EL NIVEL DE DESARROLLO DE LA GESTIÓN DE RIESGO CIBERNÉTICO EN LAS INSTITUCIONES PRESTADORAS DE SERVICIOS DE SALUD (IPS): UN ANÁLISIS BAJO EL CONTEXTO DE GOBIERNO CORPORATIVO

Camilo Andrés Martínez Díaz

Colegio de Estudios Superiores de Administración – CESA

Maestría en Administración de Empresas

Bogotá

2020

EL NIVEL DE DESARROLLO DE LA GESTIÓN DE RIESGO CIBERNÉTICO EN LAS INSTITUCIONES PRESTADORAS DE SERVICIOS DE SALUD (IPS): UN ANÁLISIS BAJO EL CONTEXTO DE GOBIERNO CORPORATIVO

Camilo Andrés Martínez Díaz

Tutores

Maria Andrea Trujillo Dávila

Alexander Guzmán Vasquez

Colegio de Estudios Superiores de Administración – CESA

Maestría en Administración de Empresas

Bogotá

2020

Tabla de contenido

Introducción

En el mundo actual, donde la operación de las compañías depende en un alto porcentaje de la tecnología (infraestructura y aplicaciones), con conexiones y comunicaciones globales a través de internet, un manejo de grandes volúmenes de datos e información; es muy común hablar sobre los servicios en la nube, el ciberespacio, ataques cibernéticos y la ciberseguridad. Es la ciberseguridad lo que anteriormente se conocía como la seguridad de la información, la cual tiene como objetivo proteger la información de todo tipo de amenazas o ataques cibernéticos garantizando su confidencialidad, integridad y disponibilidad en el ciberespacio (von Solms & von Solms, 2018).

Ante la materialización de un ciberataque, los costos directos e indirectos que debe asumir una compañía son aquellos asociados a los servicios de outsourcing para remediar el inconveniente en el caso de los directos y en los indirectos aquellos relacionados con las investigaciones al interior, la pérdida de clientes producto del incidente y la afectación de la imagen y valor de la compañía ante el riesgo reputacional generado por el incidente una vez se hace público.

Para conocer el impacto de un ataque cibernético en una compañía, vale la pena revisar algunos sucesos de este tipo que fueron revelados en los últimos años. En el año 2013 de los sistemas de información de Target Corp. fueron sustraídos los datos personales de más de 60 millones de clientes (Rothrock, Kaplan, & Van Der Oord, 2018), razón por la cual el Institutional Shareholder Services Inc. recomendó a los accionistas de la compañía cambiar 7 de los 10 miembros de la junta directiva (Georg, 2017); en el año 2014 Sony Pictures Entertainment sufrió el ataque del grupo de hackers Guandians of Peace (GOP) el cual logró sustraer información sensible de los empleados, además de guiones y películas que fueron filtrados en internet (Haggard & Lindsay, 2015), se estima que este ataque le costó a la compañía en investigación y remediación unos 15 millones de dólares (Rushe, 2015); uno de los casos más conocidos que fue relacionado con las votaciones de

las elecciones presidenciales de 2016 en los Estados Unidos de América, se ejecutó a través de Facebook, donde en el año 2018 se hizo público que para esa época fueron comprometidos datos personales de más de 87 millones de usuarios con el acceso que logró obtener la empresa de minería de datos Cambridge Analytica (Hutchinson, 2018); otra caso muy reciente está relacionado con una filial europea de Toyota Boshoku Corporation, fabricante japonés de autopartes y parte del grupo Toyota que el 6 de septiembre de 2019 hizo público un comunicado, informando que fue víctima de ordenes fraudulentas por parte de un tercero malicioso el cual logro que le generaran pagos por más de 34 millones de dólares haciéndose pasar por alguien de la compañía (Toyota Boshoku, 2019).

Como lo confirma el informe Cost of Data Breach 2018 de Ponemon Institute para IBM Security donde se exponen las implicaciones y efectos de la pérdida de datos para las empresas, las violaciones de datos generan un costo promedio de 3,86 millones de dólares a nivel mundial (IBM & Ponemon Institue, 2018 Cost of a Data Breach Study: Global Overview, 2018) y si se compara con el informe para el año 2019 este valor presenta un incremento de 1,5% llegando a los 3,92 millones de dólares (IBM & Ponemon, Cost of a Data Breach Report 2019, 2019).

Si se analiza este tipo de delitos en el sector de la salud; para el año 2017 según el Centro de Recursos contra el Robo de Identidad de los Estados Unidos de América (ITRC por sus siglas en ingles), en ese país se presentaron más de 374 casos de violaciones de datos, equivalentes a 5,06 millones de registros expuestos (Identity Theft Resources Center, 2018). Uno de los casos de robo de información más sonados en este sector durante el año 2018, se presentó en Health South East RHF la organización de atención médica que administra los hospitales en la región sureste de Noruega, donde se estima que 2,9 millones de datos de usuarios pueden tener información comprometida (Paganini, 2018).

Para el caso del mismo sector en análisis, el informe del 2018 presenta un costo promedio de 408 dólares por registro robado (IBM & Ponemon Institue, 2018 Cost of a Data Breach Study: Global Overview, 2018), mientras que en el informe del 2019 el costo asciende a 429 dólares, continuando con el liderazgo por noveno año consecutivo, como los incidentes más costosos dentro de todas las industrias analizadas en este informe y llegando a reportar costos totales por 6,45 millones de dólares para la industria de la salud (IBM & Ponemon, Cost of a Data Breach Report 2019, 2019).

Ante este panorama creciente de ataques cibernéticos cada vez más complejos y sofisticados, y dado el impacto operativo, económico, legal y reputacional en las compañías; la Unión Europea, la Organización Internacional de Estandarización (ISO por sus siglas en ingles), el Instituto Americano de Contadores Públicos Certificados (AICPA por sus siglas en inglés), la Asociación de Auditoría y Control de los Sistemas de Información (ISACA por sus siglas en ingles) y otra serie de grupos, han buscado dar a las compañías herramientas y marcos para establecer un manejo adecuado al riesgo cibernético y proteger la información de sus clientes, proveedores y de la operación misma del negocio.

Si se analiza el comportamientos de los miembros de Junta de las compañías con respecto a este tema, en general ya están reconociendo la importancia y su responsabilidad en la gestión del riesgo cibernético, como lo demuestra el resultado de la encuesta adelantada por Rothrock, Kaplan & Van der Oord con un 58% de respuesta afirmativa por parte de los encuestados, además de manifestar que las juntas no están preparadas para garantizar la ciberseguridad (Rothrock, Kaplan, & Van Der Oord, 2018).

A pesar de las condiciones mencionadas anteriormente (creciente número de ataques, costo en los 4 ámbitos, herramientas para prevenir la amenaza y la conciencia del riesgo) se percibe que el

manejo del riesgo cibernético sigue siendo un tema operativo y no estratégico para los miembros de las juntas directivas, ya que dentro del ambiente de control y de los órganos de gobierno más importantes de una organización este tema no hace parte de la agenda; y como lo mencionan Rothrock, Kaplan & Van der Oord la ciberseguridad no puede ser solo un tema que preocupe al departamento de tecnología, este es un tema que debe importar a todo el negocio, y en especial a la junta directiva (Rothrock, Kaplan, & Van Der Oord, 2018).

