un gusano y recopilando información como si se tratara de spyware. En definitiva, el código malicioso es capaz de propagarse a través de diversas vías y medios y, una vez llega a un sistema, es capaz de realizar múltiples tareas, incluso son capaces de recibir órdenes o funcionar como parte de un grupo de programas maliciosos.

Conocer cómo funcionan los diferentes tipos de malware, nos puede ayudar a prevenir posibles infecciones que afecten a nuestros sistemas y a la información almacenada en ellos.

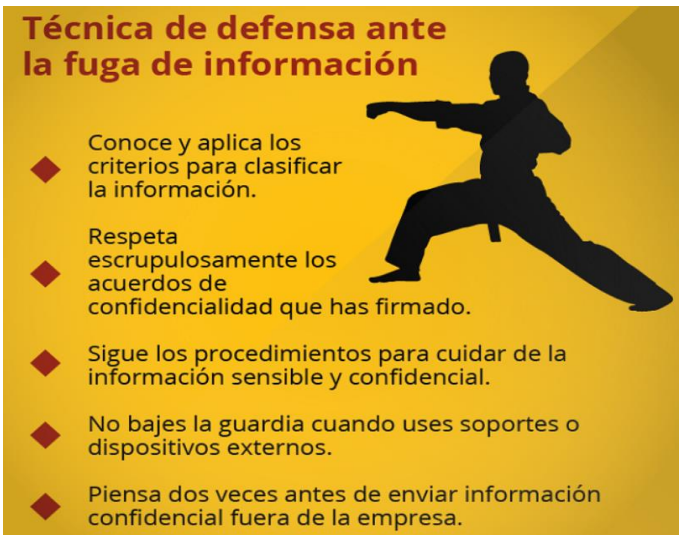

Figura 7 Defensa fuga de información [10]

No instalar programas de fuentes desconocidas

De nuevo, solo deben confiar en lo que conocen: es habitual que las entidades restrinjan la capacidad de sus colaboradores, para instalar nuevos programas en sus equipo de cómputo, de escritorio o portátiles, mediante los permisos del sistema operativo.

No obstante, si tienen credenciales suficientes para ejecutar nuevo software en sus equipos de cómputo, de escritorio o portátiles, se les debe pedir que eviten descargar de páginas que no conozcan o resulten sospechosas.

De hecho, ni siquiera deberían navegar por ellas; el navegador, también es una puerta de acceso para los delincuentes cibernéticos, en muchas ocasiones.

Un buen antivirus proporcionado por la entidad.

Antes de usar cualquier equipo de cómputo, de escritorio o portátiles o dispositivo móvil que vayan a conectarse a Internet, lo primero que se debe hacer, es instalar un buen antivirus.

Si, esta medida es importante en los entornos domésticos, en el corporativo, se vuelve fundamental. Una solución de seguridad para entidades, protege los equipo de cómputo, de escritorio o portátiles y los datos de la entidad, en multitud de circunstancias, incluso, cuando los colaboradores cometen un error o alguna imprudencia.

Concienciar a los colaboradores, proveedores y clientes al respecto [11], [12], [13].

Procedimientos seguros de contratación y desvinculación

Sabiendo que gran parte de la fuga de información se realiza por parte de colaboradores o ex colaboradores, es importante controlar los accesos y permisos de los colaboradores, en especial cuando dejan la entidad.

Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.

Asegurar que los colaboradores, proveedores y terceros entiendan sus responsabilidades y sean adecuados para los roles asignados con el propósito de reducir el riesgo de robo, fraude o mal uso de los medios.

Los colaboradores y proveedores a los que se brinde acceso a información confidencial, deberían firmar un acuerdo de confidencialidad y no divulgación, antes de tener acceso a las instalaciones de procesamiento de información.

Se debe tener una correcta recepción de la documentación requerida para generar paz y salvo entre otras características, para poder generar la desvinculación del colaborador, y así, asegurar que no existan compromisos de trabajo pendientes entre el colaborador y el área de desempeño.

El colaborador está en la obligación de recolectar el paz y salvo de las áreas o dependencias, con las cuales estuvo directamente involucrado en el ejercicio de su labor, con el fin, de dar a conocer oportunamente a todos los colaboradores de la entidad la desvinculación de su rol y poder definir qué acciones se toman con las actividades pendientes de finalización.

Cuando sea apropiado, las responsabilidades contenidas dentro de los términos y condiciones del empleo, deberían continuar durante un período definido después de finalizado el contrato, como la no divulgación de los proyectos internos o relaciones con las demás entidades, esto para evitar, dificultades con las demás entidades en futuras uniones temporales.

