INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO

FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS

ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

IDENTIFICACIÓN DE MALAS PRÁCTICAS EN ENTORNOS LABORALES PARA EL PLANTEAMIENTO DE LA CREACIÓN DE UN GRUPO DE SEGUIMIENTO A FUNCIONARIOS.

PRESENTA:

DAVID FERNANDO PRIETO AYALA

ASESORES TEMÁTICO:

WILMAR JAIMES FERNÁNDEZ

DIEGO ALEJANDRO CORRALES CARO

Mayo 2018

Indice de contenido

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Resumen

En este documento y con la ayuda de la cartilla guía y los conocimientos adquiridos hasta lo visto de la especialización de seguridad de la información, se profundizará en la identificación de ciertas situaciones cotidianas vividas en un entorno laboral de una entidad pública (sector gobierno), la cual maneja grandes volúmenes de información, además en un amplio porcentaje ésta información es sensible y confidencial y se evidencian serios problemas de manejo en la seguridad de la información debido a las malas prácticas y hábitos.

Una vez identificados estos problemas de seguridad de la información se procede a reconocer los participantes, su rol y las causas del por qué dichos actores intervienen en las falencias encontradas, igualmente llegar a determinar la afectación que podría causar las situaciones identificadas. Se llevará a cabo un análisis de la información recaudada, aplicando indicadores y flujogramas que permitan entender y clarificar los escenarios propuestos, para proyectar la conformación de un grupo de personas que realicen seguimientos personalizados a las malas prácticas y generen un nicho de distribución del conocimiento en la corrección de los errores encontrados.

Abstract

In this document and with the help of the booklet and the knowledge acquired to date of the specialization of information security, they deepened in the identification of the situations in which they lived in a work environment of a public entity (government sector), which handles large volumes of information, in addition to containing a size that is sensitive and confidential and that evidences serious management problems in the security of information due to bad practices and habits.

Once these security information problems are identified, participants will be recognized, their role and the causes of what is said to be the actors intervening in the flaws found, as well as to determine the impact that the identified situations. Make an analysis of an analysis of the information collected, apply the proposed indicators, to project the conformation of a group of people who carry out

personalized follow-ups to the bad practices and generate a niche of knowledge distribution in the correction of the errors found.

.

Palabras clave

Usuarios Finales: Personas quienes interactúan con los sistemas de información, software, equipos de cómputo y en general con información de carácter relevante, confidencial y reservada.

CID: Sigla de los principales pilares de la información Confidencialidad, Integridad y Disponibilidad.

ISO 27001: Conjunto de reglas, normas, las cuales forman un estándar de calidad en temas de seguridad de la información.

Key words

Final users: People who interact with information systems, software, computer equipment and in general with relevant, confidential and reserved information.

CID: Acronym for the main pillars of information Confidentiality, Integrity and Availability.

ISO 27001: Set of rules, standards, which form a quality standard in information security issues.

Introducción

En los últimos tiempos y teniendo en cuenta el cambio acelerado en el área tecnológica se puede observar cómo las empresas privadas y públicas han enfocado esfuerzos a dar una mayor importancia a uno de los tesoros más grandes de cualquier negocio “La información”. Si bien es cierto antiguamente se daba una prioridad a otro tipo de activos, hoy en día se podría hablar de un modelo del centro hacia afuera, teniendo como centro la información, todos los negocios tienen relación a información, bien sea información contable, información de personal, información de proveedores, información de compradores entre otra. Si entramos analizar cualquier proceso de diferentes compañías, éstos tienen una atadura inherente a información y es allí donde nacen las auditorias y los estándares para un correcto uso de la información y lo que esta conlleva.

Para esta entrega, se identificaron ciertas situaciones problema, los actores que la comprenden y sus puntos de vista.

Análisis desde el modelo de planeación estratégica situacional.

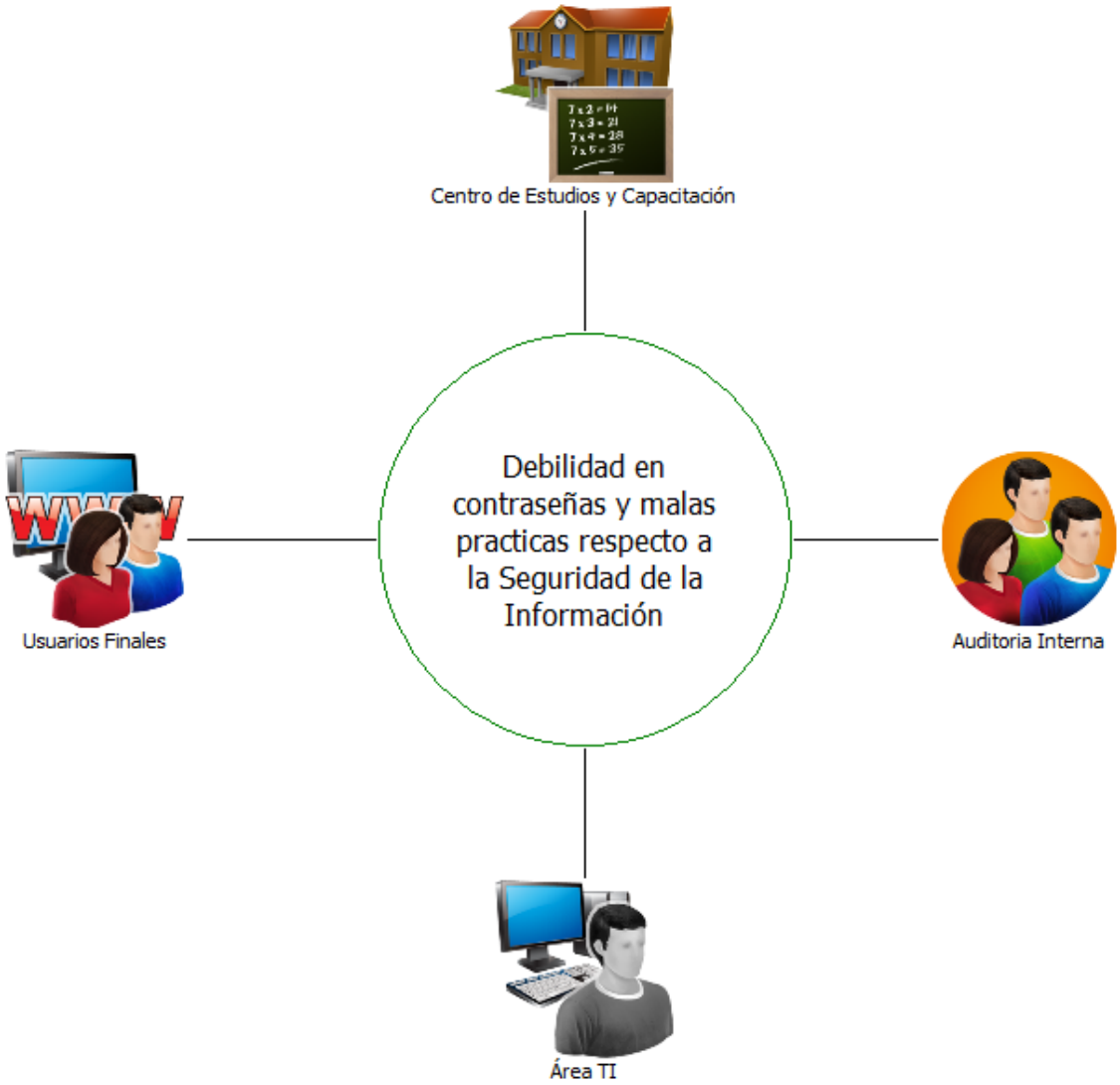
Descripción de la situación de interés.