Ante el panorama expuesto anteriormente, este trabajo buscar a partir de un diagnóstico de las prácticas de gestión del riesgo cibernético en las Instituciones Prestadores de servicios de Salud (IPS) en Bogotá bajo el contexto de Gobierno Corporativo, identificar cuáles son los principales componentes dentro de la gestión de estos riesgos, analizar la relación entre el sistema de gestión del riesgo cibernético y los órganos de Gobierno Corporativo y a partir de los resultados de este proceso confirmar si el nivel de desarrollo de la gestión de riesgo cibernético es incipiente, si realmente este no es un tema que haga parte de la agenda de los órganos de Gobierno Corporativo de los IPS, si esta es una responsabilidad que se deja a cargo de los departamentos técnicos y operativos, específicamente al área de Tecnología, donde en su gran mayoría este tema se aborda como una más de las responsabilidades del área de Infraestructura Tecnológica y no en un departamento, comité o subárea destinada específicamente a la responsabilidad del tratamiento de la seguridad informática.

El documento está compuesto por una sección teórica donde se presentan los términos importantes para la comprensión del problema expuesto anteriormente, el estado del arte del riesgo cibernético, seguido de la metodología adelantada para conocer el manejo del riesgo al interior de las IPS y por último la exposición de los resultados de la información recopilada junto con su análisis, conclusiones y recomendaciones.

Marco Teórico

Una brecha o violación de seguridad es definida por el ITRC (Identity Theft Resources Center) como un incidente en que el dato personal (información de cuentas bancarias, tarjetas de crédito, cuentas de correo o usuario con contraseña, etc.) está potencialmente en riesgo debido a una exposición electrónica o en papel (Identity Theft Resources Center, 2018).

Dentro de los principales tipos de violación de seguridad o tipos de técnicas de ataque a las compañías se encuentra el envío de malware o virus que lidera el porcentaje de técnicas de ataque con el 36%, seguido por el phishing con un 33% el cual consiste en enviar un correo invitando al usuario a acceder a una página señuelo con el objetivo de obtener información confidencial como contraseñas; se encuentran también los ataques de rasomware que buscan secuestrar la información del usuario y mediante el pago a través de monedas electrónicas como el bitcoins (moneda electrónica) dar nuevamente acceso a la información, de otro lado están los ataques de fuerza bruta que mediante sistemas computarizados buscan acceder a servidores o sistemas de información y la suplantación de identidad bajo la técnica de "men in the middle" (PWC, 2018).

Cualquiera de los tipos de violaciones mencionadas anteriormente, es generada bien sea por el ataque de un hacker (persona maliciosa que busca sustraer información para generar un daño o beneficio económico personal), un error humano al interior de la compañía o una falla en uno de los sistemas de protección; esta violación es tratada mediante la ciberseguridad que en la norma ISO/IEC 27032:2012 se define como la "preservación de la confidencialidad, integridad y disponibilidad de información en el ciberespacio", mientras que la norma ISO/IEC 27000 define la seguridad de la información como "la preservación de la confidencialidad, integridad y disponibilidad de la información"; lo cual permite concluir que la ciberseguridad aborda

únicamente la seguridad de la información en el ciberespacio, es decir todos aquellos activos de información digital que pueden llegar a ser accedidos a través de internet, mientras que la seguridad de la información cubre la seguridad en general bajo cualquier espacio o ámbito (ISO, 2018).

Por su parte la Agencia para la Seguridad de la Información y Red de la Unión Europea (ENISA) dentro de su documento "Definición de Ciberseguridad – Lagunas y solapamientos en la estandarización" define que la ciberseguridad es un término envolvente que hace imposible construir una definición que cubra todo lo que abarca este término (ENISA, 2015); de otro lado Eva Ignatuschtschenko afirma que el daño cibernético es la consecuencia perjudicial de los eventos cibernéticos, el cual puede tener consecuencias tanto físicas, como psicológicas, económicas, de reputación y/o sociales, afectando a personas, organizaciones, infraestructuras o intereses nacionales (von Solms & von Solms, 2018).

La ciberseguridad cubre todo aquello relacionado con el ciberespacio o entorno cibernético que de acuerdo con La Unión Internacional de Telecomunicaciones (ITU por sus siglas en inglés) "incluye los usuarios, redes, dispositivos, software, procesos, información almacenada o en tránsito, aplicaciones, servicios y sistemas que pueden ser conectados directa o indirectamente a las redes" (ENISA, 2015) en especial cuando se habla de conexión a redes se hace referencia a internet.

Para el manejo del riesgo cibernético en una organización, es importante contar con un Gobierno de la Ciberseguridad que de acuerdo con von Solms & von Solms se define como "el proceso de dirigir y controlar la protección de los activos de información digital de una empresa frente a los riesgos relacionados con el uso de internet". Manejo que puede darse mediante la concepción de una arquitectura de control; arquitectura que de acuerdo con COSO (The Committee of Sponsoring Organizations of the Treadway Commission) debe estar compuesta por: (i) un

ambiente de control, (ii) la gestión de riesgos, (iii) actividades de control, (iv) información y comunicación y (v) monitoreo (Superfinanciera, 2014).

Dicha arquitectura puede estar liderada o apoyada por el comité de auditoría que, como órgano de Gobierno Corporativo, tiene desde el punto de vista legal la función de supervisar el cumplimiento del programa de auditoría interna, el cual debe contemplar los riesgos del negocio y evaluar integralmente todas las áreas de la compañía (Trujillo Davila, Guzman Vasquez, & Prada Ramirez, 2015).

Estado del Arte

Los hackers o cibercriminales que anteriormente tenían como finalidad demostrar sus habilidades y conocimientos han cambiado, ahora su objetivo es realizar ataques con la intención de obtener un beneficio económico o generar algún daño, su perfil ha cambiado, ya no se trata de personas de 15 o 16 años, su promedio de edad ahora es de 36 años, algunos pertenecen a una organización criminal y son quienes manejan la industria del cibercrimen, "industria" que viene presentando una evolución en volumen, sofisticación e impacto, todo ello producto de la ciber dependencia generada por la creciente interconexión de personas, cosas y organizaciones (Deloitte, 2018). Hoy en día la tendencia del cibercrimen es creciente a nivel global, como lo demuestra el hecho de que al día sean enviados más de 6.4 billones de "fake e-mail" o que en el primer cuarto del 2018 fueron enviados 550 millones de mensajes de phishing por una sola campaña (EY, 2018). En Colombia por ejemplo desde el año 2015 se han registrado 31.498 denuncias por delitos informáticos que incluyen desde robos de información hasta suplantación de identidades (Portafolio, 2019) y para el año 2018 fue el país de América Latina con más detecciones de tipo

rasomware (secuestro de datos) con el 30% de amenazas detectadas según la empresa de seguridad informática ESET (Dinero, 2019).

Esta llamada “industria” genera según Gartner un gasto mundial en seguridad de información estimado para el 2018 de 114.000 millones de dólares y se estima que para el año 2019 el gasto superó los 124.000 millones de dólares (Moore & Keen, 2018); además se considera que deja a los cibercriminales cerca de 3,5 trillones de dólares al año superando al negocio del narcotráfico que se estima deja cerca de 1 trillón de dólares (El Telegrafo, 2019).

Dentro de las principales causas de las violaciones de datos que afectan actualmente a las compañías sobresalen los ataques maliciosos y criminales que representan para el 2019 el 51%, los errores humanos por parte de empleados y contratistas que representan el 24% y el restante 25% corresponden a fallas en los sistemas. La identificación de estas intromisiones le toma en promedio a las compañías 206 días, mientras que el tiempo promedio para contenerla es de 73 días; estos dos tiempos crecieron un 4,9% con respecto a los reportados el año anterior (197 y 69 respectivamente) en el mismo informe (IBM & Ponemon, Cost of a Data Breach Report 2019, 2019) lo que demuestra la mayor complejidad de los ataques actuales.

