



CÁMARA DE BANCOS  
E INSTITUCIONES FINANCIERAS  
DE COSTA RICA

# MODELO DE MADUREZ DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACION

Aprobado por el Foro Interbancario de Seguridad de la Información el 08 de marzo del 2017

Aprobado por la Junta Directiva en sesión del 22 de marzo del 2017

# ÍNDICE

INTRODUCCIÓN.....	3
OBJETIVO.....	4
DESCRIPCIÓN GENERAL.....	4
FACTOR 1. RESPONSABILIDAD E INVOLUCRAMIENTO.....	7
FACTOR 2. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.....	9
FACTOR 3. ORGANIZACIÓN DE LA SEGURIDAD.....	10
FACTOR 4. INVERSIÓN EN SEGURIDAD.....	12
FACTOR 5. REPORTES DE SEGURIDAD.....	13
FACTOR 6. CONOCIMIENTO DEL PERSONAL DE GESTIÓN DE SEGURIDAD.....	14
FACTOR 7. CAPACITACIÓN Y CONCIENCIACIÓN A USUARIOS.....	16
FACTOR 8. CUMPLIMIENTO LEGAL Y REGULATORIO.....	17
FACTOR 9. VALORACIÓN DE RIESGO.....	19
FACTOR 10. GESTIÓN DE LA INFORMACIÓN.....	21
FACTOR 11. SEGURIDAD EN PROYECTOS.....	22
FACTOR 12. DISEÑO DE SEGURIDAD DE RED.....	23
FACTOR 13. CONTROL DE LA PLATAFORMA Y CONTROL DE CAMBIOS.....	25
FACTOR 14. ANÁLISIS DE VULNERABILIDADES Y PRUEBAS DE PENETRACIÓN.....	27
FACTOR 15. SISTEMA DE REGISTRO, MONITOREO Y ALARMA DE EVENTOS.....	28
FACTOR 16. CONTROL ACCESO LÓGICO (AUTENTICACIÓN).....	29
FACTOR 17. ADMINISTRACION DE IDENTIDAD.....	30
FACTOR 18. CONTROLES EN EL DESARROLLO DE APLICACIONES Y APPS.....	32
FACTOR 19. ADMINISTRACIÓN DE DISPOSITIVOS DE SEGURIDAD DE LA RED.....	33
FACTOR 20. CONTROL DE MALWARE.....	35
FACTOR 21. SEGURIDAD DE USUARIO FINAL.....	37
FACTOR 22. CONTINUIDAD.....	39
FACTOR 23. ATENCIÓN DE INCIDENTES DE SEGURIDAD.....	40
FACTOR 24. MONITOREO DE INDICADORES DE SEGURIDAD.....	41
FACTOR 25. SEGURIDAD FÍSICA.....	42
FACTOR 26. TERCERIZACIÓN DE SERVICIOS (NUBE).....	44
FACTOR 27. SEGURIDAD MÓVIL.....	46
AGRADECIMIENTOS.....	48
G L O S A R I O.....	49

## INTRODUCCIÓN

La seguridad de la información se ha convertido en un tema estratégico para las organizaciones, en un mundo en donde los servicios se basan en tecnología, procurar la fidelidad y la confianza de los usuarios son factores indispensables para garantizar su permanencia en el negocio.

Es importante tener presente que no existe seguridad absoluta, existirá un mayor o menor nivel de seguridad y ese dependerá de las personas, procesos, instalaciones y tecnologías implementadas para la gestión de la seguridad<sup>1</sup>, por tanto entre mayor sea el nivel de madurez de la gestión de la seguridad, mayor será el nivel de protección de los activos de información de la empresa y de sus servicios basados en tecnología.

En razón de lo anterior, el foro interbancario de seguridad de la información de la Cámara de Bancos e Instituciones Financieras de Costa Rica, ha diseñado el presente modelo de autoevaluación del nivel de madurez de la gestión de seguridad de la información.

El modelo de madurez de Gestión de Seguridad parte de los siguientes considerandos:

- Los servicios financieros tienen una gran dependencia de la tecnología, esta sirve como un medio facilitador de las transacciones financieras que beneficia a entidades y clientes.
- La información se ha convertido en un activo fundamental que incide en la productividad y competitividad de las empresas.
- La Seguridad de la información contempla la protección de la información que se almacena, transmite y procesa en cualquier medio, instalaciones, personas, infraestructura y procesos.
- Las entidades financieras almacenan, transmiten y procesan información que es propiedad de los clientes y deben velar por su confidencialidad, integridad y disponibilidad.
- Los servicios financieros se basan en la información y, esta se ha convertido literalmente en dinero.
- El nivel de seguridad de una organización se ve afectado por el accionar de todas sus áreas, funcionarios, procesos y tecnologías.
- La seguridad de la información es un tema estratégico que impacta directamente el negocio.
- Un incidente de seguridad, además de poder provocar un eventual fraude, podría generar la pérdida de confianza en la entidad y en el sistema financiero en general.

---

<sup>1</sup> Cuando se utilice “seguridad” aquí y en el resto del documento, entiéndase como un tema general, o sea tanto seguridad de la información como seguridad de TI indistintamente.

- Cada día surgen nuevas amenazas que atentan contra la información y las plataformas tecnológicas, siendo el sector financiero uno de los principales objetivos de la delincuencia a nivel mundial.
- Las mejores prácticas en materia de seguridad de la información (ISO 27000, Cobit, NIST, PCI, Ley de Control Interno, etc.) indican que la seguridad de la información debe administrarse desde el nivel más apropiado de la organización en consecuencia de los servicios a proteger, la criticidad y el valor de los datos.
- El área de Seguridad de la información debe contar con la autoridad e independencia requerida, que evite el conflicto de intereses y que garantice que las acciones de seguridad están en línea con los requerimientos del negocio.
- El sector financiero es líder en el tema de seguridad de la información, sin embargo, existen diferencias importantes en cuanto a las prácticas utilizadas en las diferentes entidades, por lo que surgió la necesidad de definir un modelo de autoevaluación que permita al sector financiero, homologar las mejores prácticas en gestión de la seguridad de la información.

## OBJETIVO

Definir un modelo de autoevaluación, que permita unificar las mejores prácticas para la gestión de seguridad de la información de las entidades miembros de la Cámara de Bancos e Instituciones Financieras. Permitiendo a las diferentes entidades, identificar las brechas de seguridad existentes; y definir un plan integral de Seguridad de la información o “roadmap” que les permita ir mejorando su nivel de gestión y por tanto el nivel de seguridad de su información.

## DESCRIPCIÓN GENERAL

Es importante que los jefes de las diferentes entidades, entiéndase por jefes, la Junta Directiva o Consejo de Administración<sup>2</sup>, Gerente General y Comité Ejecutivo, tengan claridad sobre el impacto que un eventual incidente de seguridad de la información pueda ocasionar en la operación del negocio y por consiguiente conozcan el nivel de madurez de su entidad.

Se recomienda que la revisión del modelo de madurez, sea ejecutada por las áreas de control interno en coordinación con el área encargada de la gestión de la seguridad, en el entendido de que este no es un modelo de cumplimiento o normativo, sino una herramienta de autoevaluación, que permite tener claridad de la situación actual, identificar brechas y definir acciones que permitan

---

<sup>2</sup> En algunas entidades la figura de la Junta Directiva es sustituida por un Consejo de Administración a partir de ahora se hará referencia a la Junta Directiva, entiéndase Consejo de Administración cuando así corresponda.

mejorar la gestión de la seguridad. Este modelo no proporciona una calificación general de seguridad, ya que en términos de protección de la información, un factor que no se encuentre bien gestionado, podría afectar la seguridad como un todo.

El resultado de las brechas identificadas, debería ser presentado a la Gerencia General y a la Junta Directiva, para que la administración tenga claridad sobre el estado de la gestión de la seguridad y la oportunidad de la entidad de mejorar, considerando las eventuales limitaciones, financieras, técnicas o de otros recursos.

Este modelo simplificado de autoevaluación, contempla los principales factores que pueden afectar la gestión de la seguridad de la información, basado en un análisis de normas y modelos internacionales, tales como ESG (Enterprise Strategy Group), Cybersecurity Maturity Model, SSE-CMM (Systems Security Engineering Capability Maturity Model), Cybersecurity Capability Maturity Model (C2M2), ISM3 (Information Security Management Maturity Model) y COBIT 5.

Algunos factores como por ejemplo el “Factor 1. Responsabilidad e Involucramiento”, el “Factor 2. Marco de Gobierno de Seguridad de la Información” y el “Factor 3. Organización de la Seguridad”, tienen un impacto directo en los demás factores y podrían ser catalizadores o inhibidores del proceso de gestión de la seguridad de la información. La recomendación es que dentro de las posibilidades de cada entidad, se procure lograr un nivel de madurez, cada vez mayor para cada uno de los factores definidos. Promoviendo un modelo de calidad, que debe ser revisado y ajustado periódicamente.

La mayoría de los factores que conforman este modelo, son por lo general responsabilidad directa del área de seguridad de la información, pero dependiendo de la estructura organizacional de cada entidad, algunos de ellos son gestionados por otras áreas, con las que, el área de gestión de seguridad de la información debe coordinar para contar con la información requerida y poder realizar su función primordial de protección de la información. Algunos ejemplos de estos temas son: la clasificación de la información, que es desarrollado como parte de la arquitectura empresarial; la gestión del riesgo, que es desarrollado por el área de riesgo y el de continuidad desarrollado por el área de continuidad de TI y continuidad del negocio.

Este modelo permitirá avanzar de forma integral con los temas más relevantes que impactan la seguridad de la información. Además el “Factor 2. Marco de Gobierno de Seguridad de la Información”; al requerir el alineamiento a un marco de referencia internacional, incluye de forma implícita la implementación de controles de seguridad adicionales orientados a la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI).

Para efectos de este modelo, cuando se hace referencia a estándares internacionales o marcos de referencia, se hace pensando en la aplicación de las buenas prácticas que han sido definidas a partir de la experiencia de un grupo de expertos para lograr una adecuada gestión de la seguridad de la información y no como un tema de certificación, esto considerando que los procesos de certificación son complejos y debe ser decisión de cada entidad si opta o no por un proceso formal de certificación.

En el tema de seguridad de la información, se habla de dos grandes conceptos: Sistema de Gestión de Seguridad de la Información (SGSI) y de Arquitectura de Seguridad.

El concepto de un SGSI, implica la creación de un proceso de gestión de seguridad de la información que procure resguardar la confidencialidad, la integridad y la disponibilidad de la información y los servicios del negocio soportados por la plataforma tecnológica. Un proceso de gestión basado en un modelo de mejora continua basado en el ciclo de calidad definido por Deming<sup>3</sup>, el cual define cuatro grandes actividades conocidas como Planear, Hacer, Verificar y Actuar.

Es importante considerar que el principio de “disponibilidad” es ampliamente desarrollado bajo el concepto de “continuidad”, tanto a nivel de tecnología, como de negocio y es visto como un tema operativo, se incluye un apartado de “continuidad” en este modelo, que evalúa los temas más relevantes, sin embargo no se profundiza porque el tema en sí amerita toda una metodología de trabajo y es importante mantener el enfoque del modelo en el tema de seguridad y en el objetivo de simplicidad.

El concepto de “disponibilidad” es abarcado además en el modelo, como la no afectación de los servicios ocasionado por incidentes relacionados a la seguridad, por lo cual, en el tanto se implemente un adecuado SGSI, se minimizaran los incidentes de seguridad que eventualmente podrían afectar la disponibilidad de la información o continuidad de los servicios y en caso de presentarse un eventual incidente de seguridad, se tendrán los planes de atención de incidentes de seguridad, orientados a minimizar el impacto para el negocio .

El concepto Arquitectura de Seguridad, es un término muy amplio, que involucra prácticamente todos los controles que usualmente son incluidos dentro de una política o disposición de seguridad, orientado a controlar la tecnología, las instalaciones, los procesos y las personas. Si lo vemos a la luz de un estándar como ISO27001, es la definición del grupo total de controles de seguridad orientados a proteger la confidencialidad, integridad y disponibilidad de la información y la

---

<sup>3</sup> **William Edwards Deming**, promotor de la teoría administrativa de la calidad total.

continuidad de los servicios basados en tecnología. Existen modelos como el “Open Security Architecture” que proponen y presentan de una forma gráfica y por áreas comunes de gestión, los temas que deben ser parte de una “Arquitectura de Seguridad”.

El definir una Arquitectura de Seguridad, facilita la implementación de nuevos procesos, servicios, aplicaciones o elementos a la plataforma actual, porque define y estandariza los controles requeridos para diferentes tipos de procesos, servicios, sistemas o elementos, procurando la protección de la información.

Una Arquitectura de Seguridad empresarial, está compuesta por varios elementos de seguridad y podemos hablar entonces de arquitectura de seguridad de red, arquitectura de seguridad de datos o información, arquitectura de seguridad de sistemas, etc. Esta se convierte en un marco definido que involucra todos los controles de seguridad; para efectos de este modelo de gestión de madurez de la seguridad de la información, involucra todos y cada uno de los factores aquí definidos.

A continuación se definen los diferentes factores y su escala de madurez:

## FACTOR 1. RESPONSABILIDAD E INVOLUCRAMIENTO

La seguridad de la información es responsabilidad de toda la entidad y para tener claridad sobre la responsabilidad es indispensable el involucramiento de las diferentes áreas y personal de toda la entidad, especialmente el de la Junta Directiva y el Comité Ejecutivo.

Para asegurar la responsabilidad y el involucramiento de todo el personal, es indispensable que exista una política de seguridad emitida por la máxima autoridad de la entidad. La política debe ser de carácter general, no técnica y debe indicar el compromiso de la entidad con los principios de seguridad de la información, a saber la confidencialidad, integridad y disponibilidad.

La política de seguridad debe instar a la administración a la generación de la normativa y de los controles de seguridad requeridos.

Además es importante que tanto la Junta Directiva como el Comité Ejecutivo se mantengan informados del estado de la seguridad de la información y pueda tomar decisiones sobre los temas que considere necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información y de los servicios basados en tecnología.

Es importante mencionar, que el “**Factor 7. Capacitación y Concienciación a Usuarios**” abarca la capacitación de todo el personal, sin embargo en este factor se menciona de forma exclusiva a la Junta Directiva y al Comité Ejecutivo, porque la capacitación es un elemento indispensable para tener claridad sobre el impacto de la seguridad en la estrategia y servicios del negocio y a partir de ahí motivar el involucramiento en los temas que afectan la seguridad. Además el “**Factor 4.**

**Reportes de Seguridad**” menciona las instancias a las que se remiten los diferentes informes de seguridad de la información, sin embargo, para el tema de involucramiento es indispensable que la Junta Directiva y el Comité Ejecutivo reciban informes que les permitan tomar decisiones y por esa razón ese tema también está incluido en este Factor.

