



Informe de Evaluación de Seguridad

Análisis de Nivel de Madurez

*GMS Seguridad de la Información ofrece el servicio de análisis de la brecha de seguridad de la información en la organización, evaluando el estado actual y los controles definidos al interior de **BELLAS ARTES** y contrastándolos con las buenas prácticas indicadas el modelo de controles críticos de seguridad de la información.*

Preparada para:

Bellas Artes

2023

CONTROL DOCUMENTAL

Proyecto	Consultoría
Empresa	BELLAS ARTES
Título	Evaluación de nivel de madurez de seguridad de la información
Herramientas de edición	Microsoft Office Word

CONTROL DE VERSIONES

Versión	Autor	Fecha de validación	Descripción
2.0	GMS	07 de marzo del 2023	Creación documental

ÚLTIMA REVISIÓN

Página No.	Modificación

VALIDACIONES Y APROBACIONES

Elaborado	Adrián Calvopiña M.
Verificado	-
Aprobado	-

Índice

I.	Restricción para la publicación y uso de la información	2
II.	Descripción.....	3
2.1	Evaluación del Nivel de Madurez de Seguridad de la Información.....	3
2.2	Valoración de los Controles	4
2.3	Atributos de los Controles	5
III.	Alcance	5
3.1	Participantes y requerimientos.....	5
IV.	Objetivos	6
4.1	Objetivo general.....	6
4.2	Objetivos del servicio	6
4.3	Objetivos específicos	6
4.4	Objetivos de los de Controles	7
V.	Metodología.....	10
5.1	Actividades por fases	10
5.1.1	Fase I: INICIO.....	11
5.1.2	Fase II: PLANIFICACIÓN	11
5.1.3	Fase III: EJECUCIÓN.....	11
5.1.4	Fase IV: CIERRE	12
VI.	Resumen ejecutivo	13
6.1	Matriz de brechas de seguridad de la información	14
6.2	Matriz de Riesgo & Factibilidad	15
6.3	Matriz de Riesgo & Nivel de exposición.....	16
VII.	Conclusiones	16
VIII.	Recomendaciones sobre hallazgos relevantes.....	20
	Sobre Protección de Datos (DLP)	24
	Sobre Control y gestión en la nube	24
IX.	Plan de proyectos recomendados.....	25

I. Restricción para la publicación y uso de la información

El presente Informe de consultoría contiene información que es propiedad de GMS Seguridad de la Información, su publicación le podría otorgar ventajas competitivas a terceros ajenos a los involucrados en esta evaluación. Por lo tanto, este documento debe ser usado sólo por aquellos autorizados en dicha evaluación y no debe ser publicado o duplicado, ni entera ni parcialmente, para ningún otro propósito que no sea el de evaluar a GMS Seguridad de la Información. Los datos sujetos a esta restricción son todos los contenidos en la totalidad del documento.

Si un contrato es suministrado a GMS Seguridad de la Información, como resultado de, o con relación a, el presente Informe, cualquier derecho a duplicar, usar o publicar los datos será de acuerdo con lo establecido en dicho contrato.

Esta restricción no limita los derechos del receptor a usar la información contenida en el presente informe si la misma pasara a ser parte de una fuente de dominio público y siempre y cuando no adquiera tal carácter como consecuencia del no cumplimiento de las restricciones aquí mencionadas.

II. Descripción

2.1 Evaluación del Nivel de Madurez de Seguridad de la Información

GMS Seguridad de la Información ofrece como valor agregado el servicio de un análisis de las brechas de seguridad de la información en las organizaciones, evaluando el estado actual de los controles definidos e implementados por las Empresas y contrastándolos con un conjunto de controles de seguridad de la información, basados en estándares internacionales como CIS de SANS, NIST CF, PCI DSS 3.2 e ISO 27001:2013, más recomendaciones y buenas prácticas utilizadas para la defensa cibernética de las empresas. El servicio está definido para que en lo posterior la organización esté en la capacidad de generar un mapa de ruta claro para incrementar sus niveles de seguridad de la información.

Los controles de evaluación propuesto por GMS Seguridad de la Información se agrupan por las etapas de la arquitectura de seguridad adaptativa de Gartner más la etapa de Gestión, que es neurálgica para la seguridad de la información, este marco es muy útil para ayudar a las organizaciones a clasificar los controles de seguridad existentes y potenciales, para garantizar que exista un enfoque equilibrado de la seguridad.