Con respecto al tipo de compañías que son más propensas a sufrir algún ataque por parte de estos cibercriminales, de acuerdo con el estudio realizado por Kamiya, Kang, Milidonis, & Stulz para los 6328 casos de ataques cibernéticos reportados en el Privacy Rights Clearinghouse (PRC) entre los años 2005 y 2014, se identifican aquellas organizaciones que son más visibles, es decir, grandes empresas, empresas incluidas en la lista de Fortune 500 o aquellas que se encuentran en industrias que son menos competitivas.

A pesar de que no se identifica ninguna relación entre las características del gobierno corporativo con respecto a la proporción de miembros independientes en la junta o el número de

miembros de la misma y la probabilidad de presentarse un ciberataque, si se reconoce que las empresas que dentro de sus órganos de gobierno corporativo prestan más atención a la gestión del riesgo son menos propensas a ser atacadas (Kamiya, Kang, Milidonis, & Stulz, 2018).

Cuando las organizaciones identifican que han sufrido un ataque cibernético y lo hacen público, la pérdida promedio en la capitalización de mercado es de alrededor del 1%; este porcentaje se puede incrementar en particular en aquellas organizaciones que sufren de robos de información personal financiera, como números de tarjetas de crédito o cuentas bancarias, lo que indica una pérdida de valor de mercado promedio de 890 millones de dólares. Impacto que puede ser aún más negativo cuando no hay evidencia que demuestre la atención por parte de la Junta Directiva para el manejo del riesgo. Con respecto a la remuneración para el CEO después de un ciberataque, se ha identificado que la junta llega a reducir significativamente el porcentaje del bono con respecto a su pago total. (Kamiya, Kang, Milidonis, & Stulz, 2018).

Con el objetivo de que en las empresas se aborde la ciberseguridad con la rigurosidad necesaria, existen regulaciones que obligan a las compañías a proteger la información de sus clientes; por ejemplo en el año 2015 entró en vigencia la ley de seguridad TI en Alemania; en el caso de la Unión Europea (UE) en el año 2014 se adoptó la directiva sobre la seguridad de las redes y la información (NIS) (Georg, 2017) y para el año 2018 en la ciudad de Nueva York entraron en vigor los Requisitos de Ciberseguridad para Compañías de Servicios Financieros, en Australia el esquema de notificación de violaciones de datos (NBD por sus siglas en ingles) (Gemalto, 2018) y en la Unión Europea (UE) la Regulación de Protección General de Datos (GDPR por sus siglas en inglés) cuyo principal objetivo es unificar tanto los derechos como obligaciones de todos los países de la UE respecto a la protección de los datos y garantizar que las empresas que sufran perdidas de información de algún ciudadano de la UE, informen sobre la perdida de datos en 72

horas de lo contrario podrán ser multadas con más del 4% de su facturación anual (Sharf, 2016); para el caso de Colombia existe la ley 1581 de 2012, señalada como la ley de protección de datos personales, la cual faculta a la Superintendencia de Industria y Comercio (SIC) para imponer multas a aquellas organizaciones que pierdan datos personales de sus clientes (Congreso de La República de Colombia, 2018). En el caso del sector salud, la Super Intendencia Nacional de Salud mediante la Resolución 4559 del 11 de abril de 2018 adopta el modelo de Supervisión Basado en Riesgo (EBS), cuyo objetivo general es identificar para las entidades vigiladas los factores de riesgo que generan mayores amenazas, además de "Aumentar el compromiso y responsabilidad de las Juntas Directivas y órganos administrativos de las entidades frente a la adecuada gestión de los riesgos" (Supersalud).

Además de las regulaciones mencionadas anteriormente, existen una serie de iniciativas que buscan dar a las compañías recomendaciones para el manejo de la seguridad de la información, tal es el caso de las normas publicadas por la ISO, como la ISO/IEC 27001 que aborda los requisitos para establecer un plan para el Sistema de Gestión de Seguridad de Información (SGSI), o la ISO/IEC 27002 que plantea una serie de recomendaciones para la gestión de la seguridad de la información con 114 controles, 35 objetivos y 14 áreas, o la ISO/IEC 27014 que aborda el tema de Gobierno de Seguridad de la Información y su integración con el Gobierno Corporativo de la compañía, y con respecto a la gestión de la ciberseguridad se publicó la norma ISO/IEC 27032 (ISO, 2018). De otro lado están las Directrices para la Seguridad de Sistemas y Redes de Información publicados por la Organización para la Cooperación y el Desarrollo Económico (OCDE) que buscan promover una cultura de seguridad (Organization for Economic Co-operation and Development, 2004) o los recursos proporcionados por AICPA para la evaluación y reporte del programa de administración del riesgo de ciberseguridad y sus controles subyacentes (AICPA,

2018); además de tener también a disposición el marco de Objetivos de Control para Tecnologías de Información y Tecnologías relacionadas (COBIT), el cual propone controles específicos para IT desde la perspectiva del negocio (EAFIT, 2007). Sin embargo, es importante aclarar que el hecho de implementar estas recomendaciones no garantiza el 100% de protección de la compañía, ni que el tema de ciberseguridad esté presente dentro de la agenda de la Junta Directiva (Georg, 2017).

De acuerdo con el Reporte de Riesgo Global de 2018, realizado por el Foro Económico Mundial a partir de la encuesta de percepción de riesgos globales adelantada entre el 28 de agosto y el 1 de noviembre de 2017, los 871 encuestados en una escala de 1 a 5 (impacto: 1 impacto mínimo y 5 impacto catastrófico, probabilidad: 1 muy poco probable que ocurra y 5 muy probable que ocurra) dieron una valoración para el riesgo de ciberataques de 3,64 con respecto al impacto y de 4,01 respecto a la probabilidad; para el caso del riesgo de fraude o robo de datos la calificación fue de 3,98 respecto a la probabilidad de ocurrencia y de 3,3 respecto al impacto (World Economic Forum, 2018), estos mismos riegos junto con el de ataques a la infraestructura critica fueron incluidos en el mismo reporte para el año 2019, donde además se estiman pérdidas financieras en 2019 relacionadas con ataques de robo de datos y dinero en un 82% e interrupción de las operaciones en un 80% (World Economic Forum, 2019). Estos resultados confirman que hay conciencia respecto al impacto y materialización del riesgo cibernético y sus consecuencias.

Los riesgos cibernéticos son la segunda mayor preocupación para los directores ejecutivos, según una encuesta realizada a 103 directivos por Price Waterhouse Coopers en el año 2015(PwC) (Georg, 2017), lo cual puede confirmarse en el informe “2019 Hot topics for IT Audits in Financial Services” de Deloitte donde se indica que desde el año 2015 el tema principal a tratar dentro de las auditorías internas del departamento de Tecnología es la ciberseguridad, sin embargo a pesar

de este escenario, los miembros de junta perciben el tema de seguridad de la información como un gasto y no ven la necesidad de dedicar tiempo a este tema dentro de sus agendas; así lo demuestran los resultados de una encuesta practicada el 2014 en Estados Unidos de América a 75 miembros de junta, donde el 29% de ellos informó que no recibe ningún tipo de información con respecto a los riesgos de seguridad, mientras que el 30% indica que si recibe información pero solo una vez en el año (Georg, 2017).

El escenario es complejo, las compañías están inmersas en la tendencia de la transformación digital, buscan facilitar el crecimiento y mejorar la rentabilidad mediante el uso seguro de las nuevas tecnologías (Deloitte, 2019) reconociendo que la información se ha convertido en el activo corporativo más valioso y crítico, las características de los atacantes han cambiado, en el pasado se buscaba afectar la operación e infraestructura física, ahora se busca acceder a los recursos informáticos, el número de ataques ha crecido, el 49% de las empresas en el mundo afirma haber sufrido algún tipo de fraude entre 2016 y 2018 (PWC, 2018), en Colombia este indicador es del 39% (PWC, 2018), se ha demostrado el impacto que puede llegar a tener un ciberataque en el negocio, pero aun así, no hay conciencia en las organizaciones respecto al manejo del cibercrimen, incluso la incredulidad predomina en algunos casos donde se piensa que la compañía nunca sufrirá de ningún ataque por no estar en la mira de los ciberdelincuentes (Deloitte, 2018) y en aquellas organizaciones donde hay algo de conciencia y se reconoce la importancia de gestionar este riesgo, solo el 37% confía en su esquema de seguridad (Rothrock, Kaplan, & Van Der Oord, 2018).