#### **NIVELES DE MADUREZ:**

1. **INCIPIENTE:** No existe una política de seguridad de la información emitida por la máxima autoridad de la entidad. Los miembros de la Junta Directiva y del Comité Ejecutivo no reciben capacitación general sobre el tema de seguridad de la información. Ni la Junta Directiva, ni el Comité Ejecutivo reciben informes sobre el nivel de madurez de la gestión de la seguridad ni sobre el estado de la seguridad de la información.
2. **BAJO:** Existe una política de seguridad de la información emitida por la máxima autoridad de la entidad. Los miembros de la Junta Directiva y del Comité Ejecutivo no reciben capacitación general sobre el tema de seguridad de la información. Ni la Junta Directiva, ni el Comité Ejecutivo reciben informes sobre el nivel de madurez de la gestión de la seguridad ni sobre el estado de la seguridad de la información.
3. **MEDIO:** Existe una política de seguridad de la información emitida por la máxima autoridad de la entidad. Los miembros del Comité Ejecutivo reciben capacitación general sobre el tema de seguridad de la información, pero no los miembros de la Junta Directiva. Ni la Junta Directiva, ni el Comité Ejecutivo reciben informes sobre el nivel de madurez de la gestión de la seguridad ni sobre el estado de la seguridad de la información.
4. **ALTO:** Existe una política de seguridad de la información emitida por la máxima autoridad de la entidad. Los miembros de la Junta Directiva y del Comité Ejecutivo reciben capacitación general sobre el tema de seguridad. El Comité Ejecutivo recibe informes sobre el nivel de madurez de la gestión de la seguridad y el estado de la seguridad de la información, pero la Junta Directiva no recibe informes.
5. **ÓPTIMO:** Existe una política de seguridad de la información emitida por la máxima autoridad de la entidad. Los miembros de la Junta Directiva y del Comité Ejecutivo reciben capacitación general sobre el tema de seguridad. La Junta Directiva y el Comité Ejecutivo recibe informes sobre el nivel de madurez de la gestión de la seguridad y el estado de la seguridad de la información.

## FACTOR 2. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El Gobierno de la seguridad de la información es un elemento del Gobierno empresarial o corporativo, orientado al cumplimiento de los objetivos y planes estratégicos definidos por la empresa, minimizando los riesgos que afectan la seguridad de la información.

El objetivo principal de la gestión de seguridad es diseñar, implementar y mantener un Sistema de Gestión de Seguridad de la Información a través de un conjunto coherente de controles para la gestión eficaz de la información, minimizando los riesgos y garantizando de manera razonable la confidencialidad, la integridad y la disponibilidad de los activos de información.

Para poder definir, implementar y mantener un SGSI, es necesario contar con un proceso de gestión de la seguridad de la información, que garantice la implementación de un modelo de calidad y establezca cómo se ejecutarán las actividades de Planeamiento, Ejecución, Revisión y Acción (Plan, Do, Check, Act) de forma metodológica, a esto es a lo que se llama proceso de gestión de la Seguridad de la información.

Utilizar como marco de referencia para la gestión de la seguridad o para la implementación de un SGSI, un estándar o modelo internacional, garantiza a la entidad que su gestión considera los temas más relevantes en materia de protección de la información, permite aprovechar la experiencia de los especialistas que definen y actualizan estos estándares o modelos y facilita la implementación de un marco de gobierno de la seguridad de la información.

Para tener gobernabilidad, es importante que exista un proceso de gestión de la seguridad de la información, un marco normativo alineado a las mejores prácticas o estándares internacionales, así como un plan de seguridad debidamente alineado a la estrategia del negocio. Además, considerando el impacto que tiene la seguridad en el negocio, es indispensable que el plan de seguridad sea conocido y aprobado por el Comité de Seguridad o por el Comité que cumpla con las funciones del Comité de Seguridad, sin embargo en un nivel alto de madurez, es indispensable que exista un Comité de Seguridad.

Es ideal alinearse a un estándar de seguridad, que sea certificable, aún y cuando la entidad no se certifique, esto permite implementar las mejores prácticas definidas y permite hacer una medición objetiva del nivel de alineamiento al estándar de forma que se puedan identificar brechas y definir planes de mejora. Si una entidad eventualmente decide certificarse, eso tendrá el valor adicional de que un ente externo y especializado, revisará el nivel de cumplimiento con el estándar seleccionado.

### NIVELES DE MADUREZ:

1. **INCIPIENTE:** No existe un plan de seguridad, no existe un proceso de gestión, ni un marco normativo formalizado. Se aplican controles de seguridad, pero estos no se encuentran documentados.
2. **BAJO:** No existe un plan de seguridad, no existe un proceso de gestión, existe un marco normativo documentado y formalizado, pero no está alineado a ningún marco o estándar de referencia internacional en materia de seguridad de la información.

3. **MEDIO:** Existe un plan de seguridad, un proceso de gestión y un marco normativo documentado y formalizado, pero el plan no está alineado a la estrategia de la entidad. El proceso de gestión y el marco normativo no se encuentran alineados a ningún marco o estándar de referencia internacional en materia de seguridad de la información.
4. **ALTO:** Existe un plan de seguridad alineado a la estrategia de la entidad, un proceso de gestión y un marco normativo documentado, formalizado y alineado a algún marco o estándar de referencia internacional en materia de seguridad de la información. El plan fue conocido y aprobado por el Comité de Seguridad o el Comité que cumple con las funciones del Comité de Seguridad. Existe medición del plan de seguridad, del proceso de gestión de la seguridad y del marco normativo, pero no es informado al Comité.
5. **ÓPTIMO:** Existe un plan de seguridad alineado a la estrategia de la entidad, un proceso de gestión y un marco normativo documentado, formalizado y alineado a algún marco o estándar de referencia internacional en materia de seguridad de la información. El plan fue conocido, validado y aprobado por el Comité de Seguridad y este realiza la medición y seguimiento del cumplimiento del plan de seguridad, del proceso de gestión de la seguridad y del marco normativo.

### FACTOR 3. ORGANIZACIÓN DE LA SEGURIDAD

La seguridad de la información es un tema estratégico que tiene un impacto directo en la operación y en la continuidad del negocio; por lo tanto la forma en cómo esté organizada la seguridad en la entidad, es un factor determinante para lograr la mejor gestión de la seguridad de la información.

El área de seguridad de la información debe identificar y definir controles o medidas, tanto técnicas como administrativas, que deben ser implementados por las diferentes áreas de la entidad, para procurar la protección de la información.

El proceso evolutivo de la gestión de la seguridad, inicia con un enfoque meramente técnico, orientado a la protección del hardware, software y en especial a la información, almacenada, transmitida y procesada a través de los sistemas que soportan los servicios de una empresa. Conforme se avanza en el nivel de madurez, su enfoque se vuelve más estratégico, definiendo y monitoreando controles técnicos y administrativos, procurando la seguridad de la información en todos sus medios.

Cuando el área de seguridad de TI evoluciona hacia un área de seguridad de la información, se amplía la visión y participación a las diferentes áreas de la empresa, de forma que cada área asume su rol y responsabilidad dentro del proceso de gestión de la seguridad de la información, coordinado o gobernado de forma integral por el área de seguridad de la información. Es por lo anterior que en el nivel de mayor madurez, se evita el contar con más de un área de seguridad, a fin de establecer roles y funciones claras, que eviten la evasión y confusión de responsabilidades y que cada área asuma su rol y responsabilidad como parte de la seguridad.

Los controles definidos son aplicados por las diferentes áreas de la organización, incluyendo en gran medida a las áreas de tecnología, situación que evidencia un conflicto de intereses cuando el área de seguridad de la información reporta al área de tecnología.

En un proceso de mejora continua (Planear-hacer-verificar-actuar) la gestión de la seguridad de la información en una etapa de máxima madurez se encarga mayormente de “Planear” y “Verificar” los diferentes controles de seguridad, de manera tal, que son las diferentes áreas de la entidad las que ejecutan las funciones de “Hacer” o implementar los controles definidos y los que “Actúan” a partir de los hallazgos identificados en la fase de verificación. Esta separación de funciones refuerza los principios básicos<sup>4</sup> de control interno, a través de una adecuada segregación de funciones.

La organización para una adecuada gestión de la seguridad, depende del tamaño y nivel de complejidad de cada entidad, su nivel de madurez dependerá del nivel de autoridad e independencia que tenga el área de seguridad, para el cumplimiento de sus funciones y objetivos, así como del enfoque del área, que va desde un enfoque técnico hasta un enfoque estratégico orientado a la gestión de la seguridad de la información de forma integral, sin administrar “elementos activos” propios de la gestión tecnológica.

Entiéndase por “elementos activos” de la plataforma, aquellos que soportan las operaciones del negocio y en caso de falla afectarán los servicios brindados, tal como los equipos de “firewall e IPS”. El área de seguridad de la información en un nivel de madurez alto, se enfoca en herramientas de monitoreo y control, pero no de soporte tecnológico, esas labores son delegadas a áreas de TI.

Como un elemento adicional que agrega gobernabilidad a la seguridad de la información, las organizaciones conforman un “Comité de Seguridad” en el que se analizan las principales situaciones que afectan la seguridad de la información y en donde se presentan y aprueban los planes e informes de manera que permita a un grupo interdisciplinario promover e impulsar las prácticas de seguridad.

La conformación del Comité de Seguridad varía dependiendo de cada entidad, lo importante es que esté conformado por representantes de las áreas comerciales de alto nivel y de los responsables de las áreas de Seguridad de la Información, Riesgo Tecnológico y Tecnología. Es importante tener presente que este no es un Comité técnico, sino estratégico, cuya principal función es promover la seguridad de la información como un tema de apoyo al cumplimiento de la estrategia del negocio.

## **NIVELES DE MADUREZ:**

- 1. INCIPIENTE:** No existe un encargado de Seguridad de TI, las funciones son asignadas directamente al encargado de TI.

---

<sup>4</sup> Los principios básicos de control interno promueven la separación entre los roles de quien define, quien ejecuta y quien revisa, eliminando eventuales conflictos de interés.

2. **BAJO:** Existe un encargado de seguridad de TI. El enfoque es totalmente técnico, se encarga de la administración de equipos como el firewall, IPS, proxy, administración de usuarios, etc.
3. **MEDIO:** Existe un encargado de seguridad de TI. El enfoque es mixto, es decir, que podría encargarse tanto temas técnicos como administrativos para la protección de la información. Existe un Comité de Seguridad o las funciones de un Comité de Seguridad, han sido asignadas a algún otro Comité de la entidad.
4. **ALTO:** Existe un encargado de seguridad de TI, que se encarga de los aspectos técnicos; además existe un área de seguridad de la información, que no depende del área de tecnología, y se encarga de la gestión de la seguridad de la información, con un enfoque estratégico orientado a proteger la información y los servicios del negocio. Existe un Comité de Seguridad o las funciones de un Comité de Seguridad, han sido asignadas a algún otro Comité de la entidad.
5. **ÓPTIMO:** Existe un área de seguridad de la información, con un enfoque integral y estratégico, la cual reporta al Gerente General, Junta Directiva, al área de riesgo u otra que le permita contar con independencia y empoderamiento. Se encuentra ubicada fuera del área de TI y no administra elementos activos de la plataforma tecnológica. Los controles de seguridad aplicables a la tecnología son administrados por cada área dentro de TI de igual forma que en otras áreas del negocio, asumiendo su responsabilidad y siguiendo las directrices y lineamientos definidos por el área de Seguridad de la Información. Existe un Comité de Seguridad.

## FACTOR 4. INVERSIÓN EN SEGURIDAD

Todo negocio realiza inversiones para recibir un beneficio, en términos financieros es usual utilizar el retorno de la inversión como una medida de la rentabilidad o conveniencia de realizar una inversión.

Los controles de seguridad se implementan para disminuir o controlar riesgos que han sido identificados y que en caso de que se presenten se podrían generar pérdidas económicas a la entidad, ya sea por robo, fraude, ingresos no recibidos a partir de la afectación de los servicios, por pérdida de clientes, pérdida de imagen u otros.

Por lo anterior la inversión en seguridad se ejecuta para evitar una pérdida, no para generar una ganancia y eventualmente puede ser calculado a través de estimaciones anuales de pérdidas (Annualized Loss Expectancy ALE).

Existen varias metodologías para la estimación de pérdidas, algunas entidades, valoran la conveniencia de los controles de seguridad al momento de valorar sus riesgos, identificando en ese momento la pérdida esperada por la no implementación de un control, otras prefieren hacerlo como parte de la justificación de un nuevo proyecto de seguridad, el tema es realmente complejo por la cantidad de factores y variabilidad de las situaciones de riesgo e impacto, por esa razón, este modelo, no se involucra en la estimación de la pérdida, pero define algunos aspectos importantes, necesarios para contar con el presupuesto de seguridad requerido para la entidad.

La inversión en seguridad va a estar en función de la complejidad de la operación de cada entidad y variará año a año conforme a los planes de seguridad definidos para apoyar los planes comerciales. De forma que si existe un proyecto para incursionar en un nuevo servicio que requiere de nuevos controles de seguridad, es importante que exista esa alineación entre los planes y se puedan ofrecer los nuevos servicios con los controles de seguridad requeridos.

#### **NIVELES DE MADUREZ:**

1. **INCIPIENTE:** No existen partidas presupuestarias para seguridad, la compra de software, hardware o servicios de seguridad, no responden a ningún tipo de plan, se realizan motivadas por temas de cumplimiento y son fácilmente eliminadas del presupuesto.
2. **BAJO:** No existen partidas presupuestarias para seguridad, la compra de software, hardware o servicios de seguridad, está alineada al plan de tecnología, las adquisiciones se hacen sobre todo motivadas por temas de cumplimiento y son fácilmente eliminadas del presupuesto.
3. **MEDIO:** No existen partidas presupuestarias para seguridad, la compra de software, hardware o servicios de seguridad está alineada a un plan de seguridad no alineado al negocio, sin embargo es usual que el presupuesto sea eliminado o utilizado para otros proyectos.
4. **ALTO:** Existen partidas presupuestarias para seguridad, la compra de software, hardware o servicios de seguridad está alineada a un plan de seguridad, no alineado al negocio, el presupuesto es difícilmente eliminado o utilizado para otros proyectos.
5. **ÓPTIMO:** Existen partidas presupuestarias para seguridad, la compra de software, hardware o servicios de seguridad son parte de un plan de seguridad alineado al negocio, el presupuesto de seguridad se respeta, no se elimina ni es utilizado para otros proyectos.

## **FACTOR 5. REPORTES DE SEGURIDAD**

La seguridad de la información podría afectar sensiblemente los servicios y la operación del negocio, es por eso importante que la administración se mantenga debidamente informada del nivel de seguridad de la entidad, de forma que se puedan tomar decisiones basadas en el riesgo

de la información y de ser necesario corregir las situaciones que resulten contrarias a los objetivos estratégicos de la entidad.

#### **NIVELES DE MADUREZ:**

1. **INCIPIENTE:** No se generan reportes de seguridad de ningún tipo.
2. **BAJO:** Se generan reportes de fallas o incidentes relacionados con la seguridad, únicamente cuando existe un incidente, los reportes son de uso interno del área de seguridad, no son comunicados a ninguna jefatura o Comité.
3. **MEDIO:** Se generan reportes de los indicadores de seguridad definidos y de los incidentes de forma periódica. Los reportes son comunicados a la jefatura directa del área de Seguridad.
4. **ALTO:** Se generan reportes de los indicadores de seguridad definidos y de los incidentes de forma periódica. Así como un informe resumen de la situación general de seguridad de la entidad, al menos una vez al año. Los reportes son comunicados a la al Comité de Seguridad o al comité que cumpla con las funciones del Comité de Seguridad y al Comité Ejecutivo.
5. **ÓPTIMO:** Se generan reportes de los indicadores de seguridad definidos y de los incidentes de forma periódica. Así como un informe resumen de la situación general de seguridad de la entidad al menos cada seis meses y un informe anual de tendencias de la seguridad que permita anticipar eventuales riesgos de nuevas tecnologías o nuevas amenazas. Los reportes son comunicados al Comité de Seguridad, al Comité Ejecutivo y a la Junta Directiva.