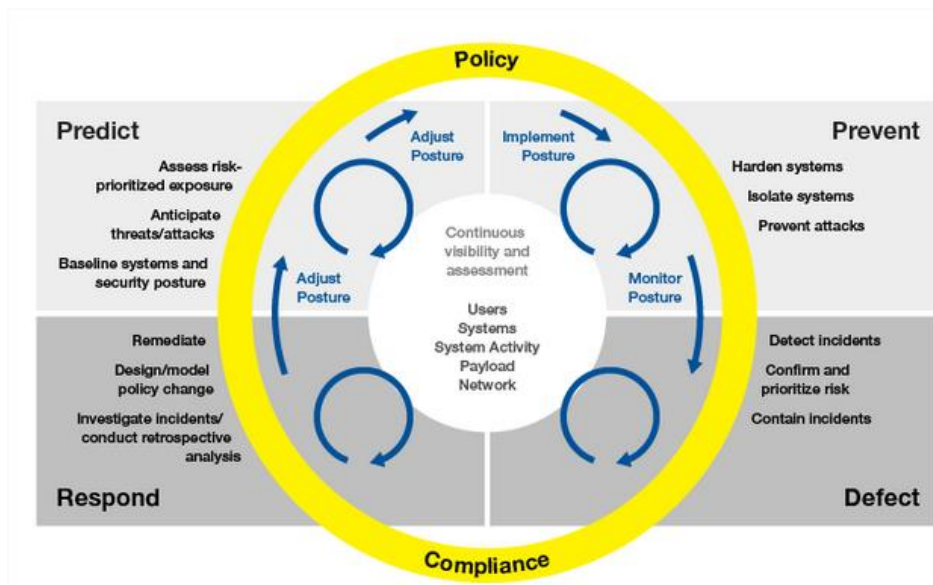
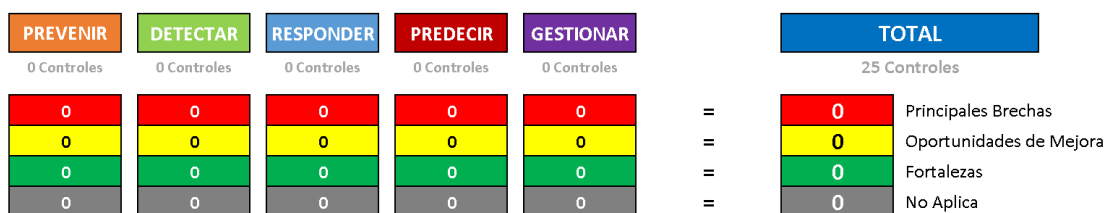


Figura No. 1 - The Four Stages of an Adaptive Security Architecture.

Cada etapa cuenta con controles específicos y estos a sus veces se expanden en sub-controles, dando un compendio de 5 etapas, 25 controles y 145 sub-controles.



⚠️ NOTA IMPORTANTE: Para efectos demostrativos y de conocimiento general, los cuadros, tablas y demás contenidos documentales pueden verse resumidos para la comprensión por parte del lector.

2.2 Valoración de los Controles

Las repuestas se ejecuta bajo los siguientes parámetros:

VALOR	DESCRIPCIÓN
0 - No existente	Control no implementado o inexistente.
1 - En fase inicial	El control se conoce y están en la etapa de planificación, arranque, compra o definición inicial.
2 - Manual o limitado	El control existe de manera básica/limitada, rudimentaria o se controlan manualmente.
3 - Implementado parcialmente	El control existe y está cubriendo parcialmente o está funcionando de manera parcial.
4 - Implementado totalmente	El control existe y está implementado a totalidad y está operando de manera óptima.
5 - No aplica	El control no es necesario con justificación aceptable y que no afecta el negocio o a la estrategia de gestión de la seguridad de la información.