Bajo el panorama en el que la mayoría de las Juntas no están preparadas para garantizar la ciberseguridad, Georg L.(2017) registra que algunas juntas han optado por asignar la responsabilidad de gestionar los informes de riesgo de seguridad al comité de auditoría; otras simplemente han entregado la responsabilidad a una aseguradora bajo un ciberseguro, o se han

desentendido del tema dejándolo de lleno bajo la responsabilidad del departamento de Tecnología, donde normalmente se han concentrado en prevenir los ataques, en mantener lejos los cibercriminales de sus sistemas de información y no ante lo que ahora se considera lo más importante, la resiliencia del negocio, que como la describen Rothrock y sus colaboradores (2018) en este caso se trata de la respuesta ante un ataque, de la posibilidad de continuar operando el negocio mientras se lucha y se recupera del ataque.

Con el objetivo de prepararse para dar una respuesta adecuada ante un ataque Rothrock et al(2018) proponen trabajar en 4 frentes: 1) Educar a la alta dirección, con el objetivo de que comprendan que está en riesgo y acepten su responsabilidad, siendo consientes además de que no existe el 100% de seguridad y la necesidad de la resiliencia; 2) Usar un lenguaje común, con el objetivo de que se entiendan los términos y el tema de riesgo cibernético haga parte del orden del día de cada reunión de la Junta; 3) Distinguir entre seguridad y resiliencia, con el liderazgo por parte de la Junta en la definición de políticas y prácticas de resiliencia encaminadas a lograr un equilibrio entre la seguridad y el negocio, 4) Hacer de la seguridad y la resiliencia una estrategia de negocio.

Otra opción que pueden tomar las organizaciones para reducir el riesgo de pérdida de datos es seguir estos pasos propuestos por Ponemon Institute, 1) Evaluar que datos se quieren proteger, 2) Considerar el monitoreo y análisis de comportamiento de quien accede a los datos y que se hace con estos, 3) Crear políticas y procedimientos, 4) Mantener la seguridad perimetral y los firewall, 5) Encriptar discos de los dispositivos portátiles y 6) Definir un plan de respuesta a incidentes (IBM & Ponemon Institue, 2018 Cost of a Data Breach Study: Global Overview, 2018).

En la actualidad son varias las opciones para tratar la ciberseguridad desde los órganos de Gobierno Corporativo, está la propuesta de tener miembros que tengan experiencia en temas de

seguridad dentro de las Juntas (Islam & Stafford, 2017) o la de contratar un CEO con experiencia en TI o implementar comités de tecnología al nivel de la Junta ya que en estos casos se tiene más probabilidad de detectar y reportar las violaciones de seguridad (Haislip, Lim, & Pinsker, 2017), o también en los casos en que las Juntas encargan al comité de auditoría supervisar estos temas, está la propuesta de Ernst & Young (EY) que hace referencia a la importancia de tener al interior del comité: a) Claridad respecto al programa de gestión de ciber riesgos, b) Confianza en la idoneidad del programa y c) Garantía en la información que reciben, además de que el programa de gestión de riesgos de ciberseguridad este alineado con el programa general de gestión del riesgo institucional de la organización y sus objetivos de negocio (Ernst & Young - EY, 2017); o está la propuesta de Deloitte de definir un programa (no un proyecto) robusto de ciber riesgo, cuyo objetivo es ser **seguro**, teniendo controles contra las amenazas conocidas y emergentes, ser **vigilante**, monitoreando amenazas para anticipar e identificar comportamientos dañinos y ser **resiliente**, estando preparado para recuperarse ante un incidente buscando además minimizar el impacto (Deloitte, 2018). Otra de las propuestas contempla que la Junta Directiva constituya un nuevo comité de ciberseguridad, el cual se encargara de liderar todo el tema de control de riesgo cibernético y como lo registran Upadhyay, Bhargava y Faircloth las empresas que cuentan con más de tres comités de supervisión tienen un efecto positivo sobre el desempeño de la empresa (Trujillo Davila, Guzman Vasquez, & Prada Ramirez, 2015).

Metodología

Esta investigación se basa en la metodología de estudios de caso, la cual permite adelantar una discusión teórica haciendo uso de la realidad empírica, sin dejar de lado la literatura relevante para el tema en cuestión (Yin, 2014). Como Yin (2014) lo menciona, esta es una metodología que de la

misma manera que los experimentos son generalizables a proposiciones teóricas y no a universos o poblaciones, es decir representa una "muestra" alineada hacia la generalización analítica y no hacia la generalización estadística.

Para la obtención de los datos a analizar, se seleccionaron dos actores relevantes que a través de entrevistas a profundidad comunicaron su percepción de como las IPS abordan el riesgo cibernético. En dichas entrevistas cualitativas a profundidad, las cuales como lo describen Taylor y Bogdan son encuentros cara a cara entre el investigador y los informantes, enfocados hacia la comprensión de las perspectivas que tienen los informantes respecto a un tema específico a tratar (Taylor & Bogman, 2008), se aplicó el cuestionario construido (Anexo 1) a partir de las mejores prácticas para el manejo del riesgo cibernético en las compañías.

Se seleccionó esta técnica de investigación cualitativa, teniendo en cuenta que esta herramienta se recomienda para abordar temas que no se discuten abiertamente con otras personas o en grupos de discusión, además de propiciar una mayor comodidad y sinceridad en las respuestas por parte del entrevistado y principalmente por la ventaja que ofrece de lograr obtener información detallada que quizás con otros métodos de recopilación de datos no se obtiene (Boyce & Palena, 2006), además de que esta técnica permite entender el fenómeno en estudio a partir del punto de vista de los entrevistado (Gubrium, Holstein, Marvasti, & McKineey, 2012).

Estas entrevistas que además pretendían identificar el nivel de conocimiento por parte de los entes de gobierno corporativo sobre el manejo al riesgo cibernético, se procuró aplicarlas a los directores del departamento de tecnología o encargados del manejo del riesgo cibernético en 2 de las Instituciones Prestadoras de servicios Salud más importantes y referentes en la ciudad de Bogotá, que en adelante llamaremos Institución A e Institución B[1].

[1] No se mencionan los nombres de las Instituciones seleccionadas por confidencialidad.

Institución A

Es una entidad privada de carácter social creada hace más de 40 años, líder a nivel nacional en la prestación de servicios de salud con la más alta calidad científica, humana, ética y tecnológica; cuyo propósito ha sido influir de manera positiva en el sector de la salud y propender por el bienestar de los individuos y comunidades, estableciendo su accionar como complemento a los servicios de salud, en educación y gestión del conocimiento y la salud pública. Esta Institución define sus valores como la excelencia, honestidad y carácter y sus principios como el respeto, la responsabilidad, la creatividad y el compromiso, los cuales le han permitido contar en la actualidad con más de 15 reconocimientos entre certificaciones, acreditaciones y galardones.