Falta de buenas prácticas en el manejo de la información, entiéndase manejo de información como la interacción del trabajador con la misma, este proceso conlleva acceso, tratamiento, integración análisis y difusión etapas que componen el ciclo de la información, procesos que están vinculados directamente con las propiedades CID (Confidencialidad, Integridad y Disponibilidad), las cuales se deben preservar a su máxima expresión y ponderando la propiedad más deseada que en este caso es la Confidencialidad.

Área de interés.

Si bien es cierto el problema citado en este documento hace parte de innumerables grupos al interior de la entidad pública en la que trabajo, el área de estudio específica es una Sección encargada del análisis de información y la difusión de reportes cuantitativos y cualitativos.

Actores Relevantes en la situación problema.



Gráfica 1: ***Situación problema VS Actores Involucrados.***

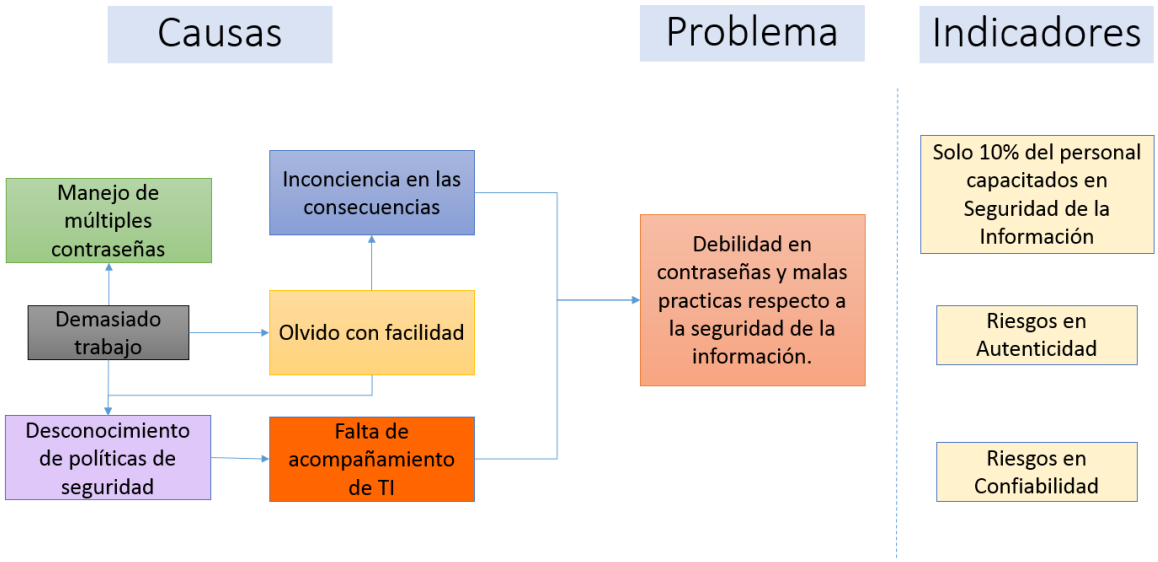
Causas de la situación problema.

A continuación se enlistan los puntos de vista obtenidos en una pequeña e informal entrevista con los diferentes actores identificados en la situación problema.

Actor	Razones
Usuarios Finales	Manejo de múltiples contraseñas.
	Demasiado trabajo.
	Olvido con facilidad en periodos de inactividad.
	Falta de capacitación en el uso de la información.
Auditoria Interna	Desconocimiento de las políticas de seguridad de la entidad.
	Desconocimiento de las guías.
	Falta de capacitación en el uso de la información.
Área TI	Desconocimiento de las políticas de seguridad de la entidad.
	Inconciencia en las consecuencias producto de los malos hábitos.
Centro de Estudios y Capacitación	Desconocimiento de las políticas de seguridad de la entidad.
	Falta de acompañamiento por el área encargada
	Falta de solicitud de capacitación

Tabla 1: ***Actores VS Causas***

Flujograma.



Gráfica 2: Flujograma.

Indicadores.

Nombre del indicador	**Incidentes de seguridad**
Propósito del indicador	Conocer los incidentes relacionados con olvidos de contraseña, perdida de información entre otros.
Destinatario	Áreas operativas, alta gerencia, TI, auditores internos
Formula	Cantidad de incidentes de seguridad relacionados / cantidad de incidentes de seguridad gestionados.
Escala	Porcentaje
Nivel para el cumplimiento	100%
Frecuencia de medición	Trimestral
Fuente de datos	Sistema de reportes de incidentes.

Tabla 2: Indicador 1.

Nombre del indicador	**Capacitación, entrenamiento y toma de conciencia**
Propósito del indicador	Medir el nivel de sensibilidad de los empleados frente al SGSI
Destinatario	Gerencia de Talento humano
Formula	Cantidad de capacitaciones programadas / capacitaciones ejecutadas
Escala	Porcentaje

Nivel para el cumplimiento	70%
Frecuencia de medición	Anual
Fuente de datos	Programa de capacitaciones y entrenamiento.

Tabla 3: Indicador 2

Nombre del indicador	**Control de acceso**
Propósito del indicador	Conocer el nivel de seguridad del control de acceso a las redes, sistemas de información e información, para medir la confiabilidad e integridad de la información.
Destinatario	Usuarios finales.
Formula	Número de controles propuestos / Número de controles implementados
Escala	Porcentaje
Nivel para el cumplimiento	85%
Frecuencia de medición	Anual
Fuente de datos	Auditorías internas.

Tabla 4: Indicador 3

Nombre del indicador	**Análisis de vulnerabilidades**
Propósito del indicador	Conocer el nivel de seguridad en los sistemas de información.
Destinatario	Área de seguridad.
Formula	Cantidad de hallazgos encontrados en los análisis / Cantidad de vulnerabilidades mitigadas
Escala	Porcentaje
Nivel para el cumplimiento	70%
Frecuencia de medición	Semestral
Fuente de datos	Reportes de análisis de vulnerabilidades.