Cada respuesta de los sub-controles cuenta con una puntuación, y suma para la valoración del control; este valor nos dará un porcentaje de madurez en el control, este valor se contrastará contra un porcentaje de valor esperado del control, esto nos arrojará el porcentaje de la brecha que tiene cada control y resultado final del nivel de madurez, el cual se presentara en porcentaje (1%-100%) y mediante una identificación de colores rojo, amarillo y verde (tipo semáforo) y gris, y tienen la siguiente definición:

Identificación de colores:

	Principales brechas
	Oportunidades de mejora
	Fortalezas
	No aplica

2.3 Atributos de los Controles

Adicional a la medición de la implementación de los controles se evaluará también los atributos de cada control bajo los siguientes parámetros y ponderación:

ATRIBUTO	DESCRIPCIÓN	PESO DE EVALUACIÓN
Documentación	Registro actualizado de la información del control que al menos incluye: Responsables, Configuración/Procedimiento de gestión del control, Método de auditoría de cumplimiento e Indicadores.	15%
Operación	Facilidades del control implementadas y en operación (Activo/Herramienta/Proceso).	40%
Normativa	Política documentada y aprobada por la organización que rige al control y responde a las necesidades de seguridad de información de la organización.	20%
Monitoreo	Facilidades de monitoreo del control implementadas y en operación, así como el mecanismo de identificación de una alarma de seguridad y un proceso de respuesta frente a la acción de una amenaza.	15%
Mejora Continua	Plan en ejecución de mejoras a los controles, enfocada en una optimización de indicadores o de cumplimiento de las necesidades de seguridad de información de la organización.	10%

III. Alcance

El servicio de análisis de nivel de madurez contempla la validación de los controles implementados por la organización para la seguridad de la información, mediante entrevistas con los responsables de ciertas áreas operativas o procesos críticos del negocio, sin verificación de evidencias físicas o digitales que corroboren que se cuenta con los controles evaluados. Dependiendo de la veracidad de las respuestas asociadas al control se realizarán los cálculos.

3.1 Participantes y requerimientos

Equipo de trabajo asignado a la evaluación:

(puede variar según organigrama y asignación de roles de la empresa).

- Coordinador de la evaluación (espónsor).
- Administrador/es de Redes (infraestructura).
- Administrador/es de IT.
- Administrador/es de Seguridad de la información.

Requerimientos mínimos:

Para poder desarrollar esta actividad, se enlistan los requerimientos con los que se deberán contar en cada una de las sesiones o workshop a ejecutar. *(se ampliarán a mayor detalle en el plan de trabajo).*

- Disponibilidad del personal perteneciente a la Organización, según el Plan de ejecución de acordado.
- Conocimiento de las instalaciones, departamento TI, Data Center.
- Sala de reuniones (virtual o física).
- Elementos para proyectar video.
- Servicio de Internet.

IV. Objetivos


4.1 Objetivo general

- Determinar el nivel de riesgo de seguridad de la información, al cual se encuentra expuesto **BELLAS ARTES**, mediante el estudio de un análisis de brechas.

4.2 Objetivos del servicio

- Identificar las brechas de seguridad de la información actual vs los controles de seguridad de información (controles de seguridad GMS).
- Dar la prioridad para enfocar acciones con altos resultados en el tiempo.
- Alinear las prioridades en función de los riesgos orientados a la vertical de negocio.
- Dar visibilidad y alinear los criterios entre todos los niveles de la Organización.
- Generar una metodología de priorización que permita establecer una hoja de ruta de proyectos que generen una mitigación de riesgos en secuencia óptima, según las necesidades y los recursos financieros.
- Recomendar las acciones pertinentes a realizar por las empresas del grupo para que, en el corto plazo, puedan llegar al nivel deseado y aprovechar al máximo las inversiones y los presupuestos.

4.3 Objetivos específicos

 **NOTA IMPORTANTE:** Los objetivos específicos correspondientes al *Análisis de Nivel de Madurez* presentado, serán acotados y estarán alineados a los requerimientos de su organización.