VII. CONCLUSIONES

Todos los planes de capacitación y sensibilización, deben estar siempre en continuo seguimiento, así, como la tecnología cambia cada día, los delincuentes cibernéticos también lo hacen y encuentran siempre diferentes herramientas para aprovechar, las vulnerabilidades de los equipos de cómputo, servidores y en general, toda la tecnología que manejan en la entidad.

Es adecuado para la entidad, que el plan de capacitación, se ejecute cada trimestre y en cada sesión, mostrar a los colaboradores, las nuevas técnicas que utilizan los delincuentes cibernéticos, de una manera dinámica, enseñarles qué sitios pueden seguir, para que ellos mismos estén al tanto de las posibles estrategias que usan, para poderles robar información.

Mantener una buena comunicación con los colaboradores, es vital para poder ganarse su confianza y concientizarlos en que deben reportar cada incidente de seguridad que ellos observen; así, al final, no llegue a ser un incidente, esto demuestra el grado de compromiso con la entidad.

REFERENCIAS

[1] "Plan de comunicación y sensibilizacion", 17 Marzo 2016. [En línea]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_G14_Plan_comunicacion_sensibilizacion.pdf. [Último acceso: 2 Mayo 2018].

[2] ConstituciónColombia.com, Articulo 15 de la Constitución Política de Colombia Ley 1266 de 2008, 9 Mayo 2018. [En línea]. Available: http://www.constitucioncolombia.com/titulo-2/capitulo-1/articulo-15. [Último acceso: 10 Mayo 2018].

[3] "MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN", 19 Julio 2017. [En línea]. Available: http://es.presidencia.gov.co/dapre/DocumentosSIGEPRE/M-TI-01-Manual-Politicas-Seguridad-Informacion.pdf. [Último acceso: 5 Mayo 2018].

[4] C. Tiempo, "Cómo prevenir y evitar la fuga de información empresarial", *portafolio.co*, 25 Junio 2012. [En línea]. Available: http://www.portafolio.co/mis-finanzas/ahorro/prevenir-evitar-fuga-informacion-empresarial-100890. [Último acceso: 29 Abril 2018].

[5] C. Tiempo, "Siete consejos para proteger los sistemas informáticos de su compañía," *Portafolio.co*, 12 Junio 2017. [En línea]. Available: http://www.portafolio.co/innovacion/siete-recomendaciones-para-proteger-los-sistemas-informaticos-de-su-compania-506755. [Último acceso: 1 Mayo 2018].

[6] "Vulnerabilidades o técnicas que aprovechan el factor humano", *YouTube*, 29 Febrero 2016. [En línea]. Available: https://www.youtube.com/watch?v=kvbYbsGoofo. [Último acceso: 5 Mayo 2018].

[7] "BOE.es-Protección de Datos de Carácter Personal", *Boe.es*, 9 Mayo 2018. [En línea]. Available: https://www.boe.es/legislacion/codigos/codigo.php?id=55&modo=1&nota=0&tab=2. [Último acceso: 9 Mayo 2018].

[8] Latinoamerica, "Eset Security Report Latinoamerica 2012", *Es.slideshare.net*, 29 Mayo 2012. [En línea]. Available: https://es.slideshare.net/ESETLA/eset-securityreportlatam2012. [Último acceso: 5 Mayo 2018].

[9] *Welivesecurity.com*, 2017. [En línea]. Available: https://www.welivesecurity.com/wp-

content/uploads/2017/04/eset-security-report-2017.pdf. [Último acceso: 20 Mayo 2018].

[10] "INCIBE - Instituto Nacional de Ciberseguridad", *Adl.incibe.es*, 2015. [En línea]. Available: https://adl.incibe.es. [Último acceso: 20- Mayo 2018].

[11] *Incibe.es*, 2018. [En línea]. Available: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_desarrollar-cultura-en-seguridad.pdf. [Último acceso: 8 Mayo 2018].

[12] "ISO 27001: Pilares fundamentales de un SGSI", *Software ISO*, 2015. [En línea]. Available: https://www.isotools.org/2015/01/13/iso-27001-pilares-fundamentales-sgsi. [Último acceso: 9 Mayo 2018].

[13] "Buscó por el término Software De Gestión Para La Excelencia Empresarial Isotools - Software ISO", *Software ISO*, 2017. [En línea]. Available: https://www.isotools.org/?s=Software+De+Gestion+Para+La+Excelencia+Empresarial+Isotools&post_type=course&c=a2500aa51e8e. [Último acceso: 8 Mayo 2018].

Autor

Christian Fabian Rubiano Gomez.

Nacido en Bogotá, el día 2 de Septiembre de 1980, Técnico de sistemas egresado del Politécnico Central, Tecnólogo de sistemas e informática empresarial egresado de (CIDE) corporación internacional de educación superior e Ingeniero de Sistemas egresado de la Universidad San José Fundación de Educación Superior.