## **FACTOR 6. CONOCIMIENTO DEL PERSONAL DE GESTIÓN DE SEGURIDAD**

Contar con personal con conocimiento y experiencia en seguridad, es uno de los factores más críticos y tiene un impacto directo en la implementación de un proceso de gestión de seguridad y por tanto en la seguridad de la información. Contar con personal con las habilidades requeridas y promover el conocimiento actualizado es un tema indispensable.

El tener perfiles de puesto con funciones claras y requerimientos de conocimiento, experiencia, así como un plan de capacitación orientado a cerrar las brechas de conocimiento, mantener el conocimiento actualizado y contar con personal certificado, garantiza a la entidad el tener al personal adecuado.

El tema de seguridad de la información es un tema muy especializado, que requiere experiencia y conocimiento. Es cierto que un buen gerente puede gestionar cualquier área, sin embargo, también es cierto que un gerente que domine el área a cargo, definitivamente será un mejor gerente y contará con el apoyo indiscutible de su equipo de trabajo.

El tema de seguridad, es un tema que requiere de conocimiento especializado y experiencia, temas son evaluados en certificaciones internacionales orientadas a la gestión de la seguridad como lo son CISSP, CISM y que garantizan a la entidad que quien gestiona la seguridad de la información cuenta con el conocimiento requerido para realizar un trabajo alineado a las mejores prácticas internacionales.

Adicionalmente existen certificaciones en temas de específicos como seguridad en redes, aplicaciones y otros que de igual forma dan un nivel alto de confianza en el trabajo que realiza el personal del área de seguridad, cuya responsabilidad en la operación del negocio y en un sector tan sensible a la confianza de los clientes, como lo es el sector financiero, requiere de un nivel alto de expertis.

Es importante tener presente que ante un tema tan variable, demandante y crítico, como la seguridad de la información, el mantener personal adecuado y actualizado es indispensable para la entidad.

#### **NIVELES DE MADUREZ:**

- 1. INCIPIENTE:** No existen perfiles de puesto <sup>5</sup>definidos, ni funciones claras, no existe un plan de capacitación para el personal del área de gestión de seguridad. Además el personal de seguridad no recibe capacitación de actualización tecnológica.
- 2. BAJO:** No existen perfiles de puesto definidos, ni funciones claras, no existe un plan de capacitación para el personal del área de gestión de seguridad. Pero el personal de seguridad recibe alguna capacitación de actualización tecnológica.
- 3. MEDIO:** Existen perfiles de puesto definidos con funciones claras, existe un plan de capacitación y el personal de seguridad recibe capacitación de actualización tecnológica, pero el plan no se enfoca en cerrar las brechas de conocimiento y mantener actualizado al personal de seguridad.

---

<sup>5</sup> Al indicar perfiles de puesto se refiere exclusivamente a los perfiles del personal responsable de la gestión de la seguridad de la información.

4. **ALTO:** Existen perfiles de puesto definidos con funciones claras, existe un plan de capacitación enfocado en cerrar las brechas de conocimiento, al menos para los temas considerados como más críticos y mantener actualizado al personal de seguridad, el nivel de ejecución del plan de capacitación es superior al 50%. El encargado del área de seguridad de la información cuenta con una certificación internacional <sup>6</sup> en gestión de la seguridad y se promueve la adquisición de certificaciones específicas <sup>7</sup> para el resto del equipo.
5. **ÓPTIMO:** Existen perfiles de puesto definidos con funciones claras, existe un plan de capacitación enfocado en cerrar las brechas de conocimiento, al menos para los temas considerados como más críticos y mantener actualizado al personal de seguridad y su nivel de ejecución es superior al 75%. El encargado del área de seguridad de la información cuenta con una certificación internacional en gestión de la seguridad y el personal del área de seguridad cuenta con certificaciones específicas de seguridad.

## FACTOR 7. CAPACITACIÓN Y CONCIENCIACIÓN A USUARIOS

Es indispensable capacitar al usuario interno y externo sobre las mejores prácticas de seguridad. El tema es muy amplio y por tanto es conveniente enfocarse en los temas más críticos, ya sea por su nivel de riesgo o por la cantidad de incidentes, situaciones que generen una gran cantidad de incidentes son temas idóneos para incluir en un plan de capacitación o de concienciación. Así como nuevas tecnologías que ameriten nuevos conocimientos o prácticas de seguridad.

El mayor reto en un plan de capacitación y de concienciación es que el mensaje sea entendido y adoptado por el público meta, para esto es indispensable analizar tanto el fondo como la forma del mensaje.

En el caso de los usuarios internos, es importante realizar una capacitación al personal de primer ingreso y al personal existente de acuerdo con el puesto de trabajo y áreas de especialización. En el caso de los usuarios externos o clientes, es indispensable al menos brindarles las recomendaciones básicas de seguridad para el uso de los servicios que se le ofrecen.

---

<sup>6</sup> Las certificaciones internacionales en gestión de seguridad más reconocidas son CISSP y CISM.

<sup>7</sup> Certificaciones en áreas como telecomunicaciones, aplicaciones, atención de incidentes, ethical hacker y otras que garantizan un nivel de especialización y mejora notablemente la gestión integral de la seguridad.

La capacitación debe ser acompañada de un plan de concienciación, que procure generar conciencia en los diferentes usuarios de la tecnología y de la información para que promuevan la seguridad, por eso es conveniente contar con un plan de concienciación efectivo que motive a los usuarios a ser responsables.

#### **NIVELES DE MADUREZ:**

- 1. INCIPIENTE:** No se imparte capacitación de concienciación en temas de seguridad de la información, ni a usuarios internos ni externos.
- 2. BAJO:** Se imparte capacitación de inducción al personal de nuevo ingreso, pero no se cuenta con un plan de concienciación a otros usuarios internos ni externos.
- 3. MEDIO:** Se imparte capacitación de inducción al personal de nuevo ingreso y se realizan algunas actividades de concienciación en temas de seguridad de la información de forma aislada, no planeada y no se incluye a todo el personal. Además no se dan recomendaciones de seguridad sobre el uso de los servicios a los usuarios externos, ni se cuenta con un plan de concientización para éstos.
- 4. ALTO:** Se imparte capacitación de inducción al personal de nuevo ingreso, se realizan actividades planificadas de concienciación en temas de seguridad de la información, pero no se imparte capacitación a personal o áreas especializadas. Se brindan recomendaciones de seguridad sobre el uso de los servicios a los usuarios externos, pero no se cuenta con un plan de concientización para estos.
- 5. ÓPTIMO:** Se imparte capacitación de inducción al personal de nuevo ingreso, se realizan actividades planificadas de concienciación en temas de seguridad de la información y se imparte capacitación a personal o áreas especializadas, tal como desarrollo de sistemas, soporte técnico y otros. Se brindan recomendaciones de seguridad sobre el uso de los servicios a los usuarios externos y se cuenta con un plan de concientización para éstos.

## **FACTOR 8. CUMPLIMIENTO LEGAL Y REGULATORIO**

Toda empresa debe cumplir con las leyes, reglamentos y regulaciones relacionadas con la seguridad de la información y de los servicios soportados por la tecnología que sean vinculantes a la operación de su negocio, para esto es indispensable tener identificadas las normas que deben cumplirse, deben ser validadas y de ser necesario deben ajustarse los procesos, sistemas o servicios para evitar incumplimientos que además de poner en riesgo la seguridad de la

información y los servicios del negocio, podrían tener consecuencias como multas o impacto a la imagen de la entidad.

En el tema de cumplimiento legal y regulatorio, intervienen varias áreas, entre ellas el área legal, el área de control interno, el área de riesgo, el área de seguridad y las áreas reguladas, para efectos del nivel de madurez a nivel de seguridad, se considera al área de seguridad como la responsable de coordinar la identificación, validación y cumplimiento de la normativa relevante a la seguridad de la información junto con todas las áreas involucradas. Además es claro que temas de carácter legal indiscutiblemente en caso de duda, deben ser analizados y dictaminados por el área legal.

#### **NIVELES DE MADUREZ:**

- 1. INCIPIENTE:** El área encargada de la seguridad, no ha identificado, ni validado con las otras áreas involucradas, las leyes, reglamentos o regulaciones sobre seguridad de la información y servicios soportados por tecnología que apliquen a la entidad.
- 2. BAJO:** El área encargada de la seguridad, ha identificado pero no ha validado con las otras áreas involucradas, las leyes, reglamentos o regulaciones sobre seguridad de la información y servicios soportados por tecnología que apliquen a la entidad.
- 3. MEDIO:** El área encargada de la seguridad, ha identificado y validado con las otras áreas involucradas, las leyes, reglamentos o regulaciones sobre seguridad de la información y servicios soportados por tecnología que apliquen a la entidad. Pero no ha identificado ni validado el nivel de cumplimiento.
- 4. ALTO:** El área encargada de la seguridad, ha identificado y validado con las otras áreas involucradas, las leyes, reglamentos o regulaciones sobre seguridad de la información y servicios soportados por tecnología que apliquen a la entidad, ha identificado el nivel de cumplimiento, pero no lo ha validado con las demás áreas involucradas.
- 5. ÓPTIMO:** El área encargada de la seguridad, ha identificado y validado con las otras áreas involucradas, las leyes, reglamentos o regulaciones sobre seguridad de la información y servicios soportados por tecnología que apliquen a la entidad, ha identificado el nivel de cumplimiento, lo ha validado con las demás áreas involucradas y todas las áreas tienen conocimiento de eventuales incumplimientos a corregir, así como el responsable de su atención.

## FACTOR 9. VALORACIÓN DE RIESGO

Los controles de seguridad deben orientarse a la gestión de riesgos de la información y por tanto es indispensable que exista una valoración que identifique los riesgos inherentes a la información y que en caso de materializarse podrían ocasionar daños o pérdidas económicas, de imagen, legales u otros a la entidad.

En la práctica y a pesar de que todo control de seguridad se implementa para mitigar un eventual riesgo, en entidades con poco nivel de madurez no se realiza una valoración formal o metodológica del riesgo, esto implica el riesgo de omitir situaciones que puedan afectar a la entidad y no se definan ni implementen los controles de seguridad requeridos.

Usualmente se habla de riesgo tecnológico, pero esto podría erróneamente considerarse que se limita a los riesgos de la plataforma tecnológica, lo cierto del caso es que todos los controles de seguridad se orientan a la protección de la información y de los servicios basados en tecnología y por tanto el concepto de riesgo tecnológico, implica todos aquellos riesgos que afectan la confidencialidad, integridad y disponibilidad de la información y por tanto incluye tanto al proceso mismo de gestión de la seguridad de la información, a los procesos de gestión de tecnología y a los procesos de negocio, de forma tal que para tener una visión integral de los riesgos de la información deberán analizarse todos los procesos de la entidad.

Debido a lo amplio y complejo del tema de riesgo y a pesar de que en el tema de seguridad una vulnerabilidad o riesgo existente en un sistema no crítico puede llegar a afectar los sistemas que sí lo son, es necesario priorizar servicios o procesos y para esto se utiliza un análisis de impacto de negocio (Business Impact Analysis o por sus siglas en inglés "BIA") de manera que tanto el riesgo, como la seguridad se enfoque inicialmente en los servicios o procesos más críticos para el negocio.

Es importante indicar que un servicio podría utilizar más de una aplicación y aunque analizar el tema de riesgos a nivel de procesos o servicios da una mayor visión, para efectos de priorización es posible identificar aplicaciones críticas para el negocio, de forma que tanto la gestión de la tecnología como la gestión de la seguridad le dé prioridad inicialmente a esas aplicaciones catalogadas como críticas.

Existen diferentes metodologías de valoración de riesgo. Para efectos de efectividad es importante que la metodología utilizada considere los conceptos de probabilidad e impacto, esto para determinar el nivel de riesgo para la entidad y con base en el nivel de riesgo identificado, estos puedan ser priorizados a fin de tomar acciones basadas en el nivel de los riesgos identificados y en el apetito de riesgo, definido por la entidad. Los riesgos deben ser presentados a un Comité que

acuerde las medidas propuestas para su atención, que podrían ir desde planes de mitigación, a la aceptación del riesgo, el traslado, para lo cual usualmente se utilizan herramientas como seguros e incluso la eliminación del riesgo, que usualmente implica la eliminación de la actividad que genera el riesgo.

Para efectos de la gestión de la seguridad, la identificación de los riesgos es un insumo importantísimo, para la adecuada definición de controles de seguridad orientados al riesgo de la entidad. Este modelo no profundiza en la manera correcta de gestionar los riesgos, pero en el tanto se utilice una adecuada metodología de valoración de riesgos, se mejorará la gestión de la seguridad.

El nivel de madurez aumenta sobre todo por el nivel de cobertura de las valoraciones de riesgo efectuadas, pasando del proceso mismo de gestión de la seguridad de la información, a incluir los procesos de gestión de la tecnología, las aplicaciones o servicios críticos y terminando al incluir los procesos de negocio, con lo cual se tendría una gestión total de los riesgos, a partir de los cuales se definen los controles de seguridad adecuados conforme al apetito de riesgo de cada entidad. Es importante tener presente que para efectos de la gestión de la seguridad, las valoraciones de riesgo son un insumo para el proceso.

#### **NIVELES DE MADUREZ:**

1. **INCIPIENTE:** No existe una metodología de valoración de riesgos. Ni se realizan procesos de valoración de riesgos.
2. **BAJO:** Existe una metodología de valoración de riesgos que considera los conceptos de probabilidad, impacto, priorización y planes de acción; y esta es aplicada al menos al proceso de gestión de seguridad. La valoración de riesgo es utilizada como un insumo del proceso de gestión de seguridad, para la definición de controles de seguridad para los riesgos identificados.
3. **MEDIO:** Existe una metodología de valoración de riesgos que considera los conceptos de probabilidad, impacto, priorización y planes de acción; y esta es aplicada al proceso de gestión de la seguridad y a los procesos de gestión de tecnología. La valoración de riesgo es utilizada como un insumo del proceso de gestión de seguridad, para la definición de controles de seguridad para los riesgos identificados.

4. **ALTO:** Existe una metodología de valoración de riesgos que considera los conceptos de probabilidad, impacto, priorización y planes de acción; y esta es aplicada al proceso de gestión de la seguridad, a los procesos de gestión de tecnología y a las aplicaciones catalogadas como críticas por la entidad. Existe un programa de trabajo para la valoración del riesgo y sus resultados son utilizados como un insumo del proceso de gestión de seguridad, para la definición de controles de seguridad para los riesgos identificados. Los riesgos identificados son presentados a un Comité y estos son mitigados, aceptados, transferidos o eliminados.
  
