CIBER RESILIENCIA ORGANIZACIONAL

tictac
Powered by CCIT

CIBER
RESILIENCIA
ORGANIZACIONAL

Agradecemos el generoso apoyo de **Microsoft** para la realización de este estudio

Agradecemos la valiosa contribución de **Data & TIC**

ÍNDICE

4 INTRODUCCIÓN

8 CIBER RESILIENCIA ORGANIZACIONAL

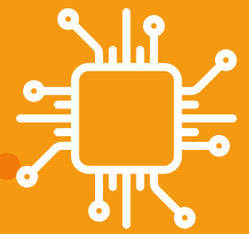
14 LINEAMIENTOS BÁSICOS DE SEGURIDAD

20 COMPUTACIÓN EN LA NUBE

26 RACIONALIZACIÓN DE INFORMES DE INCIDENTES

32 CONCLUSIONES

1



INTRODUCCIÓN

El creciente uso y dependencia de la tecnología por parte de organizaciones, la nube, el Internet de las Cosas, el *Big Data,* la alta conectividad, la Inteligencia Artificial y la premisa de que "no se trata si los eventos[1] ocurrirán, sino cuándo", demandan de las organizaciones la permanente necesidad de preparación, aprendizaje y reinvención, donde ser resiliente[2] e innovar, es el verdadero sello distintivo que se debe desarrollar para poder subsistir.

Una organización siempre se ve enfrentada a eventos que impactan en su funcionamiento. Estos eventos pueden ser internos o externos, y éstos, a su vez, legítimos e ilegítimos. Un evento externo ilegítimo es un ciberataque, un evento externo legítimo es un cambio en la normatividad. Un evento interno ilegítimo es un hecho doloso de un empleado, y un evento interno legítimo la reorganización de la estructura administrativa de una organización.

Todos los eventos enunciados y a los que se ven expuestas las organizaciones, son de gran importancia, pero dentro de éstos, y para los efectos de este documento, tienen particular importancia los ciberataques.

Con fundamento en lo anterior, y como elementos claves para desarrollar posturas de seguridad digital confiables y responder a las nuevas, dinámicas e imperativas necesidades digitales, se propone a las organizaciones centrarse en construir capacidades que les permitan seguir operando en los entornos digitales actuales, ofreciendo continuidad, confianza y valor, lo que se materializa en un esquema Ciber Resiliente[3] de la organización.

Para el diseño e implementación de un programa de Ciber Resiliencia, se propone, en el marco de la gestión de los riesgos cibernéticos, entre otras, las siguientes prácticas claves: (I) La computación en la nube[4], (II) Los lineamientos básicos de ciberseguridad[5] y, (III) La racionalización del reporte de incidentes[6]. La puesta en marcha de estas prácticas, a través de las recomendaciones planteadas en este documento, permitirá a las organizaciones alcanzar un estado de madurez ciber resiliente.

1. "Evento" se utiliza como una expresión neutral.
2. Se entiende "resiliencia" como la capacidad que tiene una organización para prepararse, adaptarse, continuar trabajando o recuperar su funcionamiento, cuando su normal operación ha sido alterada por un evento. Para mayor claridad, este concepto ha sido definido por NIST Special Publication (SP) 800-53 Revision 4 "Security and Privacy Controls for Federal Information Systems and Organizations, la Organización para la Cooperación y el Desarrollo Económico, OCDE, CONPES 3854, entre otros.
3. Capacidad de recuperación frente a las anomalías digitales, esto implica prepararse, responder y reaccionar como elementos esenciales de su fundamento.
4. Es un modelo que permite, de forma ubicua, conveniente, y por demanda, el acceso a un banco de recursos computacionales configurables (ej. Redes, servidores, aplicaciones, almacenamiento de datos, y servicios) que son provistos de forma rápida y con un mínimo esfuerzo administrativo o interacción con el proveedor. Traducción Libre del Departamento de Comercio de los Estados Unidos a través de su Instituto Nacional de Estándares y Tecnología (NIST, de ahora en adelante) en su publicación especial 800-145 "The NIST Definition of Cloud Computing", https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.
5. Instrumentos claves para definir posturas de seguridad, que puedan evolucionar, madurar y modelarse de acuerdo con las necesidades del negocio y de la organización.
6. Gestionar, de una parte, de manera útil, finalista y eficiente los incidentes de seguridad y su reporte, como pieza fundamental para la madurez y el aprendizaje de las organizaciones, atendiendo los marcos regulatorios; y de otra, ajustándose a las tendencias internacionales de construcción de confianza con las partes interesadas.

2

CIBER RESILIENCIA ORGANIZACIONAL

UN ENFOQUE INTEGRAL O UN ELEMENTO CLAVE DE LA CIBERSEGURIDAD

La resiliencia es la capacidad que tiene un sistema para prepararse, anticipar, adaptarse, continuar trabajando o recuperar su funcionamiento, cuando su normal operación ha sido alterada.

Existen varios tipos de condiciones que alteran el normal funcionamiento de una organización. Estas se dividen en afectaciones internas, que puede ser legítimas e ilegítimas; y afectaciones externas, que puede ser legítimas e ilegítimas.

La afectación externa e ilegítima, es un típico ataque cibernético. Una afectación externa legítima, es la expedición de una normatividad, que impone obligaciones a la organización.

La afectación interna e ilegítima, es una actuación desleal de un colaborador. Una afectación interna legítima, es la decisión de la organización de reestructurarse administrativamente.

Para cualquiera de los escenarios planteados, la organización debe ser resiliente para poder seguir operando con normalidad y esto se logra con la preparación y correcta implementación de elementos técnicos y administrativos.

Para resistir, absorber, recuperarse de la adversidad o un cambio en las condiciones, o adaptarse con éxito a ellas, las organizaciones deben desarrollar un programa de Ciber Resiliencia, que atienda principios[7], e integre componentes acordes con los desafíos a los que se enfrenta.