Tabla 5: Indicador 4

Antecedentes

“Mi consejo es uno: Aférrense con todas sus fuerzas y convicción a la educación. No desfallezcan; estudien mucho. El futuro no lo sabemos pero, con certeza, si nos educamos será mucho mejor”. Sergio Fajardo

En cuanto a las posturas teóricas que existen al problema planteado no son muchas, teniendo en cuenta que lo que se pretende con este documento es realizar una mezcla entre el comportamiento del ser humano cuando interactúa con un bien tan valorado en las empresas como la información y su falta de compromiso y motivación al no apropiarse de este recurso como propio. Por ende se deben tener una serie de controles; administrativos, de comportamiento y educativos. Por eso en la búsqueda de antecedentes hago mención a la tesis de grado de maestro en ciencias en ingeniería de sistemas de la Lic Diana Marisol Prado, en donde el resumen de dicho trabajo menciona: “Por lo tanto, éste trabajo de tesis, se realizó con la finalidad de proponer una metodología dirigida para aquellas empresas que quieren mejorar o evitar una situación de riesgo, por tener un escaso conocimiento en seguridad de la información”

En su trabajo de tesis la Licenciada Prado hace alusión a una metodología de seis fases desde la 0 “definición de los requerimientos de inicio” hasta la fase 5 “implantación y monitoreo de las actividades de control y capacitación del personal”, una vez leída esta metodología puedo asemejarla a la que se pretende utilizar en este trabajo debido a que cuenta con etapas como la identificación de

errores que serían los requerimientos de inicio finalizando en una serie de actividades de control en donde se incluye la formación y educación del personal del grupo que realiza las veces de PoC. Una de las fases que me parece muy interesante de la tesis de referenciada es la fase 1 “conocimiento del medio ambiente de la empresa en este trabajo”, la aterrizo al ambiente del grupo el cual teniendo en cuenta factores como la visión, misión políticas de calidad manuales de ética y buen gobierno deben cumplir una serie de tratamiento especial con la información que los rodea y deben guardar los principios de confidencialidad de la información y la reserva.

Por última referencia a este trabajo de posgrado es fundamental como su metodología es general y se puede aplicar a gran cantidad de empresas, de la misma manera que se pretende con este trabajo que si bien es cierto se sesga a un pequeño nicho de población de una empresa pública como se ha mencionado es factible la realización para varias empresas que trabajen con información confidencial de carácter reservado o sensible.

Como se ha dicho este trabajo pese a ser un proyecto de una facultad de ingeniería tiene mucho que ver con la esencia del mundo y su desarrollo; el ser humano y su comportamiento, debido a que por más controles tecnológicos que existan siempre el eslabón de la cadena se rompe por la unión más frágil en este caso las personas bien sea por su falta de educación, su falta de compromiso o peor aún a su falta de valores, por ende y a razón de una lectura que estoy realizando en el momento del presente escrito “El poder de la decencia” del actual

candidato a la presidencia de la república de Colombia Sergio Fajardo, matemático de profesión me parece interesante traer y registrar algunos pasos de su metodología de gobierno en la gobernación de Antioquia y alcaldía de Medellín. Y es que sin ánimos de inmiscuirme en la política pienso que así como el señor Fajardo pudo conectar y trasformar muchos ciudadanos de una de los lugares más peligrosos del mundo en su momento (Medellín) se puede utilizar la metodología de la educación en empresas para desarrollar y alcanzar la aprehensión de valores y hábitos de apropiación empresarial que se requiere tanto hoy en día en el sector público.

Como se cita en éste libro apostar a la educación es un proceso largo que conlleva de tiempo y por eso es que ningún gobierno lo toma en cuenta, pienso que si se tiene una mezcla de reglas y educación se puede transformar a empleados que con sus comportamientos pueden irrumpir la seguridad de la información en grupos empresas y sectores. Hago esta mención en la sección de antecedentes de este documento porque a través de la educación desde el interior y exterior del país se vio reflejado como con dar un sentido de apropiación y educación la ciudad de Medellín paso a ser una de las más educadas e innovadoras del continente y del mundo por eso pienso que con una fusión de las metodologías encontradas y analizadas se puede tener en cuenta para este trabajo.

Análisis de prospectiva y viabilidad, estrategia metodológica.

Formulación de la situación deseada.

Para este punto es importante traer a referencia el pensamiento de Godet y Ackoff en cuanto a los criterios de; inactivismo, reactivismo y el pre y el pro activismo.

De los anteriores conceptos se originan los escenarios de no hacer nada ante el problema o situación problema y que todo continué igual (inactivismo) y este pensamiento es explicable desde el sentido, que si bien existe una situación problemática ésta se mantiene en equilibrio y cualquier acción que se realice podría desencadenar y tener consecuencias negativas que perturbe el estado de equilibrio por eso este pensamiento es el de convivir con el problema y tenerlo aislado para que no cambie de estado (que todo continué igual).

Si se proyecta un escenario prospectivo de un tiempo de tres años a la situación problema descrita en este documento sin duda podríamos decir que si no se toman las acciones correctivas se podría dar dos escenarios posibles;

a) escenario de inactivismo:

Como ya se explicó anteriormente convivir con el problema sin que ocurra nada lo cual es una situación muy riesgosa pues se deja al azar el comportamiento de ocurrencia y efectivamente en este momento existe un riesgo el cual se encuentra en un estado de suspensión o inactivo y en el futuro como puede que desencadene una situación catastrófica puede que todo siga igual y no ocurra nada.

b) una situación de retroceso o consecuencias negativas:

Principalmente afecta a la entidad debido a las malas prácticas de los empleados, en cuanto a los procesos que tienen que ver con el manejo del activo más importante de la entidad (información) y es que estas son algunas consecuencias si de ser pesimistas se trata:

- Vulneración de los principios de la información, principalmente de la confidencialidad (acceso a información sensible, fuga de información etc).
- Suplantación de identidad.
- Accesos no autorizados.
- Falta de auditorías internas debido a que este grupo tiene otras prioridades y no toma en cuenta el comportamiento de los funcionarios en cuanto al manejo de la información.
- Nulidad de recursos orientados a la capacitación de los funcionarios en el manejo de la información.
- Propagación por parte de las personas con malas prácticas a funcionarios nuevos esto aunado a la falta de capacitación.

Y es que vale la pena referenciar que no solamente se pueden ocasionar afectaciones a la empresa, los empleados se pueden ver afectados en su integridad y estas serían algunos de las consecuencias:

- Pérdida del empleo.
- Investigaciones disciplinarias y/o penales.
- Sanciones económicas.

- Sanciones administrativas.

c) Escenario optimista:

Proyectando al mismo periodo un escenario cercano de tres años teniendo en cuenta una prospectiva pre activa en donde lo que se pretende es realizar cambios siempre con el fin de mejora continua. Afrontar estos escenarios de cambios es viablemente más cómodos si están acordes a la posición del líder de la empresa, es decir si están incluidos dentro del direccionamiento estratégico de la entidad.

Lo anterior se ve reflejado directamente en la adquisición de presupuesto para poder contemplar la capacitación y concientización del personal en campañas pedagógicas permanentes, reconocimientos, premios, estímulos. Lo enunciado debe ser permanente para que la gente convierta las buenas prácticas aprendidas en capacitaciones en hábitos y lo vuelvan parte necesaria de sus labores diarias, con esta incentiva se puede lograr:

- Ayudar al cumplimiento de confiabilidad, integridad y disponibilidad de la información.
- Generar controles tecnológicos para verificar el cumplimiento de las buenas prácticas del manejo de la información.
- Cumplir con estándares normativos como el ISO 27001.
- Lograr certificaciones ISO 27001.
- Profesionalización de los empleados en aspectos tecnológicos (empleados digitales).

Variables

Según la situación problemática propuesta se presentan algunas variables las cuales pueden influir en el cumplimiento del escenario pre activista del análisis prospectivo.

- Adquisición de herramientas tecnológicas que monitoreen el nivel de fortaleza de las contraseñas.
- Adquisición de herramientas generadoras de contraseñas seguras aleatorias.
- Cambio de pensamiento del nivel estratégico, el cual tenga como objetivo fortalecer las políticas en seguridad de la información.
- Aumento del presupuesto de educación dirigido a temas de educación del manejo de la seguridad de la información.
- Incentivar el buen uso de la información y las buenas prácticas.