5. **ÓPTIMO:** Existe una metodología de valoración de riesgos que considera los conceptos de probabilidad, impacto, priorización y planes de acción; y esta es aplicada al proceso de gestión de la seguridad, a los procesos de gestión de tecnología, a los procesos de gestión del negocio y a los servicios o procesos catalogados como críticos por la entidad. Existe un programa de trabajo para la valoración del riesgo y sus resultados son utilizados como un insumo del proceso de gestión de seguridad, para la definición de controles de seguridad para los riesgos identificados. Los riesgos identificados son presentados a un Comité y estos son mitigados, aceptados, transferidos o eliminados.

## FACTOR 10. GESTIÓN DE LA INFORMACIÓN

El activo informático<sup>8</sup> más importante a proteger es la información. La adecuada gestión de la información, implica que debe tenerse control de la información en todos sus medios, electrónicos, impresos u otros. Esto hace que la adecuada gestión de la información sea un tema complejo, que requiere identificar el origen de la información, sus dueños, su nivel de sensibilidad y con base en eso definir los controles de seguridad adecuados para cada tipo de información.

Además del nivel de sensibilidad de la información, para definir controles de protección es importante identificar el estado de la información, de forma que se definan controles para datos en reposo, en movimiento, en uso o en dispositivos de usuario final.

La gestión de la información toma más importancia ahora que se promueve el uso de almacenamientos de información, estructurada y no estructurada (Big Data) y de sistemas de consulta o análisis (Data Analysis, Business Intelligence, Data Mining), que permiten una gran flexibilidad y capacidad al usuario. Debe entenderse que esa es una tecnología orientada al

---

<sup>8</sup> El activo más importante para cualquier organización es el recurso humano, sin embargo, éste modelo está enfocado a la información y por tanto para hacer la diferencia se menciona "activo informático".

negocio, que no debe ser ajena a los controles de seguridad y que independientemente de la facilidad existente, deberán siempre prevalecer los principios de “necesidad de saber” (Need to know) y “menor privilegio” (less privileged) utilizados como base para la asignación de permisos a los usuarios, cualquier violación a estos principios expondrá la seguridad de la información de forma realmente innecesaria y por tanto implementar modelos del tipo “Big Data” sin respetar los controles de seguridad definidos conforme el nivel de sensibilidad de la información será un grave error.

#### **NIVELES DE MADUREZ:**

1. **INCIPIENTE:** No existe un inventario de información, ni de sus dueños, no existe una metodología o procedimiento de clasificación de la información.
2. **BAJO:** Existe un inventario de información, los dueños de la información se encuentran identificados, pero no existe una metodología o procedimiento de clasificación de la información.
3. **MEDIO:** Existe un inventario de información, los dueños de información se encuentran identificados, existe una metodología o procedimiento de clasificación que incluye niveles de sensibilidad y medidas de protección a aplicar, pero la información no se encuentra clasificada.
4. **ALTO:** Existe un inventario de información, los dueños de información se encuentran identificados, existe una metodología o procedimiento de clasificación que incluye niveles de sensibilidad, se han definido e implementado medidas de protección y la información se encuentra clasificada.
5. **ÓPTIMO:** Existe un inventario de información, los dueños de información se encuentran identificados, existe una metodología o procedimiento de clasificación que incluye niveles de sensibilidad, se han definido e implementado medidas de protección, la información se encuentra clasificada y existe una verificación de cumplimiento de las normas de manejo establecidas para cada tipo de información, así como herramientas automatizadas y procedimientos para la protección de fuga o robo de datos.

## **FACTOR 11. SEGURIDAD EN PROYECTOS**

La seguridad al igual que cualquier otro control, es mucho más eficiente y eficaz cuando se incorpora desde la fase de diseño de un servicio, aplicación o tecnología y no al momento de su implementación, cuando podrían darse inconvenientes de integración o situaciones que generen riesgos para la seguridad de la información.

Un proyecto debe pasar inicialmente por una fase de análisis de iniciativas, en las que se filtran las ideas o propuestas y se seleccionan aquellas que estén alineadas a la estrategia de la entidad. Es importante que la evaluación o participación del área de seguridad de la información, inicie desde el momento en que la iniciativa es aprobada o sea antes incluso de que sea convertido en proyecto, para incorporar los controles de seguridad requeridos para proteger la información.

#### **NIVELES DE MADUREZ:**

1. **INCIPIENTE:** Las nuevas iniciativas y proyectos son desarrollados sin la participación del área de seguridad en ninguna de las fases del proyecto.
2. **BAJO:** Las nuevas iniciativas y proyectos involucran al área de seguridad únicamente en la fase de implementación. La participación del área de Seguridad, no se realiza de forma metodológica, solamente se participa en algunos proyectos.
3. **MEDIO:** Las nuevas iniciativas y proyectos involucran al área de seguridad únicamente en la fase de implementación de forma metodológica, siempre se revisa la seguridad del servicio o producto antes de ser implementado en producción.
4. **ALTO:** Por normativa y conforme al proceso de desarrollo de proyectos, **toda nueva iniciativa o proyecto basado en tecnología**<sup>9</sup>, requiere de apoyo del área de seguridad, quien valida los requerimientos y apoya en la definición del diseño de la solución. Además el proyecto incluye una fase de revisión del diseño de la aplicación, servicio o tecnología previa a la fase de implementación.
5. **ÓPTIMO:** Por normativa y conforme al proceso de desarrollo de proyectos, **toda nueva iniciativa o proyecto de la entidad**<sup>10</sup>, cuenta con una valoración de riesgos y requiere de apoyo del personal de seguridad de la información, quien valida los requerimientos y apoya en la definición del diseño de la solución. Además el proyecto incluye una fase de revisión del diseño de la aplicación, servicio o tecnología previa a la fase de implementación.

## **FACTOR 12. DISEÑO DE SEGURIDAD DE RED**

Las aplicaciones y servicios basados en tecnología utilizan un elemento común que es indispensable para su funcionamiento, la red de comunicación, la cual se encarga de brindar el transporte de los datos entre los diferentes segmentos de red y para las diferentes aplicaciones.

---

<sup>9</sup> A este nivel de madurez, al menos los proyectos basados en tecnología deben requerir el involucramiento del área de seguridad.

<sup>10</sup> A este nivel de madurez, cualquier proyecto, sea esté basado o no en tecnología, debería requerir el involucramiento del área de seguridad, esto por cuanto aunque no esté basado en tecnología muy seguramente si hará uso de la información que es propiedad o es custodiada por la entidad.

La red se convierte en uno de los elementos principales de la plataforma tecnológica y requiere de un diseño, que defina los controles a utilizar para brindar seguridad a la información y a las aplicaciones o servicios soportados.

Un diseño de red debe considerar los diferentes escenarios, por ejemplo, conexiones internas, conexiones por Internet, conexiones por Extranet, conexiones inalámbricas, accesos remotos, etc, los diferentes tipos de usuarios, como por ejemplo: usuarios internos, clientes, proveedores, visitantes, socios de negocio, entes reguladores, etc, tipos de aplicaciones o servicios, por ejemplo, aplicaciones en n capas, aplicaciones web, aplicaciones transaccionales, aplicaciones móviles (apps), ATMs, bases de datos, sistemas de administración, de monitoreo, etc y definir zonas de seguridad y controles de seguridad de red entre zonas para los diferentes escenarios o usuarios.

El diseño de seguridad de red, permite definir de forma previa los controles de seguridad requeridos para facilitar la comunicación entre los diferentes elementos de la plataforma tecnológica, de manera que cuando se desea agregar un nuevo elemento a la plataforma y dependiendo del tipo de elemento, por ejemplo si es un nuevo servidor web para clientes que acceden por Internet, ya se cuenta con una definición de los controles de seguridad de red, definidos para ese elemento, facilitando y asegurando la integración de nuevos elementos a la plataforma tecnológica.

#### **NIVELES DE MADUREZ:**

- 1. INCIPIENTE:** No se cuenta con un diseño de seguridad de red.
- 2. BAJO:** Se cuenta con un diseño de seguridad de red en donde se diagraman los principales elementos de la plataforma tecnológica<sup>11</sup>, pero no existe una descripción que complemente esa topología y esta no se encuentra alineada al marco normativo definido. Además las áreas involucradas no lo conocen o no se apegan a lo definido y no existe una verificación de su implementación.
- 3. MEDIO:** Se cuenta con un diseño de seguridad de red en donde se diagraman los principales elementos de la plataforma tecnológica, existe una descripción que complementa el diseño, pero no se encuentra alineada al marco normativo definido. Las áreas involucradas no lo conocen o no se apegan a lo definido y no existe una verificación de su implementación.

---

<sup>11</sup> Entiéndase "Plataforma Tecnológica" por los elementos de hardware y software que soportan los servicios basados en tecnología.

4. **ALTO:** Se cuenta con un diseño de seguridad en donde se diagraman los principales elementos de la plataforma tecnológica, existe una descripción que complementa esa topología en donde se definen escenarios, tipos de usuarios, tipos de aplicaciones o servicios, zonas y controles de seguridad entre zonas, el diseño se encuentra alineado al marco normativo definido. Las áreas involucradas conocen el diseño pero no existe una verificación de su implementación.
5. **ÓPTIMO:** Se cuenta con un diseño de seguridad en donde se diagraman los principales elementos de la plataforma tecnológica, existe una descripción que complementa esa topología en donde se definen escenarios, tipos de usuarios, tipos de aplicaciones o servicios, zonas y controles de seguridad entre zonas, el diseño se encuentra alineado al marco normativo definido. Las áreas involucradas conocen y se apegan al diseño definido y existe una verificación de su implementación.

## FACTOR 13. CONTROL DE LA PLATAFORMA Y CONTROL DE CAMBIOS

En seguridad existe un principio, no es posible asegurar lo que no se conoce, por esa razón para poder asegurar la plataforma tecnológica, es necesario conocerla y procurar que esta se mantenga debidamente actualizada y controlada.

Existen plataformas tecnológicas muy complejas y parte del conocimiento de la plataforma ayuda a identificar áreas que podrían simplificarse o normalizarse, es más simple asegurar una plataforma que utiliza solamente un sistema operativo, que una que utiliza múltiples y si además existen múltiples versiones y algunas de esas versiones ya no son soportadas por los fabricantes, esto incrementa la complejidad de la administración y de su aseguramiento.

Es indispensable entonces tener claridad sobre los diferentes elementos que conforman la plataforma, debe existir un proceso formal para agregar, modificar o eliminar elementos de la plataforma, de forma que tengamos control de su estado actual.

Para aspectos de seguridad es indispensable tener control del nivel de obsolescencia tecnológica de los diferentes elementos de la plataforma tecnológica.

La obsolescencia tecnológica debe diferenciarse de la simple obsolescencia en que, para algunas empresas un elemento tecnológico no es obsoleto si cumple con su función, pero en términos de seguridad, la obsolescencia tecnológica está en función de otros factores como la existencia de soporte de parte del fabricante, entre otros factores.

## NIVELES DE MADUREZ:

1. **INCIPIENTE:** No se han definido guías de aseguramiento<sup>12</sup> para cada elemento de la plataforma, no existe un inventario de elementos de la plataforma tecnológica y no existe un proceso formal para agregar, eliminar o modificar elementos de la plataforma tecnológica.
2. **BAJO:** Se han definido guías de aseguramiento para cada elemento de la plataforma, no existe un inventario de elementos de la plataforma tecnológica y no existe un proceso formal para agregar, eliminar o modificar elementos de la plataforma tecnológica.
3. **MEDIO:** Se han definido guías de aseguramiento para cada elemento de la plataforma y existe un inventario manual o automático de elementos de la plataforma tecnológica. No existe un proceso formal para agregar, eliminar o modificar elementos de la plataforma tecnológica, ni verificación de cumplimiento de las guías de aseguramiento, ni análisis de la información del inventario.
4. **ALTO:** Se han definido guías de aseguramiento para cada elemento de la plataforma, existe un inventario automático de elementos de la plataforma tecnológica, existe un proceso formal para agregar, eliminar o modificar elementos de la plataforma tecnológica. El proceso incluye una valoración de riesgos del cambio a realizar y medidas de contingencia. Se realiza verificación de cumplimiento de las guías de aseguramiento y análisis de la información del inventario. Como parte del análisis se genera un informe con los hechos más relevantes en términos de seguridad, incluyendo aspectos como el de obsolescencia tecnológica.
5. **ÓPTIMO:** Se han definido guías y plantillas<sup>13</sup> de aseguramiento para cada elemento de la plataforma, existe un inventario automático de elementos de la plataforma tecnológica, existe un proceso formal para agregar, eliminar o modificar elementos de la plataforma tecnológica. El proceso incluye una valoración de riesgos del cambio a realizar y medidas de contingencia. Además existe un sistema que identifica y alerta o genera reportes sobre los elementos que no cumplen con las guías de aseguramiento. Se realiza verificación de cumplimiento de las guías de aseguramiento y análisis de la información del inventario. Como parte del análisis se genera un informe con los hechos más relevantes en términos de seguridad, incluyendo aspectos como el de obsolescencia tecnológica. Cualquier cambio en la plataforma es actualizado en el inventario y notificado automáticamente al área de Seguridad.

---

<sup>12</sup> Las guías de aseguramiento definen parámetros o controles que refuerzan la seguridad de los diferentes elementos.

<sup>13</sup> Las plantillas toman los parámetros o controles definidos en las guías y automatizan su implementación.

## FACTOR 14. ANÁLISIS DE VULNERABILIDADES Y PRUEBAS DE PENETRACIÓN

El nivel de seguridad se ve afectado directamente por la cantidad de vulnerabilidades existentes, en el tanto una plataforma no muestre vulnerabilidades conocidas, será mucho más difícil para un atacante lograr tener acceso a la información y sistemas de la empresa.

Es importante considerar que una plataforma que no tiene vulnerabilidades hoy, podría tener vulnerabilidades serias mañana, por esa razón el ejecutar análisis de vulnerabilidad periódicamente permite corregir de forma diligente las fallas que se vayan presentando. Además, las pruebas de penetración permiten validar que las vulnerabilidades conocidas y otras brechas que pueden ser explotadas por los atacantes están debidamente controladas por la empresa.

La diferencia entre los análisis de vulnerabilidad y las pruebas de penetración, radica en que los análisis de vulnerabilidad se ejecutan de forma automática por herramientas que validan la existencia de vulnerabilidades conocidas que son almacenadas en una base de datos, las pruebas de penetración ejecutan un proceso que combina herramientas con metodologías ejecutadas por una o un grupo de personas y que tratan de vulnerar la seguridad de una entidad.

Un análisis de vulnerabilidad o una prueba de penetración puede ser ejecutada desde el interno o externo de la red, de la entidad, la diferencia radica en que usualmente desde el exterior se aplican controles más rigurosos de seguridad y no se tiene acceso a elementos de la plataforma que si se logran acceder desde el interno.

Tanto los análisis de vulnerabilidad como las pruebas de penetración pueden ser ejecutadas por personal interno, personal externo o ambos. El utilizar terceros para realizar las pruebas de vulnerabilidad o de penetración, además de servir como complemento a las pruebas realizadas por personal interno, ofrecen imparcialidad y permiten validar el trabajo de aseguramiento que realiza el personal interno, es por eso que en niveles altos de madurez, se requiere la ejecución de análisis de vulnerabilidad y pruebas de penetración realizados por terceros.

### NIVELES DE MADUREZ:

1. **INCIPIENTE:** No se realizan análisis de vulnerabilidades internas ni externas. No se realizan pruebas de penetración externas ni internas.
2. **BAJO** El personal interno realiza análisis de vulnerabilidades externas al menos una vez al mes y existe un proceso de atención y seguimiento a las vulnerabilidades. No existe un contrato con terceros para la realización de análisis de vulnerabilidades, ni pruebas de penetración.