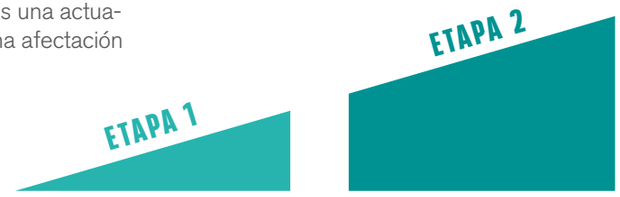


Figura 1. Modelo de madurez de la Ciber Resiliencia organizacional del World Economic Forum.

INCONSCIENTE

La organización considera que el riesgo cibernético es en gran parte irrelevante y no forma parte del proceso de gestión de riesgos de la organización. La organización no está al tanto de su nivel de interconexión.

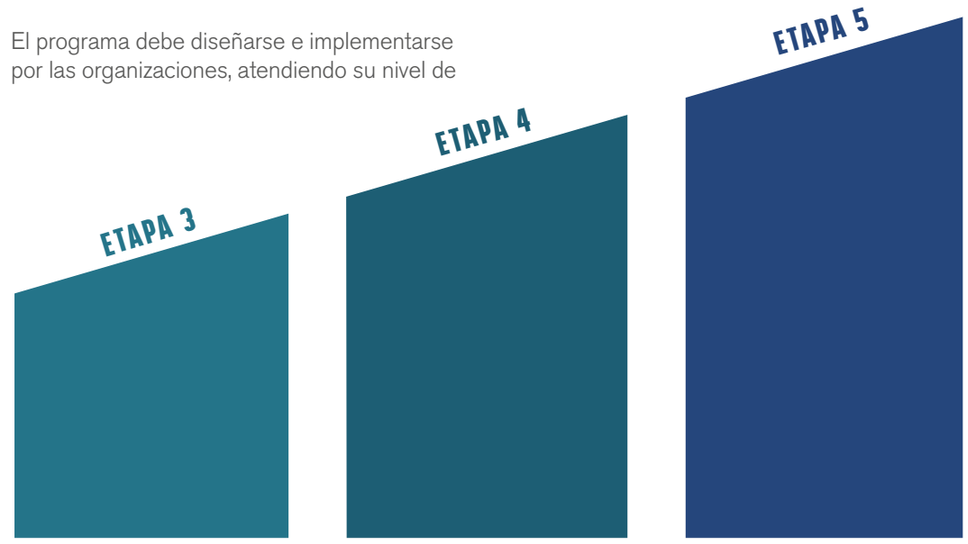
FRAGMENTADO

La organización reconoce la hiperconectividad como una fuente potencial de riesgo y tiene una visión limitada en sus prácticas de gestión de riesgos cibernéticos. La organización tiene un enfoque fragmentado del riesgo cibernético, con informes fragmentados e incidentales.

7. Partnering for Cyber Resilience. Risk and Responsibility in a Hyperconnected World - Principles and Guidelines, World Economic Forum, 2012.
8. Las organizaciones reconocen la naturaleza interdependiente de nuestro mundo hiperconectado y su propio papel para contribuir a un entorno digital compartido seguro.
9. El equipo de gestión ejecutiva de las organizaciones reconocen su papel de liderazgo y fomenta la conciencia en la gestión del riesgo cibernético.
10. La organización reconoce la importancia de integrar la gestión del riesgo cibernético dentro de sus prácticas de riesgo más amplias.
11. La organización alienta a sus proveedores y clientes a desarrollar y adoptar estos Principios y Directrices.
12. Para planear la preparación a largo plazo, una organización debe identificar activos, evaluar y administrar el riesgo de infraestructura, desarrollar capacidades para responder y recuperarse de interrupciones e invertir en investigación, educación y prácticas que contribuyan a los objetivos de Ciber Resiliencia a largo plazo.

El reconocimiento de la interdependencia[8], el rol de liderazgo[9], la gestión integrada del riesgo[10] y la promoción en la apropiación[11], son los principios que orientan la Ciber Resiliencia; y los componentes que la integran son: (I) La preparación[12], (II) La Respuesta[13] y (III) La Reinvención[14].

El programa debe diseñarse e implementarse por las organizaciones, atendiendo su nivel de madurez de Ciber Resiliencia, entendida éste como su habilidad para soportar eventos cibernéticos, medidos por la combinación del tiempo promedio hasta el fallo (MTTF[15]) y el tiempo promedio hasta la recuperación (MTTR[16]).



TOP DOWN

El CEO[17] ha establecido lineamientos para la gestión del riesgo cibernético, ha iniciado un programa de respuesta a riesgos y amenazas de arriba hacia abajo, pero no considera la gestión del riesgo cibernético como una ventaja competitiva.

GENERALIZADO

Los líderes de la organización se apropian completamente de la gestión del riesgo cibernético, desarrollan políticas y marcos, y definen responsabilidades y mecanismos de información. Comprenden las vulnerabilidades, controles e interdependencias de la organización con terceros.

CONECTADO

Las organizaciones están altamente conectadas con sus pares y socios, compartiendo información y mitigando conjuntamente el riesgo cibernético como parte de sus operaciones diarias. Su equipo muestra *ciberawareness* excepcional y la organización es un líder de la industria en la gestión del riesgo cibernético.