Matriz de valoración estratégica.

Causa	Acción	Actor (es)	Valoración estratégica	Valoración de impacto	Valoración de gobernabilidad
Altos valores en costos.	Adquisición de herramientas tecnológicas que monitoreen el	Dirección estratégica, subdirección TI y usuarios	Alto	Alto	Medio

Causa	Acción	Actor (es)	Valoración estratégica	Valoración de impacto	Valoración de gobernabilidad
	nivel de fortaleza de las contraseñas.				
Evaluación de funcionalidad y uso de software libre	Adquisición de herramientas generadoras de contraseñas seguras aleatorias.	Dirección estratégica, subdirección TI y usuarios	Alto	Medio	Medio
Ejecución de proyectos internos los cuales renueven las políticas de seguridad de la información las cuales son antiguas	Cambio de pensamiento del nivel estratégico, el cual tenga como objetivo fortalecer las políticas en seguridad de	Subdirección TI, grupos de control interno, Direccionamiento estratégico y usuarios	Medio	Medio	Medio

Causa	Acción	Actor (es)	Valoración estratégica	Valoración de impacto	Valoración de gobernabilidad
	la información.				
Adquisición de presupuesto para fortalecer procesos de capacitación y concientización	Aumento del presupuesto de educación dirigido a temas de educación del manejo de la seguridad de la información.	Ministerio de hacienda (externo), Dirección estratégica, Escuela de altos estudios y usuarios	Medio	Alto	Medio
Mantener incentivado al personal mediante premios y reconocimientos por su buen desempeño	Incentivar el buen uso de la información y las buenas prácticas.	Oficina de bienestar, usuarios.	Medio	Bajo	Bajo

Planteamiento del problema

Teniendo en cuenta la importancia de salvaguardar los pilares de integridad y confidencialidad de la información, de la entidad del estado en la que me encuentro la cual maneja información sensible, así como otras empresas del sector público y privado se ven enfrentados a una incansable batalla entre los funcionarios (quienes son los principales originadores y consumidores de información) y sus malas prácticas ante el manejo de la información. De acuerdo a un estudio parcial informal por medio de cuestionarios se ha logrado establecer una debilidad en la selección de contraseñas y en general malas prácticas con el manejo de la información como; dejar sesiones abiertas, dejar al descubierto dispositivos de almacenamiento, los cuales pueden llegar a contener información sensible, compartir contraseñas y usuarios entre amigos entre otros comportamientos inadecuados.

Lo anterior tiene una gran cantidad de causas como por ejemplo el manejo de innumerables contraseñas debido a la gran cantidad de sistemas de información que no se encuentran integrados, el gran volumen de carga laboral, la falta de acompañamiento del departamento de tecnología e información el desconocimiento de las políticas de seguridad de la entidad, pero a mi modo personal de plantear y afrontar el problema la causa principal es la inconciencia y disciplina de las personas y es que como un indicador que apoya este concepto se tiene que solo el 10% del personal conoce o está capacitada en temas de seguridad de la información.

Pero de quién es la responsabilidad de afrontar estos problemas de seguridad de la información ?, indudablemente la respuesta pasa por diferentes niveles, la parte estratégica y de direccionamiento de la entidad, los encargados de control y auditoria internas, el personal encargado de tecnología e información el usuario final o funcionarios y la escuela de capacitación y estudios de la entidad, Cada uno tiene un nivel de responsabilidad y de un porcentaje de aporte para que el escenario problema mejore. Por lo anterior es demandante, plantear la posibilidad de conformar un grupo de personas encargados de realizar seguimientos continuos a las malas prácticas de los empleados, capacitación y difusión de campañas de buenas prácticas, registro de incidentes de seguridad de la información y en general un extensivo acompañamiento inicial el cual se minimizaría de acuerdo a la mejora de los usuarios finales.

Es claro que un proyecto como estos en una entidad tan grande y extensa es algo que se debe diseñar y estudiar desde el direccionamiento estratégico, pasando por diferentes etapas, por ende, lo que se proyecta en este documento es el planteamiento de la creación de un grupo en un área determinada que en el escenario de la creación se lleve a cabo un seguimiento y estudios de factibilidad de extenderlo de manera local y nacional.

Justificación

El enfrentar el escenario problema es una necesidad para la entidad debido a que anualmente se presentan incidentes en la mesa de ayuda que se relacionan con temas de contraseñas olvidadas, alertas en las páginas a las que acceden

funcionarios y poco a poco se han conocido temas de fraude y venta de información que si bien es cierto son aislados teniendo en cuenta el número de empleados estos no deberían ocurrir por ningún motivo.

Es necesario de igual forma porque de acuerdo a las evaluaciones realizadas algunos sistemas de información se tuvo como resultado que las medidas de seguridad ofrecidas por ellos no ayuda a los que los usuarios finales adquieran disciplina como un pequeño ejemplo de ello se puede hablar que existen sistemas que no exigen el cambio de la contraseña por defecto y el usuario es un estándar de fácil conocimiento, esto sumado a la falta de disciplina de las personas da como resultado un fácil acceso desde muchas cuentas.

Por último dentro de los ítems que justifican el enfrentar esta problemática es la baja capacitación, competencias y entrenamiento de los funcionarios, quienes se ven arrollados por el continuo avance de las tecnologías.

Objetivo general

Identificar situaciones en entornos de trabajo reales que representen un riesgo o vulnerabilidad las cuales justifiquen el planteamiento de la creación de un grupo de personas que realicen seguimiento, auditoria y en general todo trabajo para mitigar y cerrar estas ventanas a los delincuentes que quieran sustraer, alterar o difundir la información sensible.

Lo anterior teniendo en cuenta los conocimientos adquiridos dentro de la formación profesional especialización en Seguridad de la Información, además potencializar la experiencia compartida por los docentes para solventar el problema planteado.

Objetivos específicos

- Realizar un estudio implementando una metodología de recolección de información para dar un dimensionamiento de la ocurrencia del problema planteado y buscar la construcción de un equipo de seguimiento y capacitadores en la formación de seguridad de la información.

- Evaluar la información recolectada identificando los actores intervinientes con el fin de interactuar con los mismos para la propuesta de soluciones.

- Ejecutar los lineamientos almacenados en el proyecto de grado el cual utiliza una metodología práctica y exitosa.

- Generar resultados documentales de la solución de la problemática planteada.