Institución B

Se proyecta como la compañía líder de atención domiciliaria, cuenta con más de 25 años de experiencia en el país, tiene presencia en otras 7 ciudades además de Bogotá, así como cobertura internacional en más de 10 países. Cuenta con el respaldo de uno de los grupos aseguradores más importante del mundo y mas de 500 médicos especialistas. Dentro de los principales valores corporativos de esta Institución se destacan la pasión por el cliente donde se busca superar las expectativas de estos, la calidez humana donde se priorizan las necesidades de los demás y el espíritu emprendedor donde constantemente buscan alcanzar metas retadoras.

Las entrevistas que se desarrollaron de manera presencial duraron entre 40 y 60 minutos, cumpliendo con la recomendación que hacen Granot, Thomas y Motta respecto a la longitud promedio de las entrevistas de una hora (Granot, Brashear, & Motta, 2012). Estas iniciaron con la presentación del objetivo del trabajo de investigación junto con el objetivo de la entrevista misma:

“Conocer sobre las prácticas de gestión del riesgo cibernético en la Institución a partir de las mejores prácticas definidas por los marcos para el manejo de este riesgo”; a continuación, se desarrolló la entrevista dividiéndola en tres partes para cubrir los siguientes temas:

1. Aspectos generales sobre la estructura y recurso humano encargado del manejo de la seguridad informática y el riesgo cibernético en la Institución.
2. Manejo de la seguridad informática y el ciberriesgo en la Institución. (Procesos, Comités, Planes de continuidad, etc.).
3. Información sobre el Gobierno Corporativo de la Entidad y su conocimiento o participación en el manejo del riesgo cibernético.

Para dar tranquilidad a los entrevistados sobre la confidencialidad de la información recopilada se les informo previamente que se trataba de un ejercicio netamente académico donde firmamos un acuerdo de confidencialidad y los resultados no serían discutidos de manera particular nombrando la Institución, sino como un agregado de lo que resulte de todas las entrevistas.

A partir de la información recopilada (se transcribe una de las entrevistas en el Anexo 2), se realizó el proceso de análisis con el objetivo de identificar comportamientos, definiciones, iniciativas y procesos en común dentro de las Instituciones para compararlos con las mejores prácticas definidas y de esta manera establecer el nivel de desarrollo en el manejo del riego cibernético, los resultados de este análisis se revisan en el siguiente capítulo.

Resultados Obtenidos

En las Instituciones desde la Junta Directiva efectivamente existe la preocupación por la gestión del riesgo cibernético declarándolo como uno de los más críticos como lo mencionó uno de los directores de TI entrevistados “Tenemos 5 grandes riesgos que valorar en seguridad y continuidad,

y uno de esos es ciberataque", sin embargo, la responsabilidad de la gestión de este se traslada al departamento de TI, específicamente al director del área.

En el departamento de TI una persona o pequeño grupo es el encargado del manejo de la seguridad informática, sobre estos recae la responsabilidad de la gestión de los controles e iniciativas para mitigar el riesgo cibernético; este recurso cuenta con el apoyo de la jefatura de riesgos, compliance, auditoría interna y/o el comité de seguridad informática constituido recientemente para la gestión de los controles, pero es claro que no comparte la responsabilidad del riesgo con estas jefaturas.

A pesar de la importancia del manejo adecuado del riesgo cibernético, las iniciativas de mitigación del riesgo que se tienen son propuestas que surgen desde el área de TI y no desde la estrategia. Los órganos de gobierno solo tienen conocimiento de estas iniciativas al momento de justificar la inclusión de estas dentro del presupuesto anual del departamento como lo menciona uno de los entrevistados "hay junta directiva mensualmente en la que una vez al año hay que presentar informe de ciber riesgos y aprobar el presupuesto de seguridad del próximo año. El año pasado en una sola reunión se trataron los dos temas".

En las Instituciones se siguen buenas prácticas como adelantar campañas o cursos virtuales al interior, con el objetivo de informar y concientizar a los funcionarios sobre el riesgo cibernético; se contratan servicios externos para evaluar la efectividad de sus controles, cuentan con herramientas para evitar fugas de información y se implementan algunas de las propuestas de la norma ISO 27001 para el manejo de la seguridad informática buscando garantizar la integridad, disponibilidad y confidencialidad de la información.

No existe ninguna normatividad o legislación que los regule con respecto al manejo de seguridad de la información, más allá del cumplimiento de la ley de protección de datos personales y la gestión del riesgo general que define la Superintendencia Nacional de Salud.

Ninguna de las Instituciones manifiesta haber sufrido algún ataque de tipo cibernético y tampoco reconoce la necesidad de contar con algún integrante dentro de la Junta Directiva con conocimientos avanzados en ciberseguridad; es posible que en este caso como lo menciona Matlay, H., & Sørheim, R "existe el peligro de que los encuestados intenten racionalizar su propio comportamiento, dando una respuesta deseable en lugar de su comportamiento real". (Matlay & Sørheim, 2005)

En conclusión, existen iniciativas y buenas prácticas que buscan mitigar la afectación ante una posible ataque cibernético, se percibe un interés por parte de los órganos de gobierno con relación al riesgo cibernético, pero no hay conocimiento sobre el resultado de las acciones que se adelantan en la Institución con el objetivo de reducir la probabilidad de materialización de dicho riesgo.

Análisis y Conclusiones

Este documento proporciona una imagen un poco más precisa del manejo del riesgo cibernético en las IPS más importantes del país; estudios futuros podrán analizar otras Instituciones cuyos resultados ayudarán ampliando la muestra y permitirán corroborar si las conclusiones que se presentan a continuación son el común denominador en las Instituciones.

Ante la hipótesis inicialmente planteada, ciertos elementos fueron desvirtuados y otros corroborados; efectivamente la responsabilidad de la gestión del riesgo cibernético recae sobre el departamento de Tecnología y no es un tema que se aborde recurrentemente dentro de la agenda de los órganos de Gobierno Corporativo; sin embargo, con respecto al manejo que se da al riesgo, este cuenta con elementos que permiten considerar un nivel aceptable de desarrollo en donde

incluso, se identificó la existencia de comités de apoyo dedicados específicamente a la mitigación del riesgo cibernético, como es el caso de la existencia del comité de seguridad informática.

Teniendo en cuenta lo anterior, con el objetivo de superar el nivel de desarrollo se recomienda que dentro de la agenda de la Junta Directiva se incluya de manera recurrente el tema del riesgo cibernético, dando acceso a las personas responsables de la gestión de este riesgo, no sin antes garantizar que los miembros de la Junta tengan una contextualización previa sobre los conceptos más importantes relacionados con el riesgo cibernético y comprendan el impacto que puede llegar a generar la materialización de un ataque de este tipo.

La preocupación respecto al riesgo cibernético por parte de los miembros de Junta en las Instituciones surge a partir de la percepción de que este es un tema del cual todos están hablando a raíz del boom de la transformación digital por la cual están pasando muchas compañías y no porque realmente conocen el impacto que puede llegar a ocasionar el hecho de no atender de manera adecuada este riesgo. Es por esto por lo que se recomienda que al menos uno de los miembros de la Junta tenga conocimientos sobre ciberseguridad o que por lo menos la Junta se acompañe de un comité de expertos en este tema que le reporte con cierta regularidad y los mantenga actualizados con respecto al manejo de la ciberseguridad.

Por otro lado, es recomendable que desde los entes que regulan la operación de los IPS, se establezca algún tipo de normatividad orientada al manejo específico del riesgo cibernético, teniendo en cuenta la información sensible que manejan y las consecuencias que puede llegar a tener la exposición de esta , como considera uno de los entrevistados, “existe una mayor exigencia al interior del grupo por la gestión del riesgo cibernético que la que nos hacen desde los entes de Gobierno”. Esto permitiría garantizar un buen nivel de desarrollo, con respecto al manejo del riesgo cibernético en las Instituciones, que no dependa como en la actualidad, de las iniciativas

que surgen más por preocupación de los integrantes del departamento de Tecnología y no como un interés general por parte de todos los funcionarios de la Institución.