4.4 Objetivos de los de Controles

Los objetivos de los 25 controles se detallan a continuación:

- ***Inventario de hardware:***
Administración activa que permita conocer e inventariar solo los dispositivos autorizados que forman parte o deben pertenecer a la red, y bloquear el acceso al resto.
- ***Inventario de software:***
Administración activa que permita conocer e inventariar todo el software de la red, no solo el instalado, si no el que se puede ejecutar.
- ***Configuraciones de seguridad de hardware y software:***
Establecer, implementar, y administrar configuraciones seguras usando una configuración rigurosa y un proceso de control de cambios que permita prevenir ataques.
- ***Seguridad de aplicaciones:***
Gestionar el ciclo de vida de todas las aplicaciones desarrolladas por la empresa, con el fin de prevenir, detectar, y corregir brechas de seguridad.
- ***Configuraciones de seguridad para dispositivos de red:***
Establecer, implementar y administrar activamente (rastros/reportes/corrección) las configuraciones seguras de los dispositivos de red, usando gestión de configuraciones seguras y un proceso de control de cambios.
- ***Control de puertos y servicios:***
Administrar (rastros/control/corrección) la operación continua de uso de puertos, protocolos, servicios en dispositivos de red para minimizar los espacios de vulnerabilidad disponibles para los atacantes.
- ***Defensa perimetral:***
Detectar/prevenir/corregir el flujo de información que se transfiere entre diferentes redes con un enfoque de protección de datos.
- ***Protección de e-mail y Web:***
Minimizar la superficie de ataque y las oportunidades de los atacantes para manipular el comportamiento humano mediante la interacción con navegadores web y correo electrónico.

- **Defensa de punto final (Endpoints):**
Controlar la instalación, propagación y ejecución de código malicioso en diferentes puntos de la organización, mientras se optimiza la habilidad de defensa, recolección de información y se aplican acciones correctivas.
- **Protección de plataformas móviles:**
Minimizar los riesgos expuestos en caso de que las organizaciones permitan utilizar dispositivos móviles en la organización, o que los colaboradores de la organización utilicen los dispositivos móviles para almacenar, procesar o transmitir datos de la organización.
- **Protección de redes inalámbricas:**
Los procesos y las herramientas usadas para rastrear/controlar/prevenir/corregir el uso seguro de redes inalámbricas en la red local (LAN), Access points, etc.
- **Protección de datos:**
Los procesos y herramientas usados para prevenir una filtración, mitigando sus efectos y asegurando la privacidad e integridad de información crítica acorde a las directrices formales y procesos aprobados.
- **Endurecimiento de servidores y estaciones de trabajo:**
Capacidades que permitan a las organizaciones implementar buenas prácticas de seguridad de la información en las configuraciones de equipos que serán utilizados en los ambientes de producción.
- **Control de acceso físico:**
Visualizar los controles necesarios en las organizaciones, que permitan controlar el acceso a las áreas de procesamiento, transmisión y almacenamiento de datos críticos de los usuarios de sus servicios.
- **Monitoreo y análisis:**
Recolección, gestión y análisis de logs de eventos que podrían ayudar a detectar, entender o recuperar de un ataque.
- **Control de cuentas:**
Gestión activa del ciclo de vida de cuentas de sistemas y aplicaciones (creación/uso/inactividad/eliminación) con el fin de minimizar que atacantes hagan uso de estas.
- **Control y gestión en la nube:**
Buenas prácticas y controles para la protección de la información para los servicios en la nube.

- **Accesos y administración de contraseñas:**
Procesos y herramientas utilizados para rastrear/controlar/prevenir/corregir el uso, la asignación y la configuración de privilegios administrativos en computadoras, redes y aplicaciones.
- **Escaneo y remediación de vulnerabilidades:**
Adquisición, evaluación y toma de acción continua, de información nueva que permita identificar vulnerabilidades, remediar, y minimizar el espacio por el cual un atacante puede ingresar a la red.
- **Gestión y respuesta a incidentes:**
Proteger la información de la organización, así como su reputación, mediante el desarrollo e implementación de infraestructura de respuesta a incidentes, para un descubrimiento rápido de ataques, y una efectiva contingencia del daño, erradicando la presencia del atacante y restaurando la integridad de la red y los sistemas.
- **Capacidad de recuperación de datos:**
Los procesos y herramientas usados para proveer una metodología adecuada de recuperación de información crítica.
- **Entrenamiento a usuarios:**
Para todos los roles y funciones de la organización, identificar las necesidades de conocimiento, destreza y habilidades para aportar en la defensa de la empresa, desarrollando y ejecutando un plan integral de evaluación, identificación de brechas, y remediación, mediante programas organizacionales de planificación, entrenamiento, y concientización.
- **Penetración test:**
Pruebas para determinar la fortaleza general de las defensas de la organización (la tecnología, los procesos y las personas) simulando los objetivos y las acciones que realizaría un atacante.
- **Gestión de seguridad de la información:**
Validar la existencia de implementación de seguridad de la información en las organizaciones, no solo como un rol; como un todo que dependiendo de la organización puede ser un equipo, presupuesto, y recursos tecnológicos debidamente dimensionados.
- **Inteligencia de seguridad de la información:**
Identificación de fuentes de información que permitan a las organizaciones conocer el estado de amenazas, y ser proactivos en las defensas y decisiones que se deben tomar, minimizando el impacto causado por posibles ataques dirigidos.