Alcance

El dimensionamiento de un proyecto como este se tiene que afrontar en etapas, dado a la gran cantidad de funcionarios aproximadamente 30.000 a nivel nacional. El proyecto que aquí se aborda es una solución escalable la cual inicialmente tendrá en cuenta un grupo compuesto de 30 servidores, los cuales harán las veces de PoC y midiendo el éxito y los resultados se proyectará para

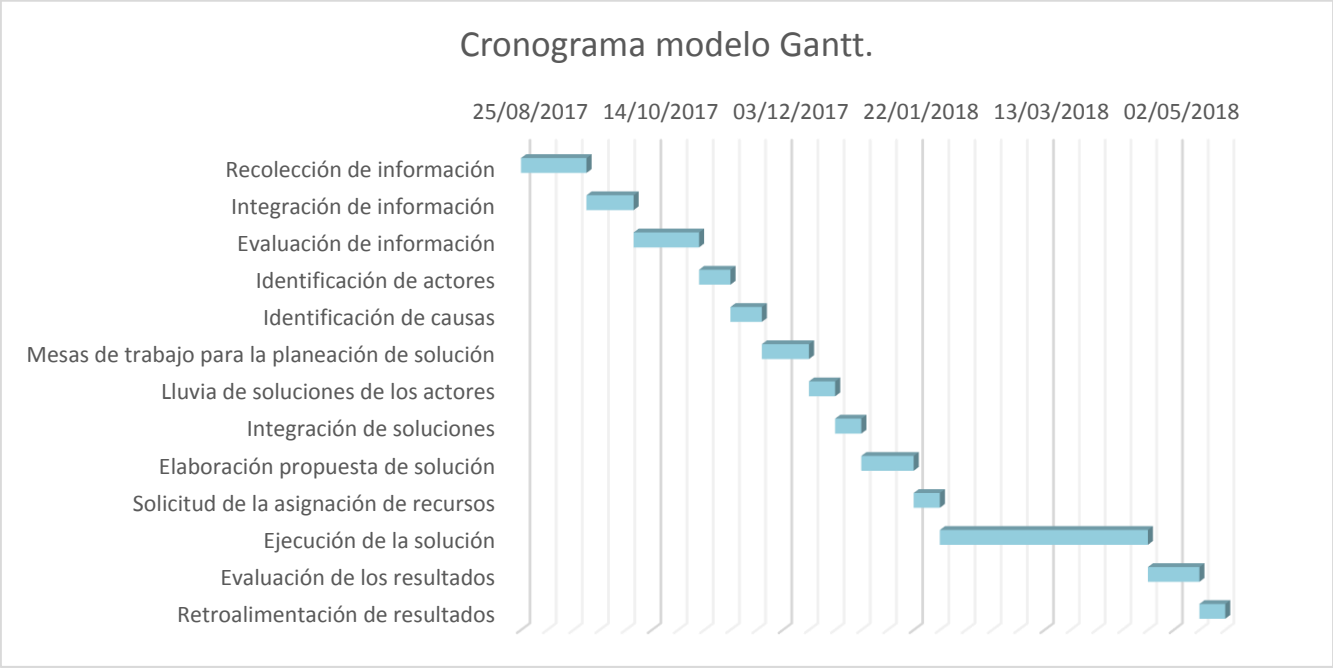
continuar su ejecución en otros grupos de la entidad hasta alcanzar porcentajes importantes de cubrimiento, cabe hacer referencia que no se cubrirá el cien por ciento de los empleados sino únicamente las áreas que manejen información extremadamente delicada por lo que se debe realizar una categorización de los grupos de acuerdo a sensibilidad de la información y de esta manera ir escalando.

Plan de trabajo

Teniendo en cuenta las observaciones realizadas por el tutor Diego Alejandro Corrales en el último encuentro sincrónico se proyecta un escenario de algo más de 270 días desde el 25 de agosto de 2017, finalizando el 22 de mayo del año siguiente.

Actividad	Fecha inicial	Duración en días	Fecha Final
Recolección de información	25/08/2017	25	19/09/2017
Integración de información	19/09/2017	18	07/10/2017
Evaluación de información	07/10/2017	25	01/11/2017
Identificación de actores	01/11/2017	12	13/11/2017
Identificación de causas	13/11/2017	12	25/11/2017
Mesas de trabajo para la planeación de solución	25/11/2017	18	13/12/2017
Lluvia de soluciones de los actores	13/12/2017	10	23/12/2017
Integración de soluciones	23/12/2017	10	02/01/2018
Elaboración propuesta de solución	02/01/2018	20	22/01/2018
Solicitud de la asignación de recursos	22/01/2018	10	01/02/2018

Tabla 6 Cronograma de actividades



Gráfica 3 Modelo de Gantt

Entregables

Para el presente proyecto se pretende realizar la entrega de los siguientes documentos:

1. Matriz de recolección y levantamiento de información.
2. Evidencias de las malas prácticas de los funcionarios.
3. Propuesta de soluciones.

Informe y presentación de retroalimentación.

Desarrollo e implementación.

De acuerdo a los entregables se ha diseñado una matriz para la recolección de información de incidentes de seguridad de la información en cuanto a las malas prácticas de los funcionarios, en la conformación de los campos para el registro de información se ha tenido en cuenta tres factores que se consideran de importancia, información de la persona que comete la irregularidad, información general de la irregularidad e información de la persona que levanta la información. El formato se ha encasillado en el proceso tecnológico de la entidad.

Una vez se ha diseñado el documento de recolección de información se ha procedido a realizar el registro de algunos incidentes de seguridad hallados, es preciso y que sea en este espacio para mencionar que las actividades que se han realizado son estrictamente académicas y con el fin de evidenciar las vulnerabilidades que se presentan día a día en el entorno laboral.

LOGO		PROCESO TECNOLÓGICO				**Código:** FGN-xxxxxx
		FORMATO BITÁCORA HALLAZGOS DE SEGURIDAD DE LA INFORMACIÓN "MALAS PRÁCTICAS"				**Versión:** 01 **Página:** 1 de]
RESUMEN HALLAZGOS ENCONTRADOS						
HORAS	SERVIDOR A QUIEN SE HACE EL HALLAZGO	DOCUMENTO SERVIDOR A QUIEN SE HACE EL HALLAZGO	RESULTADO	EVIDENCIA SOPORTE	DURACIÓN ACTIVIDAD	SERVIDOR QUIEN REALIZA HALLAZGO
INSTRUCCIONES PARA EL DILIGENCIAMIENTO DEL FORMATO						
ACTIVIDAD. Registro de la hora en que se hallo el incidente						
ACTIVIDAD. Descripción de la actividad o evento o novedad presentada.						
RESULTADO. Descripción de la medida tomada.						
DOCUMENTO SOPORTE. Documento que evidencia la actividad presentada.						
DURACIÓN ACTIVIDAD. Rango de tiempo en que se presentó la actividad o evento o novedad en formato desde (DD/MM/AAAA) hasta (DD/MM/AAAA).						

Gráfica 4 Matriz para el registro de malas prácticas de seguridad de la información

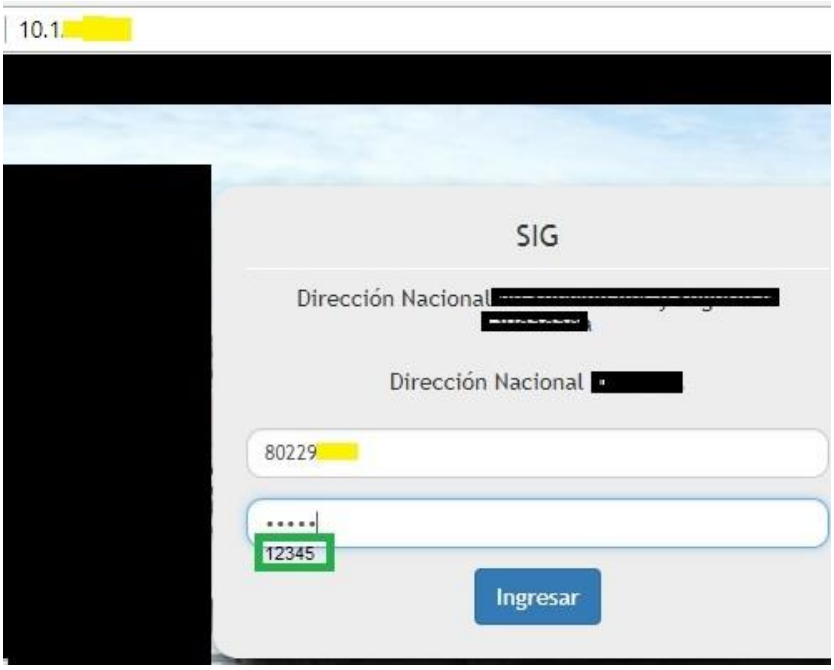
Mala práctica de seguridad de la información encontrada No 1.