Anexo 1

CUESTIONARIO PARA LA ENTREVISTA

Buen(a) día(tarde) ***(NOMBRE DEL ENTREVISTADO)***, mi nombre es Camilo Martínez Díaz soy estudiante de MBA en el Colegio de Estudios Superiores de Administración – CESA, actualmente me encuentro desarrollando el trabajo de grado cuyo objetivo busca identificar cuál es el nivel de desarrollo de la gestión de riesgo cibernético en las principales entidades de salud de Bogotá bajo el contexto de Gobierno Corporativo.

En esta conversación buscaremos a partir de sus respuestas, poder realizar un diagnóstico de las prácticas de gestión del riesgo cibernético en ***(NOMBRE DE IPS O EPS)*** y compararlos con una serie de marcos de mejores prácticas para el manejo de este riesgo. En este sentido, siéntase libre de compartir sus ideas. Aquí no hay respuestas correctas o incorrectas, lo que importa es justamente su opinión sincera.

Le recuerdo que la información aquí recopilada es confidencial y solo será tratada con propósitos académicos, además de que no registraremos nombres propios en los resultados del análisis.

Para agilizar la toma de la información, me acompaña ***(NOMBRE DE ACOMPAÑANTE)***. Tomar notas a mano y atender a sus respuestas toma más tiempo y es posible que se escapen temas importantes. Por ello quisiera solicitarle su autorización para que nos acompañe esta persona que me apoyara en el proceso de registro de sus respuestas.

Para iniciar quisiera preguntarle aspectos generales sobre su rol y el departamento que tiene a cargo:

- ¿Cuánto tiempo lleva desarrollando el cargo de ***(CARGO DEL ENTREVISTADO)*** en ***(NOMBRE DE IPS O EPS)***?.
- ¿Están dentro de sus responsabilidades el manejo de la seguridad informática y la gestión del riesgo cibernético?
- ¿Cómo está conformado el departamento de tecnología?

Si NO se mencionó dentro de las áreas el equipo de seguridad informática:

- ¿Hay un especialista al interior de la compañía o proveedor encargado del monitoreo y manejo de la seguridad informática en general?
    - **Explicación: se tienen cargos como CISO (Chief Information Security Officer), CDO (Chief Data Officer) y CRO (Chief Risk Officer).**
- ¿Esta(s) persona(s) a quien le reporta directamente?

Si se menciona dentro de las áreas el equipo de seguridad informática:

- ¿Cuántas personas conforman el equipo de seguridad informática?
- ¿Cuáles son sus perfiles?
- ¿Esta(s) persona(s) a quien le reporta directamente?

Trataremos ahora temas relacionados con el manejo de la seguridad informática y el ciber riesgo en la INSTITUCIÓN:

- ¿Un ciberataque hace parte del análisis estratégico de los riesgos que tiene la Institución?

- ¿Tienen alguna estrategia definida para la gestión de los riesgos de ciberseguridad?

Para ayudar a dar respuesta a la pregunta anterior, se puede apoyar al entrevistado haciendo las siguientes preguntas:

  - ¿Siguen algún modelo o marco de gestión de ciber riesgos?
  - ¿Tienen roles y responsabilidades definidas?
  - ¿Sigue la institución alguna metodología para medir el riesgo de seguridad al que están expuestos? ¿En esta responsabilidad se apoyan con algún área interna como Calidad y Procesos?

- ¿Existe algún comité o ente de gobierno ajeno al departamento, que se encargue de auditar o apoyar los temas de tecnología de la Institución?
- ¿Tienen definidas normas, políticas y procedimientos de seguridad de la información y ciberseguridad?
  - **Explicación: Tienen un SGSI (Sistema de Gestión de Seguridad de la Información) alineado con los principales estándares de buenas prácticas de seguridad como ISO 27001, SOGP (Information Security Forum's Standard of Good Practice) es una serie de buenas prácticas basado en las experiencias del Foro de la seguridad de la información (ISF), ISM3 (Information Security Management Maturity Model).**
  - ¿Tienen alguna normativa o legislación vigente que los regule con respecto a los temas de seguridad de la información?
- ¿Realizan escaneos de vulnerabilidades o hacking ético, además de procesos de hardening sobre sus sistemas más críticos?

SI la respuesta es afirmativa hacer estas preguntas:

- ¿Cada cuánto lo hacen?
- ¿Los resultados se presentan a la Junta?

- ¿Tienen herramientas para la detección y prevención de fugas o robo de información?
  - Explicaciones: soluciones tales como un DLP (Data Loss Prevention), control de dispositivos de almacenamiento externo.
- ¿Tienen controles de seguridad con los proveedores que prestan servicios críticos?
  - ¿Explicación: realizan algún tipo de Cyber-Security Risk Assessment dentro del proceso de selección de un proveedor?
- ¿Para la institución son claras las consecuencias que puede tener un ataque cibernético?
  - ¿Es claro para el departamento de tecnología Y/O para la junta?
- ¿La preocupación de la gestión de la seguridad cibernética es únicamente del departamento de tecnología?
- ¿Adelantan actividades e iniciativas de formación y concienciación con los empleados en temas de ciberseguridad?
  - ¿De qué tipo son?
    - Cursos virtuales
    - Campañas falsas de phishing
    - Correos
    - Intranet
- ¿Tiene la compañía un plan de contingencia ante la materialización de un ataque cibernético?

- ***Explicación: cuentan con Planes de Continuidad de Negocio (PCN) y de recuperación de desastres (PRD), o aislamiento de los sistemas publicados hacia Internet.***
- ¿Qué tan resiliente es la institución ante una falla de los sistemas o la materialización de un riesgo cibernético?
  - Como logran medirlo
- ¿Cómo reaccionarían ante un ataque cibernético?
- ¿Podría continuar su operación en el momento de un ataque cibernético?

- ¿Tiene conocimiento de si la compañía ha sufrido de algún ataque cibernético? ¿Cuál fue su impacto y como fue manejado?
  - ¿Se vio afectada la marca, reputación o propiedad industrial de la Institución?
  - ¿Se generaron sanciones o multas?

Por último, abordaremos preguntas relacionadas con respecto al Gobierno Corporativo:

- ¿Cuál es el ente de Gobierno Corporativo de mayor rango en la Institución?
  - ¿Participa alguien de su departamento en algunas de las reuniones de este ente?
  - ¿Cada cuánto lo hacen?
- ¿Sabe si se trata el tema de ciberriesgos dentro de la agenda de las reuniones de la Junta?
  - ¿Con que regularidad lo hacen?
- ¿Cuál es el nivel de conocimiento sobre ciberseguridad en los miembros de la Junta?

- ¿Qué responsabilidad tienen los consejeros o miembros de junta cuando se produce una brecha en la información confidencial que maneja la institución?
- ¿Considera que debería contar el Consejo de Administración o Junta con un experto en ciberseguridad entre sus miembros?

Ahora bien, para terminar:

¿Quisiera usted ampliar algún tema en particular o realizar algún comentario o sugerencia sobre la entrevista?

Muchas gracias por su tiempo, le recuerdo que la información brindada es de gran ayuda e importancia para el desarrollo de mi trabajo de grado y será tratada de manera confidencialidad.

Anexo 2

TRANSCRIPCIÓN DE ENTREVISTA

¿Cómo está conformado el departamento de TI?