V. Metodología

Para la ejecución del servicio, GMS cuenta con una metodología para la ejecución exitosa basada en cuatro (4) fases macros y actividades principales dentro de cada una, las cuales se detallan a continuación:



Figura No. 2 – Fases Macro de la Metodología de Ejecución.

Cada fase de la metodología tiene como objetivo identificar el avance y el estado de la ejecución del servicio, para garantizar un cumplimiento exitoso del alcance del servicio brindado.

5.1 Actividades por fases

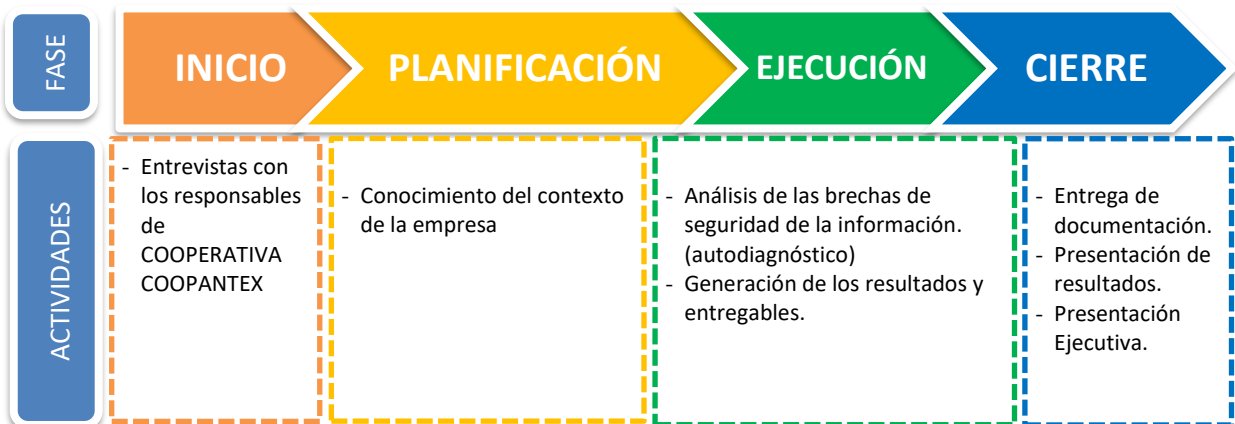


Figura No. 3 – Fases y Actividades.

5.1.1 Fase I: INICIO

Declaración de inicio del servicio.

La declaración de inicio o kick off, es la primera reunión, que se realizó con personal asignado de **BELLAS ARTES** y el especialista de **GMS** responsable de la ejecución del proceso de *Análisis de Nivel De Madurez* en mención, en la cual se hará la presentación inicial, detallando el servicio a entregar como valor agregado por parte de GMS.

En la reunión se revisó el alcance del servicio, se socializaron los temas mencionados en la metodología de trabajo a utilizar, los entregables, los requerimientos, el personal involucrado y el tiempo estimado para las actividades.

Los resultados iniciales conformarán la base para la elaboración del plan de trabajo de GMS.

5.1.2 Fase II: PLANIFICACIÓN

Conocimiento del contexto de la empresa.

En esta fase se realizó el levantamiento de información a través de entrevistas con los responsables asignados por parte de **BELLAS ARTES**, por ello la importancia de la veracidad de las respuestas:

Se conoció a través de un autodiagnóstico información como:

- Arquitectura de red.
- Infraestructura física (conexiones de redes).
- Soluciones de seguridad implementadas.
- Equipamiento de estaciones de trabajo y servidores.
- Servicios y aplicaciones críticas.
- Procesos de negocio donde participan los servidores críticos.