3. **MEDIO:** El personal interno realiza análisis de vulnerabilidades externas e internas, al menos una vez al mes y existe un proceso de atención y seguimiento a las vulnerabilidades. No existe un contrato con terceros para la realización de análisis de vulnerabilidades, ni pruebas de penetración.
4. **ALTO:** El personal interno realiza análisis de vulnerabilidades externas e internas al menos una vez al mes. Se cuenta con contrato para que personal externo realice análisis de vulnerabilidades externas al menos una vez al mes y pruebas de penetración externa al menos cada 6 meses, tanto a la red alámbrica como inalámbrica. Existe un proceso de atención y seguimiento a las vulnerabilidades.
5. **ÓPTIMO:** El personal interno realiza análisis de vulnerabilidades externas e internas al menos una vez a la semana. Se cuenta con contrato para que personal externo realice análisis de vulnerabilidades externas al menos una vez a la semana, pruebas de penetración externas y pruebas de penetración internas, al menos cada 6 meses, tanto a la red alámbrica como inalámbrica. Personal interno o externo realiza análisis de vulnerabilidad de código a las aplicaciones accesibles desde Internet, al menos cada 6 meses. Se ejecutan pruebas de vulnerabilidad a todo nuevo servidor o sistema de forma previa a su implementación en producción. Existe un proceso de atención y seguimiento a las vulnerabilidades.

## FACTOR 15. SISTEMA DE REGISTRO, MONITOREO Y ALARMA DE EVENTOS

Algunos ataques que logran burlar los controles de seguridad, podrían ser detectados a partir del monitoreo y análisis del comportamiento inusual en la plataforma de la red, pero esto es imposible de lograrlo si no se cuenta con herramientas que puedan recolectar, almacenar, consolidar y analizar los eventos (“logs”) que se generan en los diferentes elementos de la plataforma tecnológica y a partir de su “inteligencia” identificar situaciones que son inusuales y que podrían alertar sobre un eventual ataque o incidente de seguridad.

Es necesario diferenciar entre dos tipos de registros de eventos (“logs”), aquellos que se realizan en los equipos o elementos de la plataforma y que podrían evidenciar un ataque a la plataforma con el objetivo de acceder, robar o destruir la información o de afectar los servicios; y los registros de eventos (“logs”) transaccionales, generados directamente por las aplicaciones de usuario final, en las que a partir de un comportamiento inusual como podría ser el origen de una transacción, el monto, el lugar, la hora u otros elementos, podría identificarse una transacción fraudulenta.

Es usual que existan sistemas separados para realizar el registro y análisis de los dos tipos de registros y es posible que existan soluciones que puedan analizar ambos, pero en todo caso, la única manera de realizar un análisis de esta información es con el uso de herramientas

especializadas. Es prácticamente imposible y poco práctico realizar una revisión manual de este tipo de registros de eventos (“logs”).

El almacenamiento centralizado es conveniente tanto para los registros (logs) de equipos, como para aplicaciones, porque permite hacer un análisis integral de todos los eventos. Es usual que existan dos almacenamientos centrales, uno para los elementos o dispositivos y otro para las aplicaciones o servicios. Para este tipo de almacenamientos utilizar tecnología conocida como WORM (Write Once Read Many) o tecnología de solo lectura es conveniente sobre todo para análisis de incidentes que requieren garantizar que nadie puede modificar los registros del sistema.

#### **NIVELES DE MADUREZ:**

1. **INCIPIENTE:** No se almacenan los registros de eventos (logs) de ningún equipo ni aplicación, ni se almacenan de forma centralizada.
2. **BAJO:** Se almacenan los registros de eventos de algunos equipos y aplicaciones, pero no se realiza de forma centralizada, ni son analizados en tiempo real.
3. **MEDIO:** Se almacenan de forma centralizada los registros de eventos de los equipos y aplicaciones que soportan los servicios críticos, pero no se utiliza tecnología de solo lectura, ni son analizados en tiempo real.
4. **ALTO:** Se almacenan de forma centralizada los registros de eventos de los equipos y aplicaciones que soportan los servicios críticos y son analizados en tiempo real<sup>14</sup>. Pero no se utiliza tecnología de solamente lectura.
5. **ÓPTIMO:** Se almacenan de forma centralizada los registros de eventos de los equipos y aplicaciones que soportan los servicios críticos, se utiliza tecnología de solamente lectura, son analizados en tiempo real y se cuenta con una tecnología que correlaciona y genera alertas de situaciones catalogadas como inusuales, tanto a nivel de equipos, como de sistemas, aunque eventualmente con sistemas independientes.

## **FACTOR 16. CONTROL ACCESO LÓGICO (AUTENTICACIÓN)**

El control de acceso de los usuarios es un control indispensable de seguridad, que permite autenticar a los usuarios, permitiendo el ingreso a elementos de la plataforma tecnológica (redes, equipos, aplicaciones, sistemas, etc), solamente a aquellos debidamente autorizados.

---

<sup>14</sup> Para el análisis en tiempo real, es usual que los eventos de equipos sean analizados por soluciones conocidas como SIEM o similares y para los eventos en las aplicaciones es usual el uso de sistemas tipo antifraude.

El control de acceso lógico, se enfoca en la autenticación de los usuarios internos o externos (clientes) y lo que procura es validar que el usuario es quien dice ser, este proceso es diferente a la autorización, que es el proceso que se ejecuta inmediatamente después a la autenticación y que otorga los permisos de acceso a la información, sistemas u otros elementos de acuerdo al perfil o rol del usuario.

Es importante diferenciar entre el acceso de los usuarios y el acceso de los equipos. Para autenticar al usuario usualmente se utilizan sistemas de uno o más factores; Para autenticar a un equipo usualmente se utilizan sistemas del tipo “Network Authentication Control” (NAC), sistemas que generan una “huella” o valor que identifica inequívocamente al equipo que se conecta, certificados digitales u otros controles.

#### **NIVELES DE MADUREZ:**

1. **INCIPIENTE:** Se autentica el acceso de los usuarios a la red utilizando un solo factor de autenticación, no se autentica el acceso a las aplicaciones.
2. **BAJO:** Se autentica el acceso de los usuarios a la red utilizando un solo factor de autenticación, además se autentica el acceso a las aplicaciones, pero no se utiliza un sistema centralizado de autenticación.
3. **MEDIO:** Se autentica el acceso de los usuarios a la red utilizando un solo factor de autenticación, además se autentica el acceso a las aplicaciones utilizando un sistema centralizado de autenticación.
4. **ALTO:** Se autentica el acceso de los usuarios a la red utilizando un solo factor de autenticación, además se autentica el acceso a las aplicaciones utilizando un sistema centralizado de autenticación. Se utiliza un segundo factor de autenticación para aplicaciones de banca por Internet y acceso remoto de usuarios para soporte técnico, desarrollo de software, control de calidad de software, teletrabajo o usuarios móviles.
5. **ÓPTIMO:** Se autentica el acceso de los usuarios y de los equipos a la red utilizando uno o más factores de autenticación, además se autentica el acceso a las aplicaciones utilizando un sistema centralizado de autenticación. Se utiliza un segundo o tercer factor de autenticación para aplicaciones de banca por Internet, para aplicaciones catalogadas como críticas y para el acceso remoto de usuarios para soporte técnico, desarrollo de software, control de calidad de software, teletrabajo o usuarios móviles.

## **FACTOR 17. ADMINISTRACION DE IDENTIDAD**

En términos de control de acceso a la información es indispensable cumplir con dos principios básicos, “menor privilegio” y “necesidad de conocer”. Los usuarios deben tener el menor privilegio requerido para el cumplimiento de las funciones de su puesto y deben acceder a la información que sea estrictamente necesaria.

Un sistema de administración de la identidad permite asignar los permisos mínimos requeridos basado en roles o perfiles, de forma que cuando un usuario cambia de rol, de perfil o es desautorizado, sus permisos son ajustados de acuerdo a su nuevo rol, perfil o estado.

Los sistemas de administración de identidad, usualmente incluyen módulos o herramientas de autogestión, que además de brindar facilidad al usuario, mejoran la seguridad porque elimina la dificultad de identificar al usuario que requiere ser desbloqueado, quien usualmente se comunica telefónicamente al centro de soporte de usuarios. Este módulo podría ser implementado de forma independiente al sistema de administración de la identidad, pero usualmente es parte de los sistemas de administración de la identidad.

#### **NIVELES DE MADUREZ:**

1. **INCIPIENTE:** Los permisos en las aplicaciones son asignados a los usuarios en cada sistema y no a roles o perfiles.
2. **BAJO:** Los permisos en las aplicaciones son asignados a perfiles o roles, no a usuarios, en cada sistema, no existe una gestión centralizada.
3. **MEDIO:** Los permisos en las aplicaciones son asignados a perfiles o roles, no a usuarios. Existe una gestión centralizada, al menos para los sistemas catalogados como críticos.
4. **ALTO:** Los permisos en las aplicaciones son asignados a perfiles o roles, no a usuarios. Existe un sistema centralizado, al menos para los sistemas críticos, el sistema permite autogestión de usuarios, de forma que en caso de bloqueo, el mismo usuario pueda desbloquearse y existe una revisión periódica de usuarios habilitados al menos en los sistemas catalogados como críticos.
5. **ÓPTIMO:** Se utiliza un sistema de administración de identidad centralizado, las aplicaciones autentican con este sistema, en donde se definen macro perfiles o roles por puesto de trabajo, los perfiles o roles son modificados automáticamente con un cambio de puesto o eliminados en caso de una salida. Los usuarios pueden autogestionar su cuenta y en caso de requerirse un proceso de autorización en la gestión de los roles o perfiles, este es parte de un flujo de trabajo que automatiza el proceso general de gestión de identidades.

## FACTOR 18. CONTROLES EN EL DESARROLLO DE APLICACIONES Y APPS

Uno de los mayores vectores de ataque a la seguridad de las empresas son las aplicaciones. Los atacantes tratan de identificar y explotar vulnerabilidades en el código de las aplicaciones o en el manejo de los datos que se realiza como parte del proceso de desarrollo. Además existe una gran proliferación de aplicaciones para dispositivos móviles conocidas como APPs, algunas de ellas incluso contratadas por áreas comerciales, sin la validación de adecuados controles de seguridad.

Si bien es cierto existen controles a nivel de diseño que deben ser válidos, es importante que se revise la seguridad de toda nueva aplicación que se vaya a colocar en producción, independientemente de si la aplicación fue desarrollada por personal interno, por personal externo o fue adquirida.

Las aplicaciones deben pasar por los procesos de desarrollo, pruebas e integración para finalmente ser incorporadas al ambiente de producción. En términos de seguridad es indispensable que existan ambientes aislados y controlados, para cada una de esas fases, el mezclar los ambientes podría ocasionar fisuras en la seguridad de las aplicaciones o de la información.

Precisamente uno de los mayores errores al mezclar ambientes, es el utilizar datos de producción en el ambiente de desarrollo y pruebas, para evitar el uso de datos reales o de producción, se deben utilizar herramientas o métodos de ofuscamiento que se encargan de modificar los datos para que sean datos válidos, pero no reales.

### NIVELES DE MADUREZ:

1. **INCIPIENTE:** No existe una guía de aseguramiento de aplicaciones y Apps, no existe una separación de ambientes, los desarrolladores utilizan sus equipos, tienen acceso a producción y no existe control de versiones. Se utilizan datos de producción o sea reales en el desarrollo y prueba de los sistemas.
2. **BAJO:** No existe una guía de aseguramiento de aplicaciones y Apps, no existe una separación de ambientes, se desarrolla en servidores y no en estaciones, los desarrolladores tienen acceso a producción, no existe control de versiones. Se utilizan datos de producción o sea reales en el desarrollo y prueba de los sistemas.
3. **MEDIO:** Existe una guía de aseguramiento de aplicaciones y Apps, pero no es validada. Existe una separación de ambientes, se desarrolla en servidores, no en estaciones, los desarrolladores tienen acceso a producción, existe control de versiones. Se utilizan datos de producción o sea reales en el desarrollo y prueba de los sistemas.

4. **ALTO:** Existe una guía de aseguramiento de aplicaciones y Apps y su cumplimiento es validado, antes de que éstas sean puestas en producción. Existe una separación de ambientes, se desarrolla en un ambiente aislado y controlado, existe control de versiones, los desarrolladores no tienen acceso a producción. No se utilizan datos de producción o sea reales en el desarrollo y prueba de los sistemas.
5. **ÓPTIMO:** Existe una guía de aseguramiento de aplicaciones y Apps y su cumplimiento es validado, antes de que estas sean puestas en producción. Existe una separación de ambientes, se desarrolla en un ambiente aislado y controlado, existe control de versiones, los desarrolladores no tienen acceso a producción y no se utilizan datos de producción o sea reales en el desarrollo y prueba de los sistemas. Como parte de las pruebas de los sistemas se ejecutan pruebas de seguridad del código, como un requisito para que la aplicación pueda ser colocada en producción.

## FACTOR 19. ADMINISTRACIÓN DE DISPOSITIVOS DE SEGURIDAD DE LA RED

Las redes interconectan usuarios, sistemas, bases de datos y otros elementos de la plataforma, es por eso que el contar con controles de seguridad a nivel de red es indispensable para la seguridad de la información, estos sistemas o controles de seguridad, han ido evolucionando y posiblemente seguirán evolucionando, brindando cada vez controles de seguridad con un mayor nivel de inteligencia.

Si bien es cierto, el perímetro de las redes ha ido poco a poco desapareciendo con la aparición de las redes inalámbricas, usuarios móviles, integración con otras redes o servicios tercerizados (en la “nube”), los controles de red siguen siendo de gran utilidad para analizar y validar el tráfico o comunicación. El tráfico encriptado para aplicaciones utilizando SSL, TLS u otro protocolo, debe ser revisado por los equipos de seguridad, caso contrario no es posible identificar ataques realizados a través de ese tipo de conexiones. Los ataques más efectivos se realizan tomando control de equipos internos, por esa razón es indispensable el análisis del tráfico tanto entrante como saliente.

A pesar de que como parte del monitoreo de seguridad, se utilizan herramientas “inteligentes” para analizar los registros (“logs”) de los dispositivos, para los elementos de seguridad de la red, es conveniente realizar un análisis, que permita identificar situaciones inusuales que aunque eventualmente puedan ser bloqueadas por los equipos de seguridad, ameritan ser identificadas y tomar acciones adicionales; por ejemplo un eventual ataque persistente desde un origen específico, el cual podría eventualmente ser incluido en una lista negra o activar algún protocolo específico de atención.

Es importante considerar la creciente tendencia a utilizar la virtualización de la plataforma tecnológica. En ambientes virtuales el concepto de pasar el tráfico por un equipo de firewall aplica, ya sea redirigiendo el tráfico a equipos físicos o utilizando tecnologías de firewall para ambientes virtuales. En caso de utilizar tecnologías de este tipo es conveniente utilizar el concepto de micro-segmentación para ofrecer un mayor nivel de seguridad.