13. Al usar los planes y estrategias establecidos durante la fase de preparación, las organizaciones resilientes continúan funcionando durante una crisis y se recuperan rápidamente. Una respuesta flexible también es adaptable.
14. Aprender y mejorar los planes y estrategias existentes es un sello distintivo de la Ciber Resiliencia. Después de que ha pasado una crisis, el análisis es clave: identificar qué fue efectivo y dónde la respuesta fue problemática; desarrollando un plan de mejora.
15. MMTF, representa el tiempo medio de fallo, sin posibilidad de reparación
16. MTTR, representa el tiempo promedio necesario para volver a poner en funcionamiento un componente o sistema defectuoso.
17. Chief Executive Officer (o director ejecutivo)

2.1.
HACIA UN MODELO DE CIBER RESILIENCIA.
¿CUMPLIENDO LA NORMA O SIGUIENDO BUENAS PRÁCTICAS?

Desde una perspectiva internacional[18] e incluso nacional[19], se propone la ejecución de actividades y el diseño de programas de resiliencia como un propósito dirigido a encarar los retos que ofrecen las tecnologías emergentes y la hiperconectividad.

Con fundamento en lo anterior, resulta imperativo para las organizaciones públicas y privadas en Colombia, cualquiera que sea su tamaño, adoptar un programa de Ciber Resiliencia en el marco de la gestión de los riesgos cibernéticos en el cual se incluya el uso de herramientas tecnológicas que operativicen el programa.

2.2.
PROGRAMA DE CIBER RESILIENCIA

En el diseño e implementación del programa de gestión de riesgos cibernéticos, son relevantes los siguientes elementos, que variarán según la industria e incluso el tiempo:

A LA INTERDEPENDENCIA DE LAS ORGANIZACIONES.

B MEJORAR LAS PRÁCTICAS DE GESTIÓN DEL RIESGO CIBERNÉTICO.

C UN ENFOQUE BASADO EN EL RIESGO.

Por lo anterior, son cuatro los pilares que deben tenerse en cuenta para mejorar la gestión del riesgo y desarrollar un programa de Ciber Resiliencia:

1. PREPARAR.[20]

2. PROTEGER.[21]

3. DETECTAR.[22]

4. MEJORAR.[23]

La resiliencia trae consigo un desafío consistente en caracterizar y cuantificar con precisión las capacidades básicas necesarias que requiere la organización para asegurar la disponibilidad del servicio frente a los riesgos cibernéticos. Para garantizar la anticipación de los riesgos y la continuidad en la operación debe haber una práctica permanente dirigida a: (i) Identificar de manera constante las amenazas; (ii) Clasificar y priorizar los riesgos y la manera como se solventan; (iii) Establecer metas y objetivos en la actividad, (iv) Desarrollar resultados deseados y mantener el ciclo y (v) Definir roles dentro de la organización[24].

2.3.
LA TECNOLOGÍA COMO SOPORTE PARA EL DESARROLLO DE UN PROGRAMA DE CIBER RESILIENCIA

La combinación de diferentes tecnologías es indispensable en la creación de la Ciber Resiliencia. Para efectos de este documento, y reconociendo que existen prácticas claves necesarias para alcanzarla, se analizarán las más relevantes para desarrollar posturas de seguridad digital confiables: (i) Lineamientos Básicos de Ciberseguridad, (ii) Computación en la Nube y (iii) Racionalización de informes de incidentes.

18. Lineamientos OCDE, ISO 27103, ISO/IEC 27002:2013, y NIST Special Publication 800-53-
19. CONPES 3854, Ley 1581 de 2012, Circular Externa 007 de 2018 de la Superintendencia Financiera de Colombia
20. Consiste en (i) Comprender los activos críticos de la organización; (ii) Desarrollar las capacidades necesarias para abordar los diferentes niveles de riesgo; (iii) Establecer el nivel de riesgo dispuesto a aceptar; e (iv) Integrar la gestión del riesgo en toda la organización
21. Se orienta a (i) Asegurar la preparación cibernética bien fundamentada y repetible; (ii) Llevar a cabo evaluaciones de amenazas y control; (iii) Garantizar procesos apropiados de debida diligencia y verificación para terceros; (iv) Habilitar y potenciar la gestión de incidentes y capacidades de respuesta; (v) Desarrollar e implementar un plan de respuesta a incidentes; (vi) Fomentar la educación continua y formación.
22. Consiste en desarrollar capacidades de detección y monitoreo continuo para abordar anomalías y amenazas a los activos de la organización.
23. Busca crear una base de datos completa de incidentes de seguridad que soportan aprendizaje continuo y finalmente permitir la recuperación de un evento en un tiempo más corto
24. Los cinco pasos se describen de manera general en "Threat and Hazard Identification and Risk Assessment Guide", Federal Emergency Management Agency, US Department of Homeland Security, August 2013, Washington, DC. www.fema.gov/media-library-data/8ca0a9e54d-c8b037a55b402b2a269e94/CPG201_htirag_2nd_edition.pdf

3

LINEAMIENTOS BÁSICOS DE SEGURIDAD

Los lineamientos básicos de ciberseguridad son un conjunto de políticas, resultados, actividades, prácticas y controles, destinados a ayudar a gestionar el riesgo de seguridad digital.

3.1.

HACIA UN MODELO DE LINEAMIENTOS BÁSICOS DE CIBERSEGURIDAD.

¿SE DEBE PROMOVER SU DESARROLLO REGULATORIO O ADOPTAR LAS BUENAS PRÁCTICAS INTERNACIONALES?

Algunos ejemplos de Lineamientos Básicos de Ciberseguridad a nivel internacional son la Guía de controles ISO/IEC 27002; Center For Internet Security, CIS; Guías de controles del National Institute of Standards and Technology, NIST; Guía de controles críticos de seguridad de Sans Institute.

En Colombia, aunque no existe un desarrollo como el expuesto, se puede hacer referencia a una serie de políticas y normas que incorporan lo que podría ser una etapa inicial a los Lineamientos Básicos de Ciberseguridad, como el CONPES 3701[25]; el CONPES 3854[26]; el Manual para la implementación de la estrategia de Gobierno en Línea en las entidades del orden nacional de la República de Colombia de 2015[27], el Manual para la implementación de la estrategia de Gobierno Digital en las entidades del orden nacional de la República de Colombia de 2018[28], la Circular Externa 007 de 2018[29] y la Circular Externa 005 de 2019[30], ambas de la Superintendencia Financiera de Colombia.