Es conocido que tanto en el entorno público como privado se maneja uno o varios sistemas de información, los cuales sirven de consulta, registro o ambas de acuerdo a los perfiles asignados, en el hallazgo No 1 que se encontró fue colocar a prueba uno de los sistemas de información de carácter misional en donde los usuarios para ingresar al aplicativo deben digitar sus credenciales (cédula que sirve como usuario y una contraseña la cual por defecto son los caracteres del 1-5), el ejercicio de recolectar malas prácticas consistía en tomar pronunciamientos oficiales de la entidad de carácter público en donde se exponían los números de cédula de los funcionarios del grupo en donde se está llevando a cabo la PoC y se suministraba la clave por defecto 1-5. Los funcionarios que aún tuvieran la clave por defecto se convertirían en registros de malas prácticas.

En la gráfica 4 se muestra el listado de Excel público donde se evidencias los números de identificación de los funcionarios, por confidencialidad de la información se edita la imagen para no exponer la confidencialidad, seguido a esto se ingresa al sistema de información y se realiza la actividad con veinte servidores del grupo a evaluar, en la gráfica 5 y 6 se visualiza los resultados del ejercicio propuesto.

	CEDULA	NOMBRES	PRIMER APELLIDO	SEGUNDO APELLIDO	REGIONAL	SECCIONAL	PERIODOS PENDIENTES	PERÍODOS DISFRUTADOS DEL 25 ENE - 9 MAR/2018	
2									
3	79748	OSCAR		S	NIVEL		1	0	DELE
4	79763	ALVAR	Y	M	NIVEL		1	0	DELE
5	37754	MARIC		B	NIVEL		1	0	DELE
6	28698	EDILM		G	NIVEL		1	0	DELE
7	80229	MIGUE		C	NIVEL		1	0	DELE
8	52762	YUDYS		A	NIVEL		1	0	DELE
9	52715	YEIMI			NIVEL		1	0	DELE
10	51690	ELIZAB		M	NIVEL		1	0	DELE
11	7543	GONZA		C	NIVEL		1	0	DELE
12	79956	RICARD		M	NIVEL		1	0	DELE
13	39777	MARIA		H	NIVEL		1	0	DELE
14	37320	EUDELI		C	NIVEL		1	0	DELE
15	1014188	MARC		C	NIVEL		1	0	DELE
16	52470	CARME		M	NIVEL		1	0	DELE
17	66954	LUZ NE		M	NIVEL		1	0	DELE
18	93419	JUAN		V	NIVEL		1	0	DELE
19	1110509	ANGIE		L	NIVEL		1	0	DELE
20	52379	SANDR		M	NIVEL		1	0	DELE
21	39712	MARTH		U	NIVEL		1	0	DELE
22	51812	SANDR		S	NIVEL		1	0	DELE
23	1030658	MONIC		C	NIVEL		1	0	DELE
24	51919	CLAUD		D	NIVEL		1	0	DELE
25	39557	MARIA		S	NIVEL		1	0	DELE
26	79734	GUIDO			NIVEL		1	0	DELE

Gráfica 5 Pantallazo parcial de matriz de información de servidores



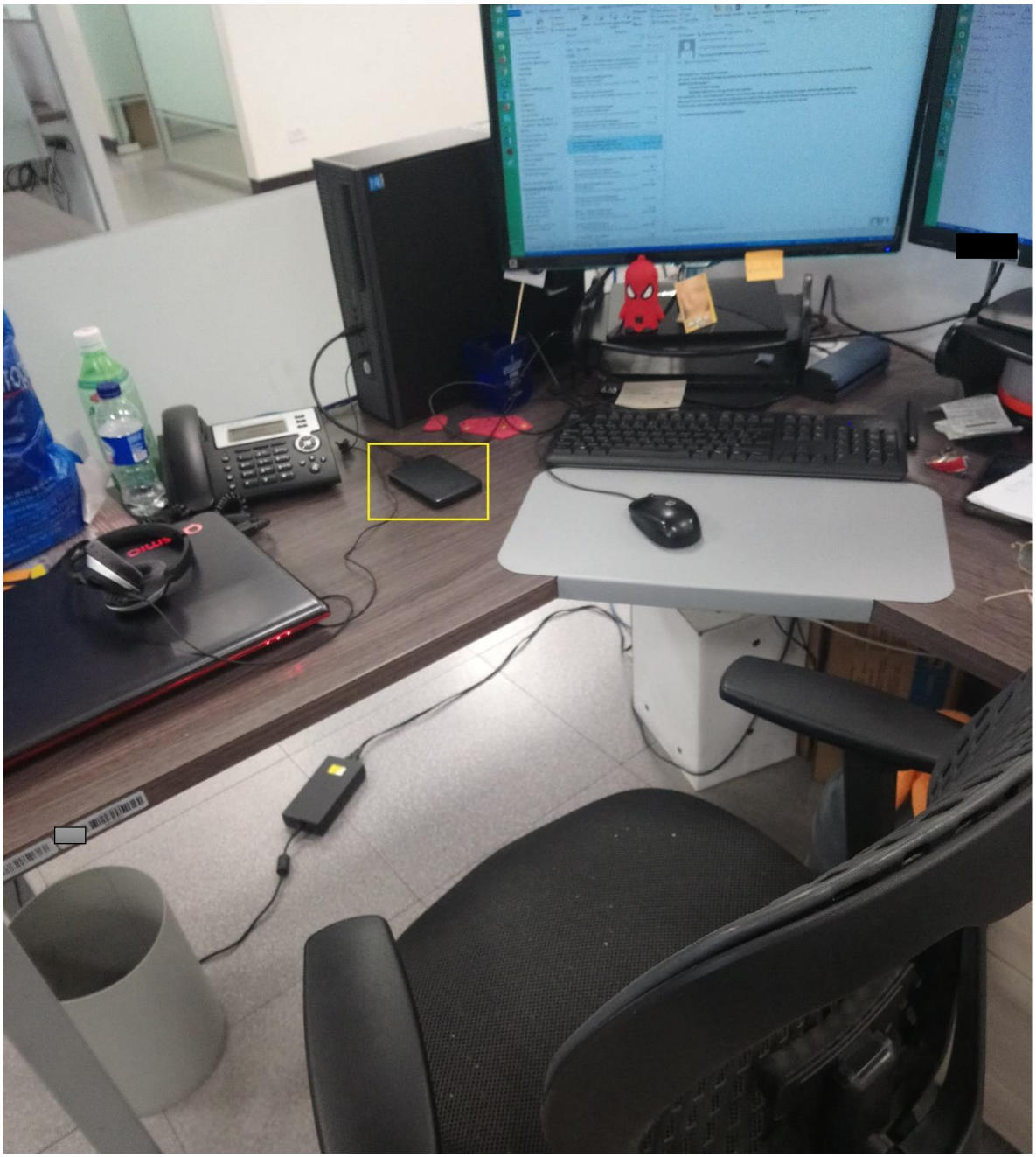
Gráfica 6 Pantallazo ingreso sistema de información.