Actualmente es usual la implementación de redes inalámbricas en las entidades y es por eso indispensable que esas redes sean aseguradas para evitar que sean utilizadas por terceros para lograr acceso no autorizado y poner en riesgo la información y los servicios soportados por la plataforma tecnológica.

#### **NIVELES DE MADUREZ:**

- 1. INCIPIENTE:** Se cuenta con equipos de seguridad perimetral (FW), para controlar y proteger el tráfico entre redes externas e internas, pero, no se utilizan para controlar DMZs internas. No se cuenta con equipos de protección de intrusos (IPS), no existe un proceso periódico de administración, que mantenga los equipos actualizados y no se analiza la información generada por estos. Si existe red inalámbrica, cualquiera se puede conectar, no se realiza autenticación de equipo, ni de usuario. Se realiza cifrado del tráfico de la red, utilizando algoritmos catalogados<sup>15</sup> como no seguros.
- 2. BAJO:** Se cuenta con equipos de seguridad perimetral (FW) para controlar y proteger el tráfico entre redes externas e internas, se utilizan DMZs internas; no se cuenta con equipos de protección de intrusos (IPS), no existe un proceso periódico de administración, que mantenga los equipos actualizados ni se realiza un análisis de la información generada por estos. Si existe red inalámbrica, se realiza autenticación de la conexión utilizando una clave de acceso fija (Técnica conocida como pre-share key), no se autentica el equipo ni al usuario. Se realiza cifrado del tráfico de la red, utilizando algoritmos catalogados como no seguros.
- 3. MEDIO:** Se cuenta con equipos de seguridad perimetral (FW) para controlar y proteger el tráfico entre redes externas e internas, se utilizan DMZs internas y las aplicaciones se separan al menos en 3 capas, que requieren pasar por el equipo de firewall para comunicarse entre ellas. Se cuenta con equipos de protección de intrusos (IPS) que controlan únicamente el tráfico desde y hacia el enlace de Internet. No existe un proceso periódico de administración, que mantenga los equipos actualizados ni se realiza un análisis de la información generada por estos. Existe red inalámbrica y se realiza autenticación de equipo utilizando una clave de acceso fija (Técnica conocida como pre-share key), se registra la dirección física del equipo autorizado y se autentica al usuario utilizando usuario y clave. Se realiza cifrado del tráfico de la red, utilizando algoritmos catalogados como seguros.

---

<sup>15</sup> Al indicar catalogados se refiere a la comunidad, existen muchas entidades encargadas de analizar la seguridad de los protocolos, algoritmos y otros elementos y cuando se identifica que no es seguro se publica en diferentes medios.

4. **ALTO:** Se cuenta con equipos de seguridad perimetral (FW) para controlar y proteger el tráfico entre redes externas e internas, se utilizan DMZs internas y las aplicaciones se separan al menos en 3 capas, que requieren pasar por el equipo de firewall para comunicarse entre ellas. Se cuenta con equipos de protección de intrusos (IPS) que controlan al menos el tráfico desde y hacia el enlace de Internet, Extranet e Intranet. Existe un proceso periódico de administración, que mantiene los equipos actualizados y se realiza un análisis de la información generada por estos. Existe red inalámbrica, se realiza autenticación de equipo utilizando un certificado digital, se autentica al usuario utilizando autenticación integrada o sea utilizando las credenciales del usuario que ingresó al equipo, sin necesidad de solicitarlas nuevamente. Se realiza cifrado del tráfico de la red, utilizando algoritmos catalogados como seguros.
  
5. **ÓPTIMO:** Se cuenta con equipos de seguridad perimetral (FW-IPS) de última tecnología <sup>16</sup> para controlar y proteger el tráfico entre redes externas e internas (Internet, Extranet, Intranet y los diferentes segmentos de red internos), se utilizan DMZs internas y las aplicaciones se separan al menos en 3 capas, que requieren pasar por el equipo de firewall e IPS para comunicarse entre ellas. Existe un proceso periódico de administración, que mantiene los equipos actualizados y se realiza un análisis de la información generada por estos. Además los equipos permiten analizar el tráfico encriptado tanto entrante como saliente y generar alertas automáticas de situaciones consideradas como inusuales. Existe red inalámbrica, se realiza autenticación de equipo utilizando un certificado digital, se autentica al usuario utilizando autenticación integrada o sea utilizando las credenciales del usuario que ingresó al equipo, sin necesidad de solicitarlas nuevamente. Se realiza cifrado del tráfico de la red, utilizando algoritmos catalogados como seguros y se utiliza cifrado para el proceso de autenticación. Se cuenta con un sistema de IPS inalámbrico (WIPS), que detecta y controla ataques realizados contra la red inalámbrica.

## FACTOR 20. CONTROL DE MALWARE

El malware es uno de los elementos más utilizado para lograr vulnerar la seguridad de una empresa. Los sistemas antimalware son cada vez más inteligentes, pero de igual forma el malware evoluciona y han existido casos de malware que logra instalarse en empresas sin ser detectado por meses o años, por esa razón es indispensable que las empresas cuenten con sistemas de detección y protección contra malware.

A pesar de que los sistemas antimalware están diseñados para actualizarse de forma automática, es indispensable monitorear el nivel de actualización, tanto de la versión del software o aplicación como de la base de datos que almacena los malware conocidos, esto es denominado en el medio

---

<sup>16</sup> La última tecnología en plataformas de seguridad agrega inteligencia y funcionalidad que permite disminuir el nivel de riesgo, en este momento al hablar de última tecnología en herramientas de FW-IPS debe considerarse aquella conocida como de nueva generación (NG), sin embargo esto podría eventualmente cambiar.

como “firmas” y consisten en patrones que identifican a un malware específico y aunque la gran cantidad de variantes y la gran cantidad de aparición de nuevos malware requiere de tecnologías más inteligentes para identificar un malware, las “firmas”, siguen siendo utilizadas como complemento a otras tecnologías que permiten identificar un malware a partir de su comportamiento.

Es importante considerar que un único equipo que sea contagiado por un malware, podría afectar la seguridad de toda la plataforma tecnológica, el ideal es que todos los equipos se mantengan debidamente actualizados, pero entre menos equipos se encuentren des-actualizados, menor será la probabilidad de que la entidad se vea afectada.

Por lo anterior la cobertura, entendida como la cantidad de equipos estaciones y servidores que cuentan con el sistema antimalware y el nivel de actualización, entendido como la cantidad de equipos que se encuentran actualizados con la última base de datos y versión del sistema anti-malware, son datos que deben monitorearse y procurar, mantener el mayor nivel de cobertura y de actualización.

#### **NIVELES DE MADUREZ:**

- 1. INCIPIENTE:** Las estaciones de los usuarios cuentan con un sistema antimalware, no así los servidores, no existe un control antimalware para correo y navegación, ni existe un proceso de monitoreo de actualización y efectividad del sistema antimalware.
- 2. BAJO:** Las estaciones de los usuarios cuentan con un sistema central antimalware, no así los servidores, no existe un control antimalware para correo y navegación. Existe un proceso de monitoreo de actualización y efectividad del sistema antimalware.
- 3. MEDIO:** Las estaciones de los usuarios y servidores cuentan con un sistema central antimalware, no existe un control antimalware para correo y navegación. Existe un proceso de monitoreo de actualización y efectividad del sistema antimalware.
- 4. ALTO:** Las estaciones de los usuarios y servidores cuentan con un sistema central antimalware, existe un control antimalware para correo y navegación. Existe un proceso de monitoreo de actualización y efectividad del sistema antimalware, se ha definido un indicador de seguridad, relacionado al antimalware, el cual requiere de un nivel ideal de cobertura y actualización de los equipos.
- 5. ÓPTIMO:** Las estaciones de los usuarios, servidores y equipos móviles cuentan con un sistema central antimalware, existe un control antimalware para correo y navegación. Existe un proceso de monitoreo de actualización y efectividad del sistema antimalware, se ha definido un indicador de seguridad, relacionado al antimalware, el cual requiere de un nivel ideal de cobertura y actualización de los equipos, adicionalmente se cuenta

con herramientas que permiten identificar el origen (equipos cero<sup>17</sup>) y medio o forma de una eventual infección de malware.

## FACTOR 21. SEGURIDAD DE USUARIO FINAL

Existen dos tipos de usuario final, los usuarios internos que forman parte de las diferentes entidades, usualmente utilizan equipos provistos y controlados por la entidad y los usuarios externos o clientes, que utilizan equipos personales o de acceso público que no son controlados por la entidad. Adicionalmente existe una tendencia a que los usuarios internos utilicen equipos que son de uso personal (“BYOD”), no controlados por la entidad, para actividades empresariales.

Existen usuarios con altos niveles de conciencia y con muy buenos hábitos con respecto a la seguridad de la información y existen otros que no cumplen con las recomendaciones de seguridad, poniendo en riesgo tanto su equipo como las redes o servicios que utiliza. Es por esta razón que el usuario final es considerado como el eslabón más débil de la cadena y se ha convertido en el vector de ataque más utilizado para vulnerar la seguridad de una entidad.

El tema de concientización se desarrolla como un factor adicional de evaluación, en este apartado se incluyen los controles que pueden ser automatizados para minimizar el riesgo ocasionado por los usuarios finales.

No todas las actividades del usuario pueden ser controladas, sin embargo, entre más control se tenga del usuario, menor es el riesgo, en ese sentido es importante limitar los permisos del usuario, el software utilizado, el acceso a dispositivos externos, los sitios web a los que tiene acceso, las redes a las que se conecta y otros controles orientados a mantener el equipo del usuario libre de vulnerabilidades o en su defecto, la implementación de ambientes aislados de trabajo, que permitan separar el ambiente personal del laboral, manteniendo un ambiente laboral controlado. Considerando que la entidad tiene mayor control sobre los usuarios internos y que para los usuarios externos se utiliza otro tipo de controles, diferentes a los requeridos en este factor, este apartado considera únicamente a los usuarios internos.

### NIVELES DE MADUREZ:

1. **INCIPIENTE:** Las estaciones de los usuarios internos son instaladas de fábrica, no se aplican guías de aseguramiento, no existe control de las aplicaciones instaladas, no se aplican parches de seguridad, no existe control de la navegación web del usuario, no existe un sistema de control de dispositivos usb, no existe control de las redes a las

---

<sup>17</sup> Equipo cero es el equipo que inició un contagio dentro de la red de la entidad.

que el usuario se puede conectar y todos los usuarios internos son administradores de sus equipos.

2. **BAJO** Las estaciones de los usuarios internos son instaladas y configuradas conforme a las guías de aseguramiento, no existe control de las aplicaciones instaladas, no se aplican parches de seguridad, no existe control de la navegación web del usuario, no existe un sistema de control de dispositivos usb, no existe control de las redes a las que el usuario se puede conectar y todos los usuarios internos son administradores de sus equipos.
3. **MEDIO:** Las estaciones de los usuarios internos son instaladas y configuradas conforme a las guías de aseguramiento de forma automática, ya sea utilizando imágenes o plantillas, se instalan solamente las aplicaciones requeridas por el usuario, se aplican parches de seguridad, existe control de a que sitios web puede navegar el usuario, no existe un sistema de control de dispositivos usb, no existe control de las redes a las que el usuario se puede conectar. Los usuarios internos no son administradores de sus equipos, salvo excepciones definidas.
4. **ALTO:** Las estaciones de los usuarios internos son instaladas y configuradas conforme a las guías de aseguramiento de forma automática, ya sea utilizando imágenes o plantillas, se instalan solamente las aplicaciones requeridas por el usuario conforme a su perfil o rol, se aplican parches de seguridad, existe control de a que sitios web puede navegar el usuario, existe un sistema de control de dispositivos usb, existe control de las redes a las que el usuario se puede conectar. Los usuarios internos no son administradores de sus equipos, salvo excepciones definidas. Toda instalación o cambio de configuración en las estaciones es registrado en la bitácora del equipo y existe un sistema que genera alarmas al administrador en caso de nuevas instalaciones en las estaciones.
5. **ÓPTIMO:** Las estaciones de los usuarios internos son instaladas y configuradas conforme a las guías de aseguramiento de forma automática, ya sea utilizando imágenes o plantillas, se instalan solamente las aplicaciones requeridas por el usuario conforme a su perfil o rol, se aplican parches de seguridad, existe control de a que sitios web puede navegar el usuario, existe un sistema de control de dispositivos usb, existe control de las redes a las que el usuario se puede conectar. Los usuarios internos no son administradores de sus equipos, salvo excepciones definidas. Los equipos utilizan un sistema que permite ejecutar únicamente las aplicaciones explícitamente permitidas, esto se conoce como listas blancas (White listing). Existe un sistema central de monitoreo que valida el nivel de cumplimiento y de riesgo de las estaciones de los usuarios. Toda instalación o cambio de configuración en las estaciones es registrado en la bitácora del equipo y es remitido además a un sistema centralizado de bitácora.

## FACTOR 22. CONTINUIDAD

Procurar la disponibilidad de la información es indispensable para garantizar el cumplimiento de los objetivos estratégicos de la entidad y la continuidad de los servicios ofrecidos a los clientes. La continuidad es un tema muy amplio que implica tanto aspectos tecnológicos como de negocio, en términos de seguridad la continuidad o disponibilidad de la información está muy relacionado a la afectación producto de un incidente de seguridad, sin embargo, cuando eventualmente se identifique un incidente de seguridad, en un nivel de madurez alto, ese incidente deberá atenderse de la misma forma en cómo se atiende cualquier otro incidente que afecte la operación del negocio.

Este modelo no profundiza en el tema de continuidad, pero al ser un tema de tanta relevancia se identifican los principales elementos que deben considerarse a nivel institucional para garantizar la continuidad de la operación.

### NIVELES DE MADUREZ:

- 1. INCIPIENTE:** Los centros de datos no cuentan con sistema de UPS (uninterruptible power supply), no se cuenta con planta generadora de energía, no se cuenta con sistema duplicado de aire acondicionado. No se han identificado los sistemas críticos para el negocio, no se cuenta con un plan de continuidad, no se cuenta con un centro alternativo de procesamiento.
- 2. BAJO:** Los centros de datos no cuentan con sistema de UPS (uninterruptible power supply), no se cuenta con planta generadora de energía, no se cuenta con sistema duplicado de aire acondicionado. No se han identificado los sistemas críticos para el negocio, no se cuenta con un plan de continuidad, no se cuenta con un centro alternativo de procesamiento.
- 3. MEDIO:** Los centros de datos cuentan con sistema de UPS (uninterruptible power supply), con planta generadora de energía, pero no cuentan con sistema duplicado de aire acondicionado. Se han identificado los sistemas críticos para el negocio, pero estos no son soportados por plataforma redundante a nivel de red, servidores y almacenamiento. No se cuenta con un plan de continuidad, no se cuenta con un centro alternativo de procesamiento.
- 4. ALTO:** Los centros de datos cuentan con sistema de UPS (uninterruptible power supply), con planta generadora de energía, con sistema duplicado de aire acondicionado, se realiza mantenimiento y pruebas periódicas del sistema de UPS, del generador de energía y de los sistemas de aire acondicionado. Se han identificado los sistemas críticos para el negocio y plataforma que los soporta es redundante a nivel de red, servidores y almacenamiento. Se cuenta con un plan de continuidad a nivel

tecnológico pero no a nivel de negocio, se cuenta con un centro alternativo de procesamiento, se realizan pruebas periódicas de continuidad.