Independientemente del enfoque -basado en resultados o controles-, los lineamientos básicos de ciberseguridad de sectores cruzados generarán un comportamiento positivo más allá de las organizaciones directamente afectadas por los enfoques regulatorios o voluntarios, incentivando a los proveedores intermedios de gobiernos u organizaciones de infraestructura crítica a implementar actividades base relevantes.

25. Lineamientos de Política Nacional para Ciberseguridad y Ciberdefensa. "busca generar lineamientos de política en ciberseguridad y ciberdefensa orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país"
26. Política Nacional de Seguridad Digital. Si bien no hace referencia explícita al concepto de Lineamientos Básicos de Ciberseguridad, expresa que el marco jurídico colombiano no contempla aspectos necesarios para facilitar la protección y defensa de las infraestructuras cibernéticas nacionales , por lo cual es "indispensable generar una estrategia de protección de la infraestructura crítica cibernética en el país (…) bajo un enfoque de gestión de riesgos de seguridad digital"; estructurando objetivos generales y específicos que se materializan en Lineamientos Básicos de Ciberseguridad.
27. Reconoce que, en atención a los avances y los nuevos retos producto de la evolución misma de la sociedad en temas como la seguridad, debe iniciarse un proceso de evolución hacia un nuevo modelo que permita el aumento del número y uso de servicios en línea, el mejoramiento de la calidad y servicio de los mismos, el acceso a mayor información y datos a través del uso eficiente de las TIC; al tiempo que deben observarse de manera permanente condiciones de seguridad. Es así que, como componente del Modelo de Gobierno en Línea, se incluye la descripción de actividades orientadas a que cada entidad cuente con una política de seguridad de la información que debe ser mejorada constantemente.
28. Este manual determina la ruta de acción que deben seguir las entidades públicas para desarrollar la política de gobierno digital, estructurado en cuatro actividades: el conocimiento; la planeación; implementación, y la medición de la política, incorporando acciones que permitan su adopción. Asimismo, indica que "las entidades públicas incorporen la seguridad de la información (…) con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos. Este habilitador se desarrolla a través del Modelo de Seguridad y Privacidad de la Información, que orienta la gestión e implementación de la seguridad de la información en el Estado".
29. A través de esta circular se adicionó el Capítulo V "Requerimientos mínimos para la gestión del riesgo de ciberseguridad" al Título IV de la Parte I de la Circular Básica Jurídica (C.E. 029 de 2014).

3.2.

PROGRAMA QUE COMPRENDA LINEAMIENTOS BÁSICOS DE CIBERSEGURIDAD

Los lineamientos básicos de ciberseguridad se pueden estructurar e implementar de diferentes maneras, según el frente de trabajo. Es así como se tratará de un enfoque centrado en resultados o en controles, como se describe a continuación:

FUENTES DE TRABAJO	ENFOQUE BASADO EN RESULTADOS	ENFOQUE BASADO EN CONTROLES
AUDIENCIAS	Grupos de interés (IT, Seguridad, Gerentes y Directivos).	IT y Grupos de Seguridad.
ORIENTACIÓN	El enfoque estratégico para la gestión del riesgo establece una "base" y procesos para la mejora continua. Permiten el crecimiento.	El enfoque centrado en el cumplimiento establece un "techo" sobre lo que debe hacerse para la seguridad. Crean la mentalidad de un punto a alcanzar y con ello una meta.
IMPLEMENTACIÓN	Describe el "qué" debe hacer una organización para mejorar la seguridad.	Describe "el cómo" una organización debería implementar prácticas de seguridad.
AUDIENCIAS	Centrarse en los resultados en lugar de en las técnicas de implementación permite la adaptabilidad y personalización a las organizaciones.	Un enfoque centrado en la implementación restringe la personalización y se ciñe a lo dicho en el marco usado.

Este capítulo agregado a la Circular Básica Jurídica establece que, en todo caso, las entidades que no están obligadas a acoger las instrucciones impartidas en dicho documento deben hacer periódicamente una autoevaluación del riesgo de ciberseguridad y seguridad de la información, que incluya una identificación de las mejoras a implementar en su Sistema de Administración de Riesgo Operativo.
Asimismo, establece que las entidades deben contar con políticas, procedimientos y recursos técnicos y humanos necesarios para gestionar efectivamente el riesgo de ciberseguridad y se sugiere, entre otros, "establecer principios y lineamientos para promover una cultura de ciberseguridad que incluya actividades de difusión, capacitación y concientización tanto al interior de la entidad como frente a usuarios y terceros que esta considere relevantes dentro de la política de ciberseguridad" precisando que estas actividades deben realizarse periódicamente y pueden incluirse, en los cursos sobre riesgo operativo que realice la entidad.
30. "La Circular 005 de 2019 de la Superintendencia Financiera de Colombia, manifiesta que las entidades sometidas a la inspección y vigilancia pueden soportar todos sus procesos y actividades en servicios computacionales en la nube. Indica que cuando se trate de la operación de sus procesos misionales o de gestión contable y financiera, además de cumplir las instrucciones y obligaciones que en la misma Circular se describen, se debe remitir a la Superfinanciera información relacionada con el nombre del proveedor, la relación de procesos que serán manejados por la nube, ubicación física donde se procesarán y almacenarán los datos, entre otros. Del mismo modo, señala que (i) Los acuerdos o contratos que se suscriban para la prestación de servicios de computación en la nube deben contemplar condiciones y elementos mínimos; (ii) Se debe disponer de un plan de continuidad de negocio y estrategia de migración; y (iii) Mantener actualizada y a disposición de la Superfinanciera información relacionada con los procesos y procedimientos que se ejecutan en la nube, de las aplicaciones que operan en la nube, entre otros."