Gráfica 7 Pantallazo de ingreso al sistema de información

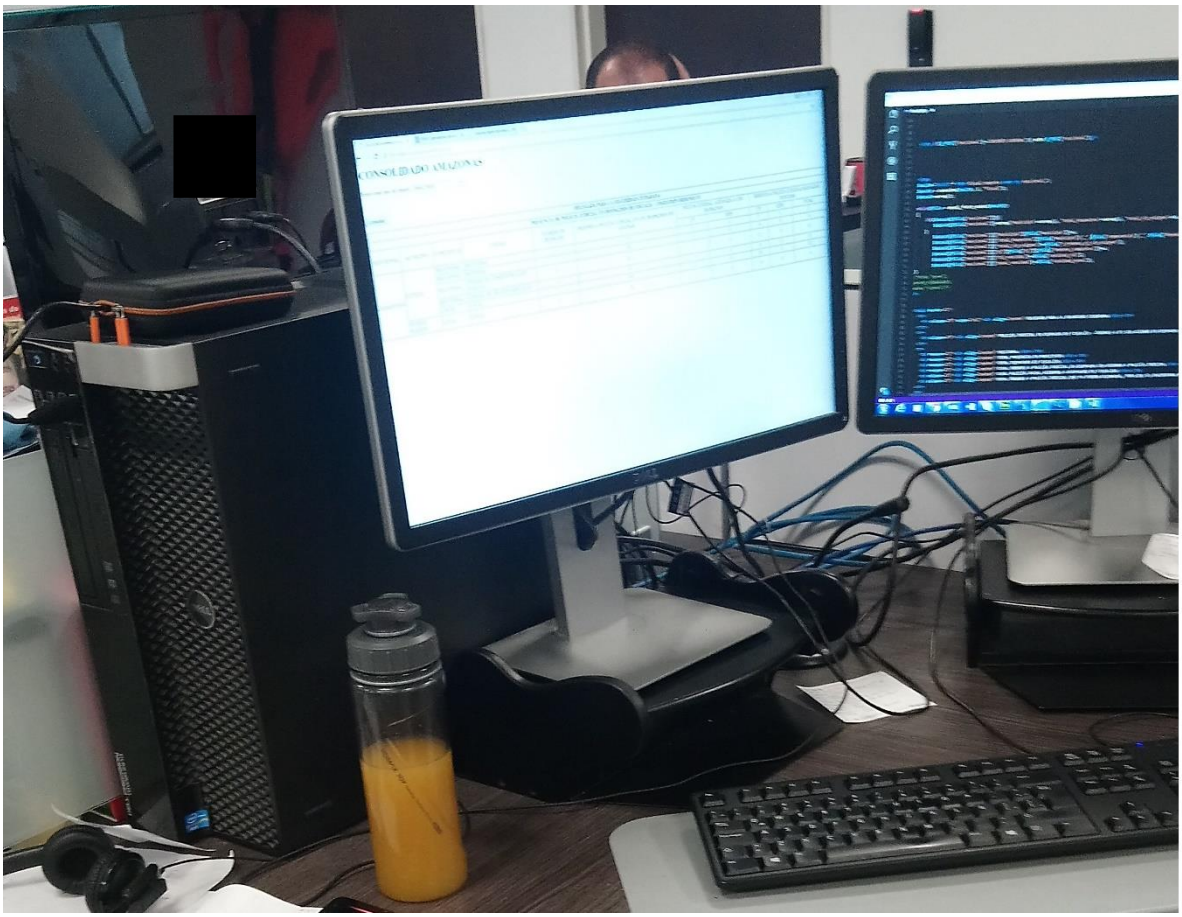
Mala práctica de seguridad de la información encontrada No 2 y 3.

Otras faltas graves que se han encontrado los cuales son muy comunes en grupos de trabajo es el dejar la sección del computador abierta exponiendo la información a las personas sin ningún tipo de restricción, este comportamiento es peligroso y ofrece vulnerabilidades debido a que bien sea en periodos prolongados o cortos se denota esta falla reiterativa por varios funcionarios exponiendo pilares críticos de la información como la Integridad y confidencialidad en ocasiones incluso hasta la Disponibilidad de la información, debido a que se dejan sesiones abiertas donde se encuentran desarrollos de software, correos institucionales y en general información sensible.

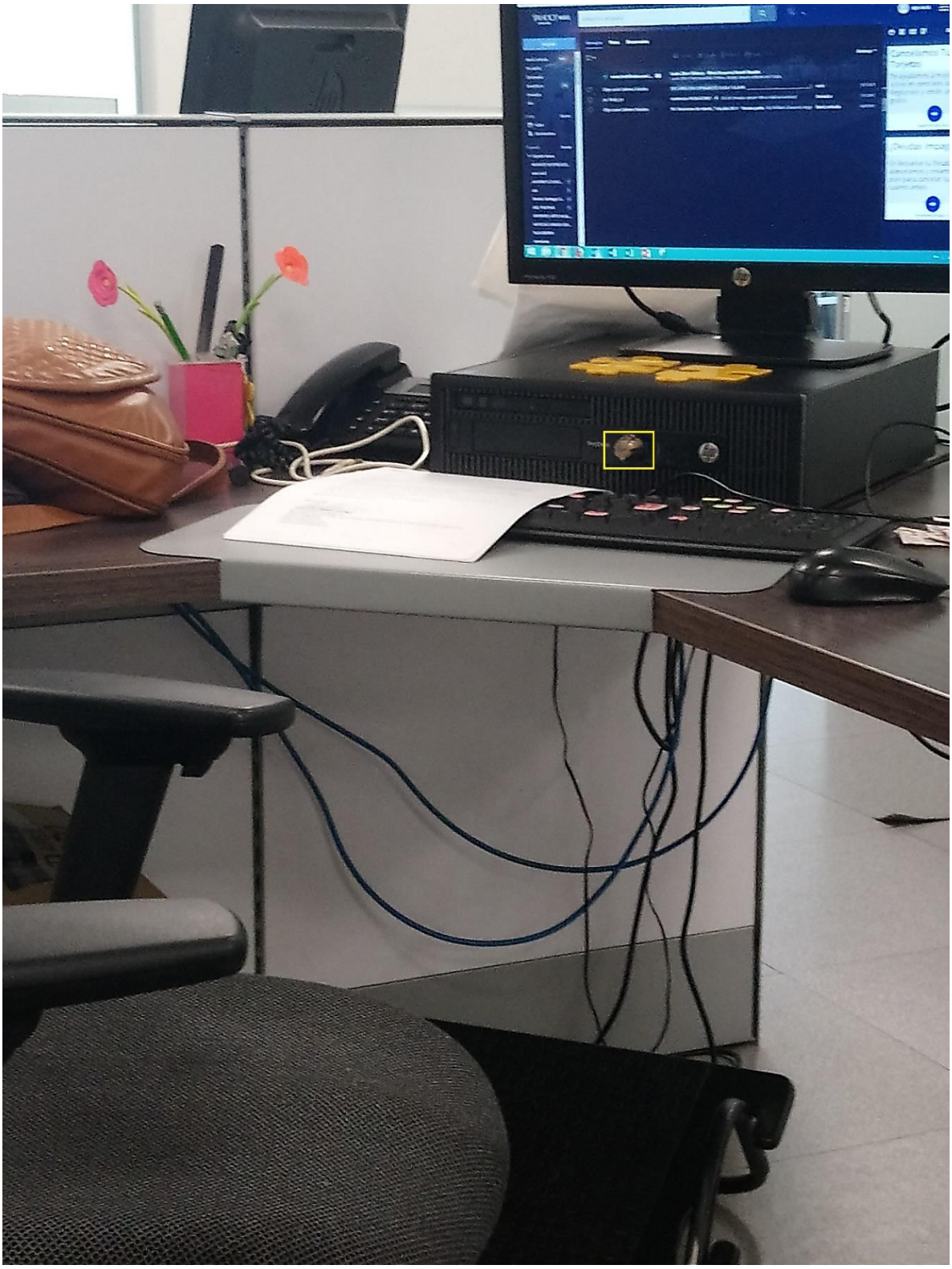
Otra de las malas prácticas encontradas, es el descuido y abandono de dispositivos de almacenamiento de información. En las siguientes gráficas se mostrara los hallazgos generales 2 y 3 mencionados anteriormente.