"El departamento de TI esta conformado por 4 áreas: 1) Infraestructura y Operación que se encarga de la parte de telecomunicaciones, soporte a usuarios y la implementación de medidas técnicas de seguridad. 2) Soluciones de tecnología que es la encargada de los sistemas de información, aplicaciones, mantenimiento y soporte sobre estos, 3) Proyectos que se encarga de los proyectos de TI y/o proyectos de negocio que tienen altos componentes de tecnología como telemedicina y 4) Seguridad informática y continuidad de negocio que responde por la gestión de riesgos, seguridad informática y resiliencia operacional. Esta última es la encargada del gobierno de seguridad informática, la parte de la infraestructura y operaciones y la implementación de las medidas. Esta dividida en IT security y Gobierno de seguridad"

¿Cuántas personas componen esta área?

"Son 2 personas en el área de Gobierno y en la parte de IT security son 3"

¿Estas personas a quien reportan directamente?

"Tienen doble nivel de reporte, un reporte al Gerente de TI y un reporte transversal a la regional de seguridad que se encuentra fuera del país"

¿Existe alguna otra área dentro de la IPS que les apoye con esta labor?

"Si, tenemos dos áreas que nos apoyan. 1) el área de riesgos que depende de riesgos corporativos que se encarga de la valoración de los riesgos incluyendo los tecnológicos y la parte de compliance

con respecto a datos personales, 2) el área adscrita a la gerencia financiera que es la que responde por el gobierno de PCI”

¿Existe algún comité ajeno al departamento que se encargue de auditar la labor de esas áreas?

“Si, se audita en varios caminos, Un camino es que hay un comité trimestral de seguridad informática en el cual participa el espónsor (CEO del Instituto), la CISO de Colombia, el gerente de TI, el área de riesgo y el CISO Región, donde validan el cumplimiento y avances de riesgos, medidas técnicas, cumplimientos de planes y manejos de incidentes esa es la agenda normal. Otro esquema de control es que hay unos planes de implementación anuales en 6 diferentes frentes en los que tenemos que dar reportes mensuales:

1. Frente en ISO 27001, No estamos certificados, pero cumplimos con los temas de la norma y Deloitte nos mide el nivel de madurez con respecto a este marco de referencia.
2. Medidas técnicas, que hagan los hardening de x forma, la autenticación y log de tal forma.
3. Medidas de seguridad. Cosas que hace el negocio y tecnología para hacer pruebas de seguridad. Seguridad física, de acceso, controles anti-incendio, desarrollo seguro.
4. Data lost prevention, como prevenimos la perdida de información corporativa sobre todo de las joyas de la corona.
5. Web Presence, como mitigamos que se tengan riesgos para la marca y las aplicaciones que están expuestas a internet.
6. Continuidad de negocio, desde esta área se hace el gobierno de la resiliencia del negocio y le da los parámetros para que el área de operaciones haga la parte de ITSCM (IT Service Continuity Management).

¿Un ciberataque hace parte del análisis estratégico de los riesgos que hace la IPS?

"Si, tenemos 5 grandes riesgos que tenemos que valorar en seguridad y continuidad, y uno de esos es ciberataque"

¿Para quienes son claras las consecuencias que puede tener un ataque cibernético?

"El 100% de la compañía ha hecho awareness y ha hecho el curso formal de los riesgos principales que tiene el ataque cibernético y la ingeniería social"

¿Tienen alguna normativa o legislación vigente que los regule con respecto a los temas de seguridad informática?

"Pues tenemos 2, 1) la Super Intendencia que son los generales para la protección de datos personales y 2) las normativas de Supersalud, que son genéricas para IPS, son mas las normativas del Grupo que las que nos exigen afuera"

¿Siguen algún marco o modelo de gestión del ciber riesgo?

"Si, ISO 27000, NIST en la parte de Cloud y la norma de continuidad.

¿Qué metodología siguen para medir el riesgo?

"La tradicional, tablas de riesgo, probabilidad, impacto financiero, impacto reputacional. Se definen los mapas de calor y tienen unos tiempos de cierre"

¿Realizan escaneo de vulnerabilidades?

"Si, tenemos 3 mecanismos para esto. 1 antes de salir a producción cualquier aplicación expuesta a internet se le hace un ethical hacking por una compañía colombiana; una vez al año desde región

se hace un PENTEST (Pruebas de penetración) a cada aplicación expuesta a internet y 2 veces al año se hace un PENTEST a la infraestructura."

¿Este informe se lleva a la junta?

"NO, se presenta en el comité de seguridad, se muestran los hallazgos y se gestionan los critical y los high critical."

¿Tienen DLP o alguna herramienta para la prevención de fugas o robo de información?

"Eso está para este año, el año pasado se adelantó la parte de clasificación documental, etiquetado, en el 2020 se va a adquirir la plataforma"

¿Tienen controles de seguridad con los proveedores que les prestan servicios críticos?

"SI, hacemos un assessment de los proveedores de misión crítica, que es casi una auditoria ISO27000 y se definen unos planes. Con los que se comparte información critica se les hace un PENTEST autorizado.

¿Adelantan actividades e iniciativas de formación y concienciación con los empleados en temas de ciberseguridad?

"SI, tenemos 3 píldoras mensuales y 3 cursos publicados en la intranet. Curso de DRP, Seguridad informática y continuidad de negocio. Son obligatorios y hace parte de la inducción de los nuevos.

¿Qué tan resiliente es la IPS ante la falla de los sistemas?

“Hoy en día ya se le hizo pruebas de alta disponibilidad a los sistemas de misión critica midiendo el RTO y RPO. Para el sistema de historias clínicas y telefonía se midieron los mismos indicadores RTO y RPO”[2]

¿Cómo logran medir esa resiliencia?

“Hacemos dos cosas para el negocio el año pasado hicimos pruebas de escritorio en plan de continuidad de negocio y en plan de continuidad tecnológica hacemos simulacros reales con datos reales, la pasamos de un datacenter x a uno y”

¿Tiene conocimiento de si han sufrido de algún ataque cibernético?

“NO, no tengo conocimiento”

Quiere decir que no se ha visto afectada la marca ni la reputación.

“NO se ha visto afectada”

¿Cuál es el ente de Gobierno Corporativo de mayor rango en la Institución?

“La junta directiva del grupo”

¿Participa alguien de su departamento en algunas de las reuniones de este ente?

“Del departamento no, nuestro CEO hace parte de la Junta”

¿Sabe si se trata el tema de ciber riesgos dentro de la agenda de las reuniones de la Junta y con qué regularidad lo hacen?

“SI, hay junta directiva mensualmente y mínimo una vez al año hay que presentar informe de ciber riesgos y aprobar el presupuesto de seguridad del próximo año. Son dos temas que mínimo al año

[2] No se mencionan los valores mencionados por confidencialidad.

deben tratarse en las juntas directivas por estatutos. El año pasado en una reunión se trataron los dos temas”

¿Cuál es el nivel de conocimiento sobre ciberseguridad en los miembros de la Junta?

“Ellos aprueban la política de seguridad informática de la IPS, aprueban los lineamientos generales y firman el apetito de riesgo”

¿Considera que debería contar la Junta con un experto en ciberseguridad entre sus miembros?

“NO, porque los expertos están en el backoffice que se tienen en la región y en la casa matriz”

Hemos terminado ¿Desea agregar algo más a la entrevista?