- 5. ÓPTIMO:** Los centros de datos cuentan con sistema de UPS (uninterruptible power supply), con planta generadora de energía, con sistema duplicado de aire acondicionado, se realiza mantenimiento y pruebas periódicas del sistema de UPS, del generador de energía y de los sistemas de aire acondicionado. Se han identificado los sistemas críticos para el negocio y plataforma que los soporta es redundante a nivel de red, servidores y almacenamiento. Se cuenta con un plan de continuidad a nivel tecnológico y a nivel de negocio y considera a todas las áreas involucradas. Se cuenta con un centro alternativo de procesamiento ubicado en una zona de diferente impacto <sup>18</sup> al centro principal de datos. Se realizan pruebas periódicas de continuidad.

## FACTOR 23. ATENCIÓN DE INCIDENTES DE SEGURIDAD

Para poder atender un incidente de seguridad es indispensable estar preparado. Los controles preventivos se definen para evitar incidentes, pero en caso de que sucedan, se debe tener claridad sobre cómo atenderlos y minimizar su impacto, es por eso que debe existir una definición y organización orientada hacia los incidentes de seguridad.

Los incidentes de seguridad pueden ser causados por múltiples factores, pero lo importante es estar preparado para los incidentes más conocidos, para esto se debe contar con un inventario de incidentes conocidos, que aunque no hayan sucedido, permite definir protocolos o procedimientos específicos de cómo atenderlos.

Los incidentes de seguridad tienen un impacto directo en la continuidad del negocio y por tanto es importante que exista una atención integral del incidente, que involucre a todas las áreas interesadas, como podría ser el área de Capital Humano, el área de comunicación empresarial, el área legal y cualquier otra, según corresponda. Es por eso que en un nivel de madurez alto la atención de incidentes de seguridad se integran con el plan de continuidad empresarial, orientado a procurar la continuidad de los servicios, a minimizar los tiempos de fallas y en caso de una eventual caída, la recuperación más pronta del incidente.

---

<sup>18</sup> Entiéndase por zona de diferente impacto, una zona que no comparta los mismos riesgos de la zona en donde se ubica el centro principal de datos.

## **NIVELES DE MADUREZ:**

- 1. INCIPIENTE:** No existe una identificación de eventuales incidentes de seguridad, ni un procedimiento para su atención, estos se atienden cuando suceden y según sea el caso.
- 2. BAJO:** No existe una identificación de eventuales incidentes de seguridad, existe un procedimiento o protocolo de atención general, no específico para cada tipo de ataque, además, éste no se encuentra integrado al plan de continuidad de forma que involucre a todas las áreas relacionadas.
- 3. MEDIO:** Existe una identificación de eventuales incidentes de seguridad, existe un procedimiento o protocolo de atención general, no específico para cada tipo de ataque, éste no se encuentra integrado al plan de continuidad de forma que involucre a todas las áreas relacionadas.
- 4. ALTO:** Existe una identificación de eventuales incidentes de seguridad, existe un procedimiento o protocolo de atención específico para cada tipo de ataque, éste no se encuentra integrado al plan de continuidad de forma que involucre a todas las áreas relacionadas.
- 5. ÓPTIMO:** Existe una identificación de eventuales incidentes de seguridad, un procedimiento o protocolo de atención específico para cada tipo de ataque y éste se encuentra integrado al plan de continuidad de forma que involucra a todas las áreas relacionadas.

## **FACTOR 24. MONITOREO DE INDICADORES DE SEGURIDAD**

Las empresas implementan diferentes controles de seguridad, sin embargo, esos controles requieren ser monitoreados, para verificar constantemente su efectividad. Es por esto indispensable la definición de indicadores que permitan monitorear el nivel de seguridad y se tomen las acciones requeridas para mantenerse en un nivel óptimo y evitar niveles que impliquen una posición de riesgo para los servicios basados en tecnología.

Qué indicadores definir, es un tema que está en función de cada entidad, sin embargo, es usual definir indicadores en términos de cantidad de vulnerabilidades existentes, nivel de actualización de equipos (parcheo, versiones SO, antimalware), cantidad de malware detectados, cantidad de ataques recibidos, etc. Estas situaciones se dan constantemente pero las cantidades o niveles serán diferentes para cada entidad, es por eso importante que cada entidad determine la cantidad que se puede considerar como “usual” y que cantidad podría ser considerada “inusual”.

Al identificar las cantidades “usuales” e “inusuales” es posible definir niveles predefinidos de atención, o sea valores o rangos, con diferentes categorizaciones, como ideal, normal y alerta, y a partir de esos valores o rangos definir acciones a realizar para volver a la normalidad.

#### **NIVELES DE MADUREZ:**

1. **INCIPIENTE:** No se monitorea ningún control de seguridad y no existen una definición de indicadores con niveles predefinidos de atención.
2. **BAJO:** Se monitorean algunos controles de seguridad de forma aleatoria, sin un procedimiento definido, no existe una definición de indicadores con niveles predefinidos de atención.
3. **MEDIO:** Se monitorean algunos controles de seguridad de forma periódica y conforme a un procedimiento definido, no existe una definición de indicadores con niveles predefinidos de atención.
4. **ALTO:** Existen indicadores de seguridad definidos con rangos que especifican acciones dependiendo de su valor, procurando mantenerse en el nivel óptimo. Estos indicadores son monitoreados periódicamente, conforme a un procedimiento definido, pero estos son generados manualmente.
5. **ÓPTIMO:** Existen indicadores de seguridad definidos, con rangos que especifican acciones dependiendo de su valor, procurando mantenerse en el nivel óptimo. Generados automáticamente y monitoreados periódicamente, conforme a un procedimiento definido.

## **FACTOR 25. SEGURIDAD FÍSICA**

La seguridad debe proteger la información en todas sus formas, tanto aquella almacenada, procesada y transmitida por medios electrónicos, como aquella que se encuentra impresa o en otros medios. Sin embargo un alto porcentaje de la información se encuentra en medios electrónicos, siendo el centro de datos y los cuartos de comunicaciones los lugares de mayor riesgo para un eventual incidente físico, que atente contra la información, por lo tanto es importante contar con medidas de protección, de forma que se garantice su confidencialidad, integridad y disponibilidad.

Los controles orientados a la seguridad de la información impresa u otros medios no digitales son importantes, pero éstos deben ser definidos como parte de los controles o requerimientos de manejo de la información definidos en el “Factor 4. Gestión de la Información”.

En este apartado se definen controles indispensables para proteger físicamente la plataforma tecnológica que almacena la mayor cantidad de información y que en caso de verse afectada, podría comprometer la confidencialidad, integridad y disponibilidad de la información y de los servicios soportados por la plataforma tecnológica.

Los controles de acceso a sitios en donde se ubican elementos de la plataforma tecnológica o incluso información en otros medios deben definirse de forma estándar y para eso es indispensable que la entidad defina zonas de acceso y procure mantener los controles requeridos para cada zona, de esta forma, los controles no quedarán a criterio del responsable del edificio y se implementaran los que hayan sido previamente definidos.

Los centros de datos, deben aislarse del resto de instalaciones, esto implica ubicarlo en un espacio físico independiente y separado al resto de las oficinas, de forma que se puedan implementar controles que restrinjan el acceso únicamente al personal autorizado. Aislarlo no implica necesariamente la existencia de un edificio exclusivo para el centro de datos, aun y cuando podría ser lo ideal.

Cuando se hace referencia al centro de datos, debe entenderse como cualquier centro de datos existente en la entidad, ya sea este el centro de datos principal, alternativo o cualquier otro, es importante que todos cumplan con los mismos controles.

- 1. INCIPIENTE:** Los centros de datos no se encuentran aislados, no se cuenta con control de acceso físico a los centros de datos, no se cuenta con controles de temperatura, humedad, ni video vigilancia. No se cuenta con un sistema automático de control de respaldo, los equipos se instalan en gabinetes (“racks”) en instalaciones tipo oficina. No se cuenta con cuartos de comunicaciones. No existen zonas de seguridad definidas.
- 2. BAJO:** Los centros de datos se encuentran aislados, no se cuenta con control de acceso físico a los centros de datos, no se cuenta con controles de temperatura, humedad, ni video vigilancia. Se realizan respaldos, pero no se cuenta con un sistema automático de control de respaldos, los equipos se instalan en gabinetes (“racks”). No se cuenta con cuartos de comunicaciones. No existen zonas de seguridad definidas.
- 3. MEDIO:** Los centros de datos se encuentran aislados, se cuenta con control de acceso físico los centros de datos, se cuenta con controles de temperatura, humedad y video vigilancia. Se realizan respaldos pero no se cuenta con un sistema automático de control de respaldo, los equipos se instalan en gabinetes (“racks”). No se cuenta con cuartos de comunicaciones. No existen zonas de seguridad definidas.

4. **ALTO:** Los centros de datos se encuentran aislados, se cuenta con control de acceso físico a los centros de datos, se cuenta con controles de temperatura, humedad y video vigilancia. Se realizan respaldos utilizando un sistema automático de control de respaldo, se envían copias de los respaldos a un sitio externo al centro de datos. Los equipos se instalan en gabinetes (“racks”) y se cuenta con cuartos de cableado que cumplen con controles de acceso físico, de temperatura y de humedad. Existen zonas de seguridad definidas, pero los controles no son validados aunque eventualmente estén implementados.
5. **ÓPTIMO:** Los centros de datos se encuentran aislados, se cuenta con control de acceso físico a los centros de datos, se cuenta con controles de temperatura, humedad y video vigilancia. Se realizan respaldos utilizando un sistema automático de control de respaldo, se envían copias de los respaldos a un sitio externo al centro de datos. Los equipos se instalan en gabinetes (“racks”) y se cuenta con cuartos de comunicaciones que cumplen con controles de acceso físico, de temperatura y de humedad. Existen zonas de seguridad definidas y los controles definidos para estas son validadas periódicamente.

## FACTOR 26. TERCERIZACIÓN DE SERVICIOS (NUBE)

La tercerización de servicios de almacenamiento o procesamiento de la información y el uso de aplicaciones tercerizadas o en la nube, tiene implicaciones de seguridad que deben ser debidamente valoradas con el fin de no exponer información de los clientes, que es custodiada por las entidades o información que resulta crítica para la operación de la entidad.

Al igual que cualquier otra tecnología o proceso, es indispensable, analizar los riesgos y definir controles de seguridad, que procuren la confidencialidad, integridad y disponibilidad de la información y de los servicios soportados. Por lo anterior es indispensable, definir los requerimientos de seguridad.

Considerando que el control de la información o de los servicios se pierde o es limitado al ser implementados en la “nube”, parte de los controles a definir, podría implicar la solicitud de experiencia y el cumplimiento de normas o estándares internacionales de seguridad, así como el uso de encriptación de la información tanto en el transporte como en el almacenamiento de la información.

Algunas entidades no utilizan este tipo de servicios y por tanto podría ser que este factor no requiera ser evaluado. Los niveles siguientes se definen para aquellas entidades que utilizan algún tipo de tercerización.

## **NIVELES DE MADUREZ:**

1. **INCIPIENTE:** Se utilizan servicios de tercerización, contratados directamente por las áreas usuarias sin apoyo del área de tecnología, no se cuenta con un inventario de servicios tercerizados, no existen requerimientos de seguridad definidos, no existe una valoración de riesgo y no existe autorización explícita del dueño de la información.
2. **BAJO:** Se utilizan servicios de tercerización, contratados por las áreas usuarias en coordinación y apoyo del área de tecnología, se cuenta con un inventario de servicios tercerizados. No existen requerimientos de seguridad definidos, no existe una valoración de riesgo, no existe autorización explícita del dueño de la información.
3. **MEDIO:** Se utilizan servicios de tercerización, contratados por las áreas usuarias en coordinación y apoyo del área de tecnología, se cuenta con un inventario de servicios tercerizados, existen requerimientos de seguridad definidos y validados. No existe una valoración de riesgo y no existe autorización explícita del dueño de la información.
4. **ALTO:** Se utilizan servicios de tercerización, contratados por las áreas usuarias en coordinación y apoyo del área de tecnología, se cuenta con un inventario de servicios tercerizados, existen requerimientos de seguridad definidos y validados, existe una valoración de riesgo y existe autorización explícita del dueño de la información y del Comité de Riesgo.
5. **ÓPTIMO:** Se utilizan servicios de tercerización, contratados por las áreas usuarias en coordinación y apoyo del área de tecnología, se cuenta con un inventario de servicios tercerizados, existen requerimientos de seguridad definidos, existe una valoración de riesgo y existe autorización explícita del dueño de la información, del Comité de Riesgo y del Comité de Seguridad. El área de seguridad verifica periódicamente el cumplimiento de los requerimientos de seguridad de los servicios tercerizados.

## FACTOR 27. SEGURIDAD MÓVIL.

La aparición de los dispositivos móviles, vinieron a modificar el escenario de la seguridad, porque debido a un factor de conveniencia los usuarios requieren tener acceso a sistemas, servicios e información, desde cualquier parte del mundo y utilizando cualquier dispositivo móvil, llámese Smartphone, Tablet, portátil o cualquier otro dispositivo que tenga acceso a internet.

Lo anterior implica una serie de retos importantes respecto a cómo brindar la movilidad requerida por los usuarios internos y externos, de forma que se promueva la confidencialidad, integridad y disponibilidad de la información y de los servicios basados en tecnología.

Algunas entidades no utilizan servicios móviles y por tanto podría ser que este factor no requiera ser evaluado. Los niveles siguientes se definen para aquellas entidades que utilizan algún tipo de movilidad.

### NIVELES DE MADUREZ:

1. **INCIPIENTE:** Los sistemas o servicios basados en tecnología pueden ser accedidos utilizando dispositivos móviles o desde cualquier lugar, sin existir restricción ni control alguno.
2. **BAJO:** Los sistemas o servicios basados en tecnología pueden ser accedidos utilizando dispositivos móviles o desde cualquier lugar, el acceso es restringido a usuarios autorizados, pero estos no utilizan controles específicos para dispositivos o usuarios móviles.
3. **MEDIO:** Los sistemas o servicios basados en tecnología pueden ser accedidos utilizando dispositivos móviles o desde cualquier lugar, el acceso es restringido a usuarios autorizados, los dispositivos utilizados cuentan al menos con un sistema antimalware y encriptan la comunicación con la aplicación, utilizando TLS, VPN o algún otro método de encriptación.
4. **ALTO:** Los sistemas o servicios basados en tecnología pueden ser accedidos utilizando dispositivos móviles o desde cualquier lugar, el acceso es restringido a usuarios autorizados, los dispositivos utilizados cuentan al menos con un sistema antimalware, encriptan la comunicación con la aplicación, utilizando TLS, VPN o algún otro método de encriptación, se autentica el dispositivo origen y se utiliza algún

mecanismo de autenticación de dos factores, ya sea OTPs (One Time Passwords), certificados digitales, NFC, biometría u otro medio.

5. **ÓPTIMO:** Los sistemas o servicios basados en tecnología pueden ser accedidos utilizando dispositivos móviles o desde cualquier lugar, el acceso es restringido a usuarios autorizados, los dispositivos utilizados cuentan al menos con un sistema antimalware, encriptan la comunicación con la aplicación, ya sea utilizando TLS, VPN o algún otro método de encriptación y utilizan algún mecanismo de autenticación de dos factores, ya sea OTPs (One Time Passwords), certificados digitales, NFC, biometría u otro medio. Se utilizan sistemas de aislamiento, que permiten crear un ambiente virtual totalmente independiente en su dispositivo, de forma que permite aislar el ambiente laboral o el ambiente de acceso a los servicios de Banca para el cliente, del ambiente personal.