Gráfica 8 Sesión de usuario abierta y dispositivo de almacenamiento abandonado



Gráfica 9 Sesión de desarrollador abierta.



Gráfica 10 Sesión de usuario y de correo abierta y dispositivo de almacenamiento abandonado.

Mala práctica de seguridad de la información encontrada No 4.

Otra mala práctica de seguridad encontrada es la configuración de algunos dispositivos de ayuda en las labores ofimáticas como impresoras, plotters entre otras, a manera demostración de uno de los hallazgos se muestra en la siguiente gráfica la no protección de la configuración de seguridad de una impresora en donde cualquier usuario puede no solo consultar la ip a la cual se encuentra registrada en red, además puede cambiar dicha dirección ip causando un caos administrativo, logístico y el desperdicio de recursos como papelería, tinta y demás.

Gráfica 11 Evidencia de ip de impresora y vulnerabilidad.

Resultados.

Algunos de los resultados se evidencian desde la misma fase de desarrollo, pero a manera de resultados y luego de 25 días de recolección de información de malas prácticas en un grupo de 32 personas se logró establecer lo siguiente.

En cuanto a la Hallazgo denominado No 1 en la fase de desarrollo se estableció que un 40,6 % de personas aún tienen la clave por defecto, lo que equivale a un total de 13 personas.

En los hallazgos No 2 y 3 se logró establecer que de las 32 personas un porcentaje del 65,6 % ha dejado en algún momento la sesión de usuario abierta o ha descuidado los dispositivos de almacenamiento por lo menos cuatro veces en el periodo de recolección de información (15 días), lo que equivale a 21 personas.

Lo que se refiere al hallazgo No 4 se estableció que de un total de 10 impresoras utilizadas por el grupo dos tienen las fallas de configuración descritas, lo que equivale a un 20 %.

Existen otras fallas en cuanto a buenas prácticas de seguridad de la información como; (el uso compartido de usuarios y contraseñas, contraseñas repetitivas en distintos sistemas, contraseñas vulnerables por ingeniería social debido a la proximidad con datos evidentes) que son difíciles de documentar pero

que existen y se pueden seguir trabajando para documentar y tenerlas dentro del planteamiento del problema.

Refencias.

Bijker, W. (2001). The social construction of Bakelite: toward a theory of invention. In W. Bijker, T. P. Hughes, & T. Pinch (Eds.), The social construction of technology systems: New directions in the sociology and history of technology. (Eighth., pp. 159–187). Cambridge: The MIT Press.

Callon, M. (1998). El proceso de construcción de la sociedad. El estudio de la tecnología como herramienta para el análisis sociológico. In M. Domènech & F. Tirado (Eds.), Sociología Simétrica: Ensayos sobre ciencia, tecnología y sociedad. (pp. 143–170). Barcelona: Editorial Gedisa.

Dagnino, R. (2009). Planejamento Estratégico Governamental. (p. 168). Florianópolis-SC: Departamento de Ciências da Administração / UFSC-CAPES-UAB.

Feenberg, A. (2002). Transforming technology: a critical theory revisited (p. 232). New York: Oxford University Press.

Hughes, T. P. (1986). The Seamless Web: Technology, Science, Etcetera, Etcetera. Social Studies of Science, 16(2), 281–292. doi:10.1177/0306312786016002004

Latour, B. (2008). Reensamblar lo social: una introducción a la teoría del actor-red (p. 392). Buenos Aires: Manantial.

Lundvall, B.-Ä. (1994). The Learning Economy. Journal of industry studies, I(2), 23–42.

Matus, C. (1996). Adeus, senhor presidente: governantes governados (p. 219). São Paulo: Fundap.

Pinch, T., & Bijker, W. (2001). The social constrution of facts and artifacts: or how the sociology of science and the sociology of technology might benefit each other. In W. Bijker, T. Hughes, & T. Pinch (Eds.), The social construction of technology systems: New directions in the sociology and history of technology. (Eighth., pp. 17–50). Cambridge, Massachusetts: The MIT Press.

Quintanilla, M. (2005). Tecnología: un enfoque filósofico y otros ensayos de filosofía de la tecnología (p. 296). México D.F.: Fondo de Cultura Económica.

SENA. (2012). Informe de gestión SENA: noviembre 2011-octubre de 2012. Dirección de Planeación y Direccionamiento Corporativo. Retrieved from http://mgiportal.sena.edu.co/downloads/rendiciontrabajo/documentos/03_informe_gestion_sena_noviembre_2011_octubre_2012.pdf

Thomas, H. (2008). Estructuras cerradas versus procesos dinámicos: trayectorias y estilos de innovación y cambio tecnológico. In H. Thomas & A. Buch (Eds.), Actos, actores y artefactos: Sociología de la tecnología (pp. 217–262). Bernal-Buenos Aires: Universidad Nacional de Quilmes-Editorial.

Thomas, Hernán, Santos, G., & Fressoli, M. (Eds.). (2013). Innovar en Argentina: seis trayectorias empresariales (p. 260). Buenos Aires: Lenguaje Claro Editora.

Prado Oseguera, Diana Marisol. (2010). Metodología para el establecimiento de objetivos de control como un medio de seguridad en el área de tecnologías de información. México: Tesis de Maestría, http://tesis.ipn.mx/xmlui/handle/123456789/6771

Alcantar Hernández, Fernando. (2010). Revisión de normas y estándares de sistemas de gestión de seguridad de la información. México: Tesis de Maestría, http://tesis.ipn.mx/xmlui/handle/123456789/6885

Fajardo, Sergio. (2017). El poder de la decencia. Colombia