Tanto sector público como privado pueden aprovechar lo mejor de ambos enfoques en el desarrollo o la evolución de lineamientos básicos de ciberseguridad. Para hacerlo, es necesario pensar en la orientación en resultados como elemento base, y usar el enfoque de controles cuando sea necesario. Es así como los lineamientos básicos de ciberseguridad eficaces tienden a adoptar, entre otras, las siguientes mejores prácticas con un enfoque de resultados:

1.
APROVECHAR LA MULTIDISCIPLINARIEDAD, CONOCIMIENTOS, EXPERTICIA Y EXPERIENCIA MEDIANTE LA UTILIZACIÓN DE UN PROCESO DE DESARROLLO DE POLÍTICAS.

2.
APOYAR EL CRECIMIENTO ECONÓMICO.

3.
TOMAR DECISIONES DE MANERA ÁGIL E INFORMADA, AL UNIR LA COMPRENSIÓN DE LA GESTIÓN DE RIESGOS TANTO DENTRO COMO ENTRE LAS ORGANIZACIONES.

4.
ADMINISTRAR LOS RIESGOS, A TRAVÉS DE UN CONJUNTO DE PRÁCTICAS DE REFERENCIA PRIORITARIAS Y BASADAS EN EL RIESGO.

5.
PERMITIR LA INNOVACIÓN, DIRIGIÉNDOSE HACIA LOS RESULTADOS DE SEGURIDAD DESEADOS EN LUGAR DE UN MERO CUMPLIMIENTO NORMATIVO.

6.
AVANZAR, APROVECHANDO LAS BUENAS PRÁCTICAS.

4

COMPUTACIÓN EN LA NUBE

"La computación en la nube es la tecnología que permite gestionar servicios informáticos de manera remota, de tal forma que cualquier servicio o procesamiento de datos, que antes se realizaba localmente, puede ejecutarse a través de la red de Internet, tal como el uso de aplicaciones, almacenamiento, gestión de datos, entre otros, haciendo un uso eficiente y económico de recursos al compartir hardware y software como plataformas, licencias, capacidad de almacenamiento y servicios con muchos usuarios, con un alto nivel de disponibilidad, flexibles y por demanda; características que reducen tiempos de acceso y costos, pero se debe incrementar la seguridad en las operaciones, especialmente en la de tipo público, donde la infraestructura y demás recursos son compartidos públicamente en internet"[31].

En relación con los tipos o modelos de servicio de computación en la nube, se pueden mencionar tres grandes categorías: Infraestructura como servicio (IaaS)[32], Plataforma como servicio (PaaS)[33] y Software como servicio (SaaS)[34].

Finalmente, entre los tipos de implementación de la computación en la nube, podemos advertir las nubes públicas[35], nubes privadas[36], e híbridas[37] y comunitaria[38].

31. Guía de Protección de Datos Personales en los Servicios de Computación en la Nube (Cloud Computing) de la Superintendencia de Industria y Comercio, SIC. Para mayor referencia consultar: Gartner, Publicación Especial 800-145 del 2011 y numeral 2.3 de la Circular 005 de 2019 de la Superintendencia Financiera de Colombia, entre otros

32. Modelo de servicio en el cual el proveedor de servicios de computación en la nube pone a disposición de una entidad la infraestructura que le permite ejecutar software de cualquier tipo, con el propósito de obtener la capacidad de procesamiento informático o de almacenamiento de información mediante servicios estandarizados." Subnumeral 2.3.3. de la Circular 005 de 2019..

33. Modelo de servicio en el cual el proveedor de servicios de computación en la nube pone a disposición de una entidad las plataformas en las cuales desarrollan y prueban distintas aplicaciones, mediante el uso de lenguajes y herramientas de programación que son gestionadas por el prestador de servicios. La entidad no administra ni controla la infraestructura del proveedor. Subnumeral 2.3.2. de la Circular 005 de 2019.

34. "Modelo de servicio en el cual el proveedor de servicios de computación en la nube pone a disposición de una entidad las aplicaciones que corren en la infraestructura de éste, bajo demanda y que pueden ser utilizadas de forma compartida con otros usuarios. La entidad no administra ni controla la infraestructura del proveedor." Subnumeral 2.3.1. de la Circular 005 de 2019.

35. Las nubes públicas son propiedad de un proveedor de servicios en la nube y son operados por este, el cual entrega sus recursos informáticos, como servidores y almacenamiento, a través de Internet. Con una nube pública todo el hardware, software y otra infraestructura de soporte es propiedad y está administrado por el proveedor de la nube. Se accede a estos servicios y administra la cuenta usando un navegador web.

36. Una nube privada se refiere a los recursos de computación en la nube utilizados exclusivamente por una sola empresa u organización. Se puede ubicar físicamente en el centro de datos de la empresa en el sitio. Algunas compañías también pagan a proveedores de servicios de terceros para alojar su nube privada. Una nube privada es aquella en la que los servicios y la infraestructura se mantienen en una red privada.

37. Las nubes híbridas combinan nubes públicas y privadas, unidas por una tecnología que permite compartir datos y aplicaciones entre ellos. Al permitir que los datos y las aplicaciones se muevan entre nubes privadas y públicas, la nube híbrida brinda a las empresas una mayor flexibilidad y más opciones de implementación

38. Servicios disponibles para el uso exclusivo de una comunidad específica de organizaciones que tienen objetivos similares. Subnumeral 2.4.3. de la Circular 005 de 2019

4.1.

HACIA UN MODELO DE SEGURIDAD EN LA COMPUTACIÓN EN LA NUBE.

LA NUBE NO DEBE SER UNA OPCIÓN; SU USO DEBE SER IMPERATIVO.