“Si, no somos el caso normal de las IPS en Colombia, acá debemos tener muy desarrollado el tema de la ciberseguridad, todavía hay cosas por trabajar en esta área, pero siento que para darle confianza a nuestros afiliados creemos que hacemos lo que hay que hacer para que por ese ítem no se corran riesgos para nuestros afiliados”

Bibliografía

AICPA. (Noviembre de 2018). *Cybersecurity Resource Center*. Obtenido de AICPA: https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/cyber-security-resource-center.html

Boyce, C., & Palena, N. (2006). *Conducting in-depth interviews: A guide for designing and conducting in-depth interviews for evaluation input.*

Congreso de La República de Colombia. (25 de Octubre de 2018). *Ley Estatutaria 1581 DE 2012.* Obtenido de Página Web Secretaria General del Senado: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Deloitte. (2018). *Ecosistema de ciberseguridad: Preparándonos para la defensa. Physical, Cyber or Human, where are weakest links?* Bogotá. Obtenido de https://www2.deloitte.com/content/dam/Deloitte/co/Documents/risk/PPt%20evento%20Colombia%20ago15_18%20para%20compartir.pdf

Deloitte. (2019). *Riesgo cibernético en la Transformación Digital y el rol de la Junta Directiva.*

Dinero. (11 de Octubre de 2016). *Las mejores IPS de Colombia en 2016*. Obtenido de Pagina Web de la Revista Dinero: https://www.dinero.com/edicion-impresa/informe-especial/articulo/las-mejores-ips-de-colombia-en-2016/238782

Dinero. (12 de Enero de 2019). *Colombia, el país con más secuestro de datos en América Latina, según reporte*. Obtenido de Revista Dinero: https://www.dinero.com/tecnologia/articulo/paises-con-mas-ataques-de-ransomware-en-america-latina/265958

EAFIT. (10 de Mayo de 2007). *Universidad EAFIT.* Obtenido de COBIT: Modelo para auditoría y control de sistemas de información:

http://www.eafit.edu.co/escuelas/administracion/consultorio-contable/Documents/boletines/auditoria-control/b13.pdf

El Telegrafo. (18 de Septiembre de 2019). *El cibercrimen mueve cerca de $3.5 trillones anualmente.* Obtenido de Periodico el Telegrafo: https://www.eltelegrafo.com.ec/noticias/judicial/12/cibercrimen-estafa-empresas-negocio-delitos-mercado-negro

ENISA. (2015). *Definition of Cybersecurity – Gaps and overlaps in standardisation.*

Ernst & Young - EY. (2017). *The evolving role of the board in cybersecurity risk oversight.*

EY. (2018). *Is cybersecurtity about more than protection? EY Global Information Securuty Survey 2018-19.*

Gemalto. (2018). *2018: Data Privacy and New Regulations Take Center Stage.* Obtenido de https://safenet.gemalto.com/resource/partnerasset.aspx?id=64424543953&langtype=1033

Georg, L. (2017). Information security governance: pending legal responsibilities of non-executive boards. *Journal of Management & Governance*, *21*(4), 793-814.

Granot, E., Brashear, T. G., & Motta, C. P. (2012). A structural guide to in-depth interviewing in business and industrial marketing research. Journal of Business & Industrial Marketing. *Journal of Business & Industrial Marketing*, *27*(7), 547-553.

Gubrium, J. F., Holstein, J. A., Marvasti, A. B., & McKineey, K. D. (2012). *The SAGE handbook of interview research: The complexity of the craft.* SAGE.

Haggard, S., & Lindsay, J. R. (2015). *North Korea and the Sony Hack: exporting instability through cyberspace.* East-West Center.

Haislip, J., Lim, J. H., & Pinsker, R. (2017). Do the Roles of the CEO and CFO Differ when it comes to Data Security Breaches?

Hutchinson, B. (9 de Abril de 2018). *87 million Facebook users to find out if their personal data was breached.* Obtenido de ABC NEWS: https://abcnews.go.com/US/87-million-facebook-users-find-personal-data-breached/story?id=54334187

IBM, & P. I. (2019). *Cost of a Data Breach Report 2019.*

IBM, & Ponemon Institue. (2018). *2018 Cost of a Data Breach Study: Global Overview.*

Identity Theft Resources Center. (2018). *2017 Annual Data Breach Year-End Review.* Obtenido de https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf

Islam, M., & Stafford, T. (2017). Information Technology (IT) Integration and Cybersecurity/Security: The Security Savviness of Board of Directors.

ISO. (Noviembre de 2018). *ISO/IEC 27000:2018.* Obtenido de International Organization for Standardization: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en

Kamiya, S., Kang, J. K., Milidonis, A., & Stulz, R. M. (2018). What is the impact of successful cyberattacks on target firms? *National Bureau of Economic Research.*

Matlay, H., & Sørheim, R. (2005). Business angels as facilitators for further finance: an exploratory study. *Journal of Small Business and Enterprise Development*, 178-191.

Moore, S., & Keen, E. (15 de Agosto de 2018). *Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019.* Obtenido de Gartner: https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019

Organization for Economic Co-operation and Development. (2004). *Directrices de la OCDE para la seguridad de sistemas y redes de información: Hacia una cultura de seguridad.* Obtenido de https://www.oecd.org/sti/ieconomy/34912912.pdf

Paganini, P. (19 de Enero de 2018). *Health South East RHF data breach exposed health records for half of Norway's Population.* Obtenido de Security Affair: https://securityaffairs.co/wordpress/67922/data-breach/health-south-east-rhf-databreach.html

Portafolio. (7 de Abril de 2019). *Colombianos ya podrán asegurarse contra delitos informáticos*. Obtenido de Portafolio.co: https://www.portafolio.co/economia/finanzas/colombianos-ya-podran-asegurarse-contra-delitos-informaticos-528293

PWC. (2018). *Fraude al descubrimiento. Encuesta Global Crimen Económico 2018.* Obtenido de https://www.pwc.com/co/es/assets/document/crimesurvey_2018.pdf

PWC. (2018). *Pulling fraud out of the shadows.* Obtenido de https://www.pwc.com/gx/en/forensics/global-economic-crime-and-fraud-survey-2018.pdf

Rothrock, R. A., Kaplan, J., & Van Der Oord, F. (2018). The Board's Role in Managing Cibersecurity Risk. *MIT Sloan Management Review, 59*(2), 12-15.

Rushe, D. (4 de Febrero de 2015). The Interview Revenge Hack Cost Sony Just $15m. *The Guardian*. Obtenido de https://www.theguardian.com/film/2015/feb/04/guardians-peace-revenge-hack-sony-finances-unscathed

Sharf, E. (2016). Information exchanges: regulatory changes to the cyber-security industry after Brexit: Making security awareness training work. *Computer Fraud and Security, 2016*(7), 9-12.

Superfinanciera. (2014). *Código País de Colombia, Código de Mejores Prácticas Corporativas.* Bogotá.

Supersalud. (s.f.). Obtenido de Sitio web de la Super Intendencia Nacional de Salud: https://docs.supersalud.gov.co/PortalWeb/Comunicaciones/MemoriasEventos/lineamiento-del-marco-de-supervision-basado-en-riesgos-de-la-SNS.pdf

Taylor, S. J., & Bogman, R. (2008). *La entrevista en profundidad. Métodos cuantitativos aplicados* (Vol. 2).

Toyota Boshoku. (6 de Septiembre de 2019). *Toyota Boshoku.* Obtenido de https://www.toyota-boshoku.com/global/content/wp-content/uploads/190906e.pdf

Trujillo Davila, M. A., Guzman Vasquez, A., & Prada Ramirez, F. J. (2015). *Juntas Directivas en el desarrollo del Gobierno Corporativo.* Bogotá: CESA.

von Solms, B., & von Solms, R. (2018). Cybersecurity and information security – what goes where? *Information & Computer Security*, *26*(1), 2-9.

World Economic Forum. (2018). *Global Risk Report 2018.* Obtenido de http://reports.weforum.org/global-risks-2018/global-risks-landscape-2018/#landscape/R_CYBERATTACKS//

World Economic Forum. (2019). *Global Risk Report 2019.* Obtenido de http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

Yin, R. K. (2014). *Case Study Research: Design and Methods.* Thousand Oaks: SAGE.