## AGRADECIMIENTOS

Este modelo ha sido elaborado por el Foro Interbancario de Seguridad, conformado por los encargados de la seguridad de la TI y seguridad de la información de las entidades miembro. Adicionalmente fue revisado por especialistas externos que basados en su conocimiento sobre mejores prácticas y su experiencia, colaboraron en la revisión y validación de los factores y criterios definidos en este modelo.

## GLOSARIO

**Administración de la identidad:** Sistema que permite administrar de forma integral la autenticación de los usuarios, sus privilegios, derechos o restricciones de acceso a la información, a sistemas e incluso a áreas físicas dependiendo de su rol o perfil relacionado a su puesto de trabajo.

**Ambiente de desarrollo:** Área lógica que contiene los elementos de software y hardware requeridos para poder trabajar en el desarrollo de una o varias aplicaciones.

**Ambiente de producción:** Área lógica que contiene los elementos de software y hardware que soportan las aplicaciones o servicios de una empresa.

**Ambiente de prueba:** Área lógica que contiene los elementos de software y hardware requeridos para poder trabajar en la prueba de nuevas aplicaciones o de cambios realizados a estas, antes de que esta sea colocada en el ambiente de producción.

**Análisis de vulnerabilidad:** Análisis sistemático que se ejecuta sobre una infraestructura física o electrónica para determinar posibles brechas de seguridad

**Análisis de vulnerabilidad de código:** Proceso basado en una aplicación o Sistema que revisa el código de las aplicaciones en búsqueda de errores de programación que puedan convertirse en vulnerabilidades de seguridad.

**Acceso remoto:** Acceso a una red empresarial desde una ubicación externa a la red.

**Activos de información:** Se refiere a todo elemento que genere, almacene, procese o transmita información que sea considerada de valor para la entidad, tales como: bases de datos, contratos, acuerdos, documentación de los sistemas, manuales de los usuarios, material de formación, recursos informáticos, equipos, redes, sistemas, personas.

**Autenticación de un factor:** Método de autenticación de usuarios basado en algo que se sabe o conoce, como por ejemplo una clave de acceso.

**Autenticación de dos factores:** Método de autenticación de usuarios basado en algo que se sabe o conoce, como por ejemplo una clave de acceso y en algo que se tiene, como por ejemplo un dispositivo.

**Autenticación de tres factores:** Método de autenticación de usuarios basado en algo que se sabe o conoce, como por ejemplo una clave de acceso, en algo que se tiene, como por ejemplo un dispositivo y en algo que se es, o sea en algún factor biométrico, como podría ser la huella digital, el iris, la forma y elementos de la mano, cara u otros.

**BIG Data:** El concepto de “Big Data” se refiere a repositorios de datos que consolidan información estructurada (bases de datos y estructuras) y no estructurada (archivos, documentos, etc) y que permiten a través de herramientas de análisis de información, generar informes o reportes de alto valor para el negocio u otras áreas. A pesar de que usualmente son repositorios de gran tamaño, el concepto de “Big Data” trata más de la variedad de fuentes de información, que de la cantidad.

**BYOD:** Acrónimo del inglés “Bring Your Own Device” práctica implementada por varias empresas a nivel mundial y que permiten al usuario interno o empleado utilizar su dispositivo o equipo de uso personal para uso en la empresa en que labora, con beneficios para ambas partes, pero con riesgos que afectan la seguridad de la información y que requieren ser controlados.

**CISM:** Acrónimo de “Certified Information Security Manager”. Es una certificación del conocimiento y experiencia en la gestión de la seguridad de la información, cubre cuatro grandes temas de la gestión de la seguridad y quien la posee debe demostrar dominio de los diferentes temas manteniéndose actualizado a través de actividades como capacitación, publicación de artículos, participación en actividades y otras.

**CISSP:** Acrónimo de “Certified Information Systems Security Professional”. Es una certificación del conocimiento y experiencia en la gestión de la seguridad de la información, cubre 10 diferentes áreas conocidas como dominios y que conforman un marco de trabajo que incluye las mejores prácticas, metodologías, tecnologías y conceptos de seguridad de la información y quien la posee debe demostrar dominio de los diferentes temas manteniéndose actualizado a través de actividades como capacitación, publicación de artículos, participación en actividades y otras.

**COBIT:** Es un marco de trabajo para gestión de las tecnologías de la información. Define procesos de gestión y objetivos de control orientados a la realización de una debida administración de los procesos, además define un modelo que permite medir el nivel de madurez de las empresas respecto a la debida gestión de las tecnologías de información.

**Confidencialidad de la información:** Principio de seguridad de la información que establece que esta, debe ser accedida únicamente por aquellos que han sido autorizados, por lo que debe ser protegida del acceso de terceros no autorizados.

**Datos en dispositivo de usuario final:** Se refiere a los datos que se encuentran en las estaciones de trabajo o laptops de los usuarios, así como los dispositivos de almacenamiento removibles a los que potencialmente tengan acceso (Disco Compacto, USBs, etc)

**Datos en movimiento:** Se refiere a los datos que se encuentran en tránsito a través del uso protocolos especializados de red tales como: HTTP, FTP, SMTP, P2P, IM.

**Datos en reposo:** Se refiere a los datos que se mantienen inactivos y almacenados en servicios especializados tales como: bases de datos, servidores de archivo, servidores de Intranet, etc).

**Datos en uso:** Se refiere a los datos que están activos en la memoria de acceso dinámico (RAM), cache de CPU, etc.

**Disponibilidad de la información:** Significa que tanto la información como los sistemas de información se encuentren accesibles en tiempo y forma, cada vez que sean requeridos por los usuarios. En el caso específico de la seguridad de la información, la disponibilidad usualmente se limita a la no afectación de la disponibilidad por incidentes de seguridad de la información, de forma que la disponibilidad por otro tipo de fallas usualmente es gestionada por el área de continuidad.

**Dispositivos USB:** Dispositivos que se conectan a través de puertos tipo USB (Universal Serial Bus), este es uno de los estándares de conexión más utilizado para dispositivos externos que se conectan a diferentes tipos de equipos.

**DMZ:** Es el acrónimo de inglés “Demilitarized zone”, se refiere a segmentos de red físico o lógico utilizado para aislar un grupo de equipos de los demás.

**Firewall:** sistema diseñado para controlar el acceso entre diferentes segmentos de red, permitiendo la comunicación explícitamente autorizada entre un segmento y otro y negando o rechazando cualquier comunicación no autorizada.

**Guía de configuración:** guía utilizada para definir los requerimientos mínimos de un tema específico, como podría ser la configuración de un equipo o funcionalidades de una aplicación.

**Imágenes:** Concepto utilizado para copiar configuraciones de un equipo a partir de una configuración inicial definida.

**Incidente de seguridad:** Incidente con consecuencias negativas para la organización, como podría ser una falla o interrupción del servicio, fraude u otro provocado por una falla o falta en los controles de seguridad existentes.

**Infraestructura tecnológica:** Se refiere a los elementos tecnológicos comunes, requeridos para soportar los sistemas o aplicaciones

**Integridad de la información:** Principio de seguridad de la información que establece que la información debe ser modificada únicamente por los medios que han sido autorizados, por lo que debe ser protegida de modificaciones realizadas por cualquier otro medio no autorizado.

**IPS:** Sistema diseñado para analizar el tráfico entre diferentes segmentos de red, identificando y previniendo eventuales ataques, de los que lleva un registro y basado en diferentes criterios puede tomar acción, tales como, bloquear la comunicación o generar alertas al administrador.

**ISM3:** Acrónimo de "Information Security Management Maturity Model".

**ISO27000:** Grupo o serie de estándares de gestión de seguridad de la información emitidos por la ISO, usualmente se hace referencia al estándar 27001 porque es el que es certificable o al 27002 porque es la que define las prácticas de control, además existen otros estándares en la serie como el 27003 que son directrices para la implementación de un sistema de gestión de seguridad de la información, 27004 orientado a métricas de seguridad de la información, 27005 sobre la gestión de riesgos de la seguridad de la información, 27006 define los requisitos para acreditación de organizaciones de certificación, 27007 es una guía de cómo auditar el cumplimiento de la norma, 27035 orientado a la gestión de incidentes de seguridad de la información.

**Malware:** Código malicioso, creado para afectar a equipos, redes y servicios de computación de forma negativa y con diferentes objetivos, como podría ser afectar la operación, ocasionando fallas, robar información, espiar, tomar control de un equipo o red u otros.

**NFC:** Acrónimo de "Near Field Communication", tecnología de proximidad, utilizada para múltiples utilidades, en el tema específico de seguridad, es utilizada como un doble factor de autenticación, ya sea al utilizar tarjetas de proximidad o dispositivos como los celulares que pueden ser utilizados tanto como lector de proximidad como dispositivo y servir como un segundo factor de autenticación.

**Nube:** servicio de procesamiento o almacenamiento de la información contratado a una empresa externa, quien cuenta con su plataforma tecnológica, usualmente en múltiples ubicaciones con el fin de brindar además disponibilidad, servicios que son accedidos a través de la red de Internet. El servicio se basa en el concepto de recursos compartidos y el uso de recursos en demanda.

**Open Security Architecture:** Modelo de arquitectura de seguridad, definido por la comunidad o sea por la participación de especialistas que voluntariamente participan y agregan valor al modelo.

**OTP:** Siglas del inglés “One Time Password” o claves de una sola vez, mecanismo de seguridad que puede ser implementado a nivel de hardware con el uso de dispositivos conocidos como “tokens” o a nivel de software y que permiten generar un password o clave que es válida una única vez, brindando un mejor nivel de seguridad, porque en caso de que la clave sea capturada, ya no podría ser utilizada.

**Parche:** código de software diseñado para corregir o mejorar aplicativos, sistemas operativos u otros programas.

**Plantilla de configuración:** Formato que incluye la configuración a aplicar para un tipo específico de equipo, basado en su función o en su tipo de usuario. Las plantillas a diferencia de las guías, se pueden definir para que sean aplicadas de forma automática.

**Plataforma tecnológica:** Conjunto de equipos (hardware), sistemas (software) y enlaces de comunicación que soportan los servicios tecnológicos de una empresa.

**Proceso de Gestión de Seguridad de la Información:** Para definir, implementar y mantener un Sistema de Gestión de Seguridad de la información (SGSI) es indispensable contar con un proceso metodológico, que permita implementar un proceso de mejora continua que involucre las fases de Planear, Hacer, Revisar y Actuar.

**Prueba de penetración (Penetration Test):** La prueba de penetración, es un método o proceso utilizado para verificar la efectividad de la seguridad de la información a nivel tecnológico, dando como resultado el nivel de exposición en el que se encuentra la infraestructura implementada en una organización, a la explotación de vulnerabilidades o brechas de seguridad existentes mediante la aplicación de amenazas conocidas.

**Prueba de penetración externa:** La prueba de penetración externa, es ejecutada desde el exterior de la red y usualmente por un tema de imparcialidad es también ejecutada por personal externo a la organización.

**Prueba de penetración interna:** La prueba de penetración interna, es ejecutada desde el interior de la red y podría ser ejecutada por personal interno o externo a la organización.

**Registros de eventos (logs):** Los registros de eventos o (Log) es el registro de las acciones o actividades ejecutadas en los diferentes equipos o aplicaciones, utilizados para dejar rastro que quien, cuando, desde donde e algunas veces como, logró ejecutar la acción realizada.

**Riesgo Inherente:** Riesgos que existen per se, independientemente de la existencia o no de controles, son riesgos que son inherentes a una actividad.

**Roadmap:** Término muy utilizado en el ámbito tecnológico para indicar un plan de ruta, el cual básicamente resume las macro actividades o hitos importantes que deben irse cumpliendo a través del tiempo para lograr un objetivo específico, usualmente se relacionan estas actividades a soluciones tecnológicas específicas. A diferencia de un cronograma, no se especifican actividades específicas, ni responsables, es básicamente un documento que permite tener visibilidad de los grandes temas a desarrollar.

**Seguridad de la información:** Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

**Seguridad de TI:** Es el conjunto de controles orientados a proteger la plataforma tecnológica que soporta los servicios de una empresa, tanto hardware como software y especialmente, la información almacenada, procesada o transmitida por diferentes sistemas informáticos.

**Servicios críticos:** Servicios relacionados a la operación principal de una empresa y que en caso de falla, provocarían serios daños, económicos, de imagen u otros. Los servicios críticos usualmente son identificados por el área de negocio a partir de un análisis de impacto.

**SIEM:** Acrónimo de "Security Information and Event Management", es un Sistema diseñado para recolectar los eventos que se generan en los diferentes dispositivos de la plataforma tecnológica, aplicando métodos de correlación que permiten identificar actividades inusuales que requieran ser notificadas o incluso en algunos casos activar acciones para controlar o mitigar un eventual incidente.

**Sistema de Gestión de Seguridad de la Información (SGSI):** Un Sistema de Gestión de Seguridad de la Información, es la definición e implementación de un proceso de gestión orientado a promover la confidencialidad, integridad y disponibilidad de la información y de los servicios soportados por la plataforma tecnológica. El término es utilizado por la familia de estándares ISO27000 y promueven la implementación de un modelo de mejora continua con la

implementación del ciclo de Demming, conocido como Planear-Hacer-Revisar-Actuar (Plan-Do-Check-Act).

**SSE-CMM:** Acrónimo de “Systems Security Engineering Capability Maturity Mode”, define las actividades del ciclo de vida de la Seguridad, incluyendo definiciones conceptuales, análisis de requerimientos, diseño, desarrollo, integración, instalación, operación, mantenimiento y otras que describen las características esenciales de un proceso de gestión de seguridad.

**TLS:** Acrónimo del inglés “Transport Layer Security” es un protocolo de encriptación que permite proteger la información que es enviada a través de Internet entre un usuario y una aplicación web.

**Topología:** Gráfico que muestra la ubicación lógica de los diferentes elementos de red y que muestra cómo se interconectan unos con otros.

**Usuarios administradores:** Usuarios que se encargan de las actividades administrativas de una herramienta, entre ellas la creación, eliminación y modificación de usuarios y privilegios o permisos.

**Usuarios privilegiados:** usuarios a los que se les ha asignado privilegios o permisos adicionales a las que tiene un usuario normal.

**Usuarios de soporte:** usuarios a los que se les ha asignado privilegios o permisos relacionados con el soporte de las aplicaciones o equipos, usualmente podrían bajar, subir aplicaciones, modificar su configuración y otras actividades que podrían afectar la operación de una aplicación, equipo o servicio.

**Valoración de riesgo:** proceso metodológico para la identificación, análisis, evaluación, administración y revisión de los riesgos, tanto de fuentes internas como externas, que afectan una actividad, proceso o servicio.

**VPN:** Acrónimo de “Virtual Private Network” o red privada virtual, es una tecnología de red que permite una extensión segura de la red de área local(LAN) sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada. Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.

Aprobado por el Foro Interbancario de Seguridad de la Información el 08 de marzo del 2017

Aprobado por la Junta Directiva en sesión del 22 de marzo del 2017