Como parte de los esfuerzos a nivel internacional[39] algunos marcos de referencia en materia de seguridad en la nube, definen lineamientos para la adopción e implementación de servicios y tecnologías basados en la computación en la nube. Hasta la expedición de la Circular 005 de 2019[40] en Colombia[41] solo existían referencias a las mejores prácticas desarrolladas a nivel internacional.

Sobre este aspecto es preciso advertir que en Colombia la computación en la nube tiene un uso en el sector industrial del 54,7% respecto de otras tecnologías[42], de forma tal que surge como una herramienta para hacer frente a los desafíos en el uso del Big Data[43], con lo cual es posible afirmar que en Colombia toma mayor relevancia la condición de seguridad de la nube.

39. Cloud Security Alliance (CSA Security Guidance for Critical Areas of Focus in Cloud Computing v4.0), NIST Cloud Computing Related Publications (https://www.nist.gov/itl/nist-cloud-computing-related-publications; Security Framework For Governmental Clouds, ENISA, (https://www.enisa.europa.eu/publications/security-framework-for-governmental-clouds/at_download/fullReport); ISO/IEC 27017 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services (http://www.iso27001security.com/html/27017.html) ; ISO 27018. Code of Practice for Protecting Personal Data in the Cloud (https://www.iso.org/standard/61498.html)

40. La Circular 005 de 2019, de manera expresa manifiesta que las entidades sometidas a la inspección y vigilancia de la Superintendencia Financiera de Colombia pueden soportar todos sus procesos y actividades en servicios computacionales en la nube. Asimismo, indica que cuando se trate de la operación de sus procesos misionales o de gestión contable y financiera se deben cumplir las instrucciones que en la misma Circular se describen, tal como verificar una disponibilidad de al menos el 99,95%, establecer mecanismos que permitan contar con respaldo de la información que se procesa en la nube, garantizar la independencia de información, disponer de un plan de continuidad y estrategias de migración, entre otros aspectos.

41. CONPES 3854 "Política Nacional de Seguridad Digital"; CONPES 3920 "Política Nacional de Explotación de Datos BIG DATA"; Ley Estatutaria 1581 de 2012, que si bien no hace referencia a la nube, la ley desarrolla el concepto Seguridad, como un principio rector para el tratamiento de datos personales y como un deber de los responsables y encargados del tratamiento, dando lugar a la cartilla "Protección en los servicios de computación en la nube (CLOUD COMPUTING)"que entre otros aspectos, hace referencia a la seguridad como una de las principales consideraciones a tener en cuenta en la contratación del servicio de cómputo en la nube; señalando que la seguridad debe incrementarse en las operaciones que se desarrollen en la nube; Circular Externa 029 de la Superintendencia Financiera de Colombia, Si bien la Superintendencia Financiera no ha impartido instrucciones particulares a las entidades objeto de vigilancia sobre el uso de "cloud computing a nivel Bancos"; si ha impartido a sus vigiladas instrucciones de obligatorio cumplimiento en materia de seguridad y calidad de la información , normas de control interno para la gestión de la tecnología , así como las reglas relativas a la administración del riesgo operativo SARO, las cuales tienen plena aplicación frente a los servicios de computación en la nube implementados por las entidades vigiladas.

42. Documento CONPES 3920 "Política Nacional de Explotación de Datos BIG DATA)". Gráfico 20. Uso de tecnologías en el sector industrial, página 69.

43. "Big data needs on-demand high performance data processing and distributed storage as well as variety of tools required to accomplish activities of the big data ecosystem which are described in clause 6.2. Cloud computing meets the challenges of big data as described in clause 6.1. The burst nature of workloads makes cloud computing more appropriate for big data challenges such as scalability and timeliness. The big data ecosystems, which are supported by a cloud computing system context, can be referred to as cloud computing based big data". Big data – Cloud computing based requirements and capabilities, TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU, Y.3600

4.2.
PROGRAMA DE SEGURIDAD EN LA COMPUTACIÓN EN LA NUBE

La Seguridad, como elemento transversal en la computación en la nube, comprende desde la seguridad física hasta la seguridad digital constituyéndose en un factor de competitividad, confianza y resiliencia de las organizaciones que hacen uso de la computación en la nube.

La confianza de la computación en la nube[44] está centrada en las siguientes condiciones claves: (i) Seguridad, (ii) Control y privacidad, (iii) Cumplimiento de estándares y (iv) Transparencia.

Dada la pluralidad y singularidad de las organizaciones, no existe una solución única de nube, por lo que debe explorarse si se usa un modelo de inmersión completa en la nube o un modelo híbrido.

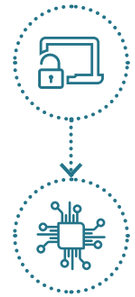
Un programa de seguridad en la nube debe tener en cuenta, entre otros, los siguientes aspectos:

1.
EL ACCESO FÍSICO A LOS DATOS, TODA VEZ QUE LA NUBE REQUIERE UNA UBICACIÓN E INFRAESTRUCTURA FÍSICA.

2.
UNA MEJOR COMPRENSIÓN DEL ENTORNO DE AMENAZAS, PARA DETERMINAR EL TIPO Y SEGURIDAD DE LA NUBE, DADO QUE LA NUBE, A TRAVÉS DE SU ENTORNO DIGITAL, OFRECE EN MATERIA DE SEGURIDAD UN ESPECTRO MÁS AMPLIO QUE LOS LÍMITES FÍSICOS DE LA INFRAESTRUCTURA LOCAL.

3.
LA INTELIGENCIA Y NUEVAS TECNOLOGÍAS -BIG DATA, MACHINE LEARNING, IOT- PARA ANTICIPAR AMENAZAS DIGITALES.

4.
LA NUBE COMO UNA HERRAMIENTA DE RESILIENCIA, YA QUE AUMENTA LA SEGURIDAD, LA CAPACIDAD DE RECUPERACIÓN Y EL EVENTUAL DESBORDAMIENTO DE UN ATAQUE - DDOS -.



5.
LA PRIVACIDAD E INNOVACIÓN COMO ASPECTOS DIFERENCIALES.

6.
LA TERCERIZACIÓN, QUE CON OCASIÓN DE LA PROFESIONALIDAD PERMITE NO SOLO ADMINISTRAR LA SEGURIDAD, SINO TAMBIÉN LOS CONTROLES DE RED, DE IDENTIDAD Y ACCESO, CON LAS MEJORES PRÁCTICAS Y DEDICACIÓN DE RECURSOS TECNOLÓGICOS Y HUMANOS MÁS ALLÁ DE LOS ESTÁNDARES.

Además de cumplir lo dispuesto en la Circular 005 de 2019 de la Superintendencia Financiera de Colombia, como buenas prácticas que deben adoptar los Programas de Seguridad en la Computación en la Nube se propone:

1.
ALINEACIÓN, ENTRE EL PERSONAL DE TI Y SEGURIDAD EN LA ORGANIZACIÓN.

2.
LA AUTENTICACIÓN DE USUARIO Y CIFRADO DE INFORMACIÓN CLASIFICADA COMO CONFIDENCIAL EN TRÁNSITO O EN REPOSO, USANDO ESTÁNDARES Y ALGORITMOS RECONOCIDOS INTERNACIONALMENTE.

3.
RACIONALIZACIÓN DEL PORTAFOLIO DE HERRAMIENTAS DE SEGURIDAD.

4.
UNA VISIÓN HOLÍSTICA O SISTÉMICA DE TODO EL ECOSISTEMA DIGITAL.

44. https://www.ulb.ac.be/dinfo/office365/docs/About-Microsoft-Cloud-Security.pdf

5

RACIONALIZACIÓN DE INFORMES DE INCIDENTES

5.1.
HACIA UN MODELO DE RACIONALIZACIÓN DE INFORMES DE INCIDENTES.

Un Incidente de Seguridad se define como la vulneración o inminente amenaza a la infraestructura a una organización. Puede entonces, tratarse de un acceso o intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información, la imposibilidad de operar normalmente las redes, sistemas o recursos informáticos.

El incidente se da de forma inesperada, poniendo en riesgo toda o parte de la información. Es por ello que es preciso contar con medidas técnicas, humanas y administrativas necesarias, con el fin de mitigar los riesgos de su ocurrencia, conforme al principio de seguridad y dentro de un esquema de resiliencia de la organización. Asimismo, es preciso indicar que aunque genéricamente se haga referencia a "incidente", por la connotación de su alcance y definición, se sugiere referirse a "brecha".

Internacionalmente[45] son varios los documentos que desarrollan y establecen las diferentes etapas y acciones de los incidentes o brechas de seguridad[46].

En Colombia[47], además del CONPES 3701 y CONPES 3854, hacen referencia expresa al informe de incidentes, la Guía para la Gestión y Clasificación de Incidentes de Seguridad del MinTIC[48], la Circular 003 de 2018 de la SIC[49] y la Circular Externa 007 de 2018 de la Superfinanciera[50] y la Circular Externa 005 de 2019 de la Superfinanciera[51].

45. ISO 27001; ISO 27002; Reglamento General de Protección de datos -RGPD- o GDPR
46. https://www.aepd.es/media/guias/guia-brechas-seguridad.pdf
47. Con el fin de abordar las incertidumbres, los riesgos, las amenazas, las vulnerabilidades y los incidentes digitales, en el 2011, el Gobierno Nacional expidió el documento CONPES 3701 Lineamientos de política para ciberseguridad y ciberdefensa. Asimismo, El documento CONPES 3854 del 11 de abril del 2016 "Política Nacional de Seguridad Digital", además de definir incidente digital, manifiesta que la creciente relevancia del entorno digital ha traído consigo un conjunto de incertidumbres, vulnerabilidades e incidentes de seguridad de diferentes tipos, frente a lo cual el gobierno colombiano estableció lineamientos de política para ciberseguridad y ciberdefensa
48. El Ministerio de la Tecnologías de la Información, propone lineamientos en la materia a las Entidades públicas de orden nacional y entidades públicas del orden territorial, así como proveedores de servicios de Gobierno en Línea, y terceros que deseen adoptar el Modelo de Seguridad y Privacidad de TI en el marco de la Estrategia de Gobierno en Línea.
49. Determina la obligación de informar los eventos que pueden tratarse como incidentes de seguridad y cuando deben ser reportados a la autoridad de protección de datos personales, entre otros aspectos.
50. Establece que los eventos que afecten de manera significativa la confidencialidad, integridad o disponibilidad de la información manejada en los sistemas que soportan los canales de atención al cliente de las entidades vigiladas por la Superintendencia Financiera de Colombia, deben informarse a esa Superintendencia haciendo una breve descripción del incidente y su impacto, tan pronto se presenten.
51. Establece que los acuerdos o contratos que se suscriban para la prestación de servicios de computación en la nube deben contemplar, entre otros, la resolución de incidentes y horarios de atención del proveedor del servicio.

5.2.
PROGRAMA DE RACIONALIZACIÓN DE INFORMES DE INCIDENTES

Antes de definir la racionalidad en los informes de incidentes, es preciso advertir que todas las organizaciones, deben contar con un modelo de gestión de incidentes donde se incluya la preparación, detección-evaluación-análisis y la contención-detección-recuperación de la organización frente a un incidente. Así mismo, la organización debe contar con una política de incidentes y una política de comunicación de los incidentes de seguridad.

Sobre **el momento de reportar,** la Guía del MinTIC propone que debe hacerse cuando haya sospecha de materialización del incidente, mientras que la Superintendencia de Industria y Comercio[52] y la Superintendencia Financiera de Colombia[53] establecen términos y condiciones sobre el cómo y cuándo debe hacerse el reporte. Por otra parte, en Europa, el RGPD[54] indica que el reporte debe notificarse a la autoridad de control competente, sin dilación y a más tardar en las 72 horas siguientes.

Otro punto importante a determinar **es a quién debe dirigirse el reporte,** toda vez que las diferentes entidades tienen alcance y capacidad jurídica diferente, por lo que no puede establecerse un reporte "universal" o "fits all".

Aunado a lo anterior, no hay claridad respecto de la **finalidad** de los reportes requeridos; por lo cual resultaría preciso que las autoridades establecieran la "finalidad" que se busca con el reporte, con el fin de alcanzar mejores efectos.

52. La Circular Externa 003 de 2018 establece, tanto para los obligados como para los no obligados a realizar el reporte ante el RNBD, que cuando ocurra un incidente que: "…afecte la información contenida…", deben reportarlo dentro de los quince (15) días hábiles siguientes al momento en que: (i) Se detecten los incidentes y (ii) sean puestos los incidentes en conocimiento de la persona y área encargada de atenderlos.
53. La Superintendencia Financiera de Colombia, en la Circular Externa 008 de 2018, establece que las entidades vigiladas deben informar a la Superintendencia "los eventos que afecten de manera significativa la confidencialidad, integridad o disponibilidad de la información manejada en los sistemas que soportan los canales de atención al cliente, haciendo una breve descripción del incidente y su impacto. Los incidentes se deben reportar tan pronto se presenten". (Subraya fuera del texto).
Por su parte, el numeral 3.7 del Anexo de la Circular Externa 007 de 2018 establece que las entidades deben contar con políticas, procedimientos y recursos técnicos y humanos necesarios para gestionar efectivamente el riesgo de ciberseguridad.
54. El RGPD indica que el reporte deberá hacerse tan pronto se tenga conocimiento que se ha producido una brecha de la seguridad de los datos personales, y además se debe efectuar la correspondiente notificación a la autoridad de control competente, sin dilación. https://www.boe.es/doue/2016/119/L00001-00088.pdf. Página 17 (85).

Sobre la **obligatoriedad** de reportar los incidentes, la Circular 003 de 2018 de la SIC hace obligatorio el reporte cuando haya datos personales involucrados, aunado a la exigibilidad de lo dispuesto en la Circular 007 de la Superfinanciera. Con fundamento en lo anterior se puede afirmar que en Colombia, en la práctica, es obligatorio reportar todos los incidentes, toda vez que en general los incidentes afectan datos personales.

Frente al anterior escenario de la obligatoriedad, y habiendo determinado la entidad ante la cual se va a reportar el incidente; el reporte debe atender: (i) La capacidad jurídica de la entidad, (ii) Al tipo de incidente que requiere la entidad sea reportado, (iii) La finalidad que se persigue con el reporte, y (iv) Exigir que el reporte sea confidencial, en la medida que el propósito a perseguir debe ser el fortalecimiento del sistema y no la "sanción por la sanción".

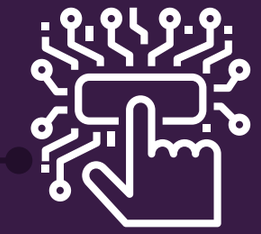
Con lo anterior se pretende buscar un equilibrio y un debido proceso entre los administradores y los administrados, donde los primeros persigan fines últimos y generales, y los segundos la continuidad de sus negocios, en un entorno cada vez más seguro con el concurso de las diferentes organizaciones.

5.3.
LA TECNOLOGÍA COMO SOPORTE PARA EL CUMPLIMIENTO DE LA OBLIGACIÓN DE REPORTAR INCIDENTES.

Para el reporte de incidentes, las organizaciones deben contar con herramientas que permitan hacer una adecuada gestión de datos, su identificación, clasificación, ubicación y el establecimiento del volumen de los mismos. El reporte debe poderse hacer de una manera expedita y soportada en los informes de los incidentes.

En la actualidad existen productos y servicios, que suplen en buena medida las necesidades derivadas de la gestión de datos y el levantamiento de los informes.

6



CONCLUSIONES

1.
DESARROLLAR UN PROGRAMA DE RESILIENCIA NO ES UNA OPCIÓN, ES UNA OBLIGACIÓN LEGAL Y UNA PRIORIDAD ORGANIZACIONAL.

2.
LA RESILIENCIA. UN CONCEPTO PARA IMPLEMENTAR "A LA MEDIDA".

3.
CONTAR CON HERRAMIENTAS TECNOLÓGICAS PARA SER RESILIENTE PERMITE SOPORTAR PROGRAMAS Y PLANES DE ACCIÓN.

4.
LINEAMIENTOS BÁSICOS DE CIBERSEGURIDAD. ESTÁNDARES QUE GENERAN RESILIENCIA COLECTIVA.

5.
LA REGULACIÓN PERMITE LA ADOPCIÓN DE LA NUBE[55].

6.
LA NUBE, PERMITE SER MÁS RESILIENTE.

7.
LA NUBE COMO INSTRUMENTO PARA POTENCIAR LAS CAPACIDADES ORGANIZACIONALES, PUEDE CONSIDERARSE UN LINEAMIENTO BÁSICO DE CIBERSEGURIDAD.

8.
LA SEGURIDAD EN LA NUBE. UN CRITERIO FUNDAMENTAL PARA SU ADOPCIÓN.

9.
LA NUBE UNA HERRAMIENTA DE LA RESILIENCIA.

10.
REPORTE DE INCIDENTES DE SEGURIDAD SÍ, PERO BAJO UN CRITERIO DE RACIONALIZACIÓN.

55. http://download.microsoft.com/documents/australia/cloud/keynote/gartner_cloud_keynote.pdf

.Puntoaparte
bookvertising

Dirección editorial
Andrés Barragán

Dirección de arte
Mateo L. Zúñiga
David Vargas

Diseño y diagramación
Jerson Siabatto