Se llevó a cabo **1 sesión de entrevista** con los responsables e involucrados que proporcionaron toda la información requerida.

5.1.3 Fase III: EJECUCIÓN

Análisis de brechas de seguridad de la información.

- Entrevistas con las personas que administran, operan, gestionan, o conocen de las herramientas, controles o procesos de la seguridad de la información.

El presente servicio no contempla actividades de Ethical Hacking o Penetration Testing, estas se pueden considerar posteriormente a la evaluación, deben ser solicitados y cotizados por separado acorde al alcance requerido.

Se debe considerar que el resultado del diagnóstico dependerá de la veracidad de las respuestas que se hayan dado en el proceso por parte del equipo de trabajo de **BELLAS ARTES**.

GMS no solicitó documentación dado que la actividad no tiene alcance de verificación documental o evidencias.

Generación de los resultados y entregables.

Posterior a todo el trabajo realizado, se genera un informe final con los detalles y análisis realizados.

5.1.4 Fase IV: CIERRE

Entrega de documentación.

Se procederá con la entrega del informe generado en formato digital (PDF)

Presentación de resultados.

Se realizará una reunión entre **BELLAS ARTES** y GMS, para presentación a detalle de los resultados del nivel de madurez y propuesta de controles/proyectos a ejecutarse según la hoja de ruta.

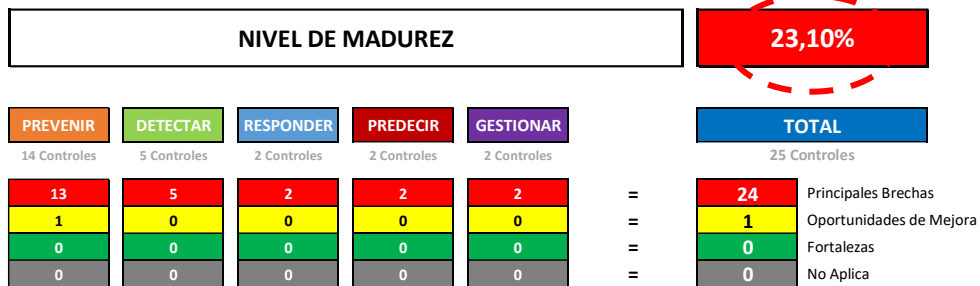
Presentación ejecutiva.

Se realizará una reunión entre el cliente (Gerencias o Stakeholders) y GMS Seguridad de la Información, para presentación Ejecutiva de los resultados del nivel de madurez y propuesta de controles/proyectos a ejecutarse según la hoja de ruta.

VI. Resumen ejecutivo

Posterior al levantamiento de información, realizado el **22 de septiembre del 2022**, junto con el personal de **BELLAS ARTES**, se entregan los resultados obtenidos resumidos en el presente documento:

3. RESUMEN DE LOS RESULTADOS



4. SEMAFORO DE LOS CONTROLES

Inventario de Hardware	Inventario de Software	Configuraciones de Seguridad de Hardware y Software	Seguridad de Aplicaciones	Configuraciones de seguridad para dispositivos de red
Control de Puertos y Servicios	Defensa Perimetral	Protección de Email y Web	Defensa de punto final (Endpoints)	Protección de plataformas móviles
Protección de redes inalámbricas	Protección de Datos	Endurecimiento de Servidores y Estaciones de trabajo	Control de acceso físico	Monitoreo y Análisis
Control de Cuentas	Control y Gestión en la Nube	Accesos y Administración de Contraseñas	Escaneo y remediación de vulnerabilidades	Gestión y Respuesta a Incidentes
Capacidad de Recuperación de Datos	Entrenamiento a usuarios	Penetración Test	Gestión de Seguridad de la Información	Inteligencia de Seguridad de la Información

Los controles de seguridad de GMS son un conjunto de recomendaciones y buenas practicas basados en estándares internacionales para la seguridad de la información como la SANS, NIST CF, PCI 3.0 e ISO 27002:2013, utilizadas para la defensa cibernética de las empresas, que proporcionan una visión y soluciones concretas para detener los ataques más invasivos y peligrosos de la actualidad. Un beneficio principal de los controles es que priorizan y enfocan un número menor de acciones con altos resultados y permiten evaluar el nivel de madurez en seguridad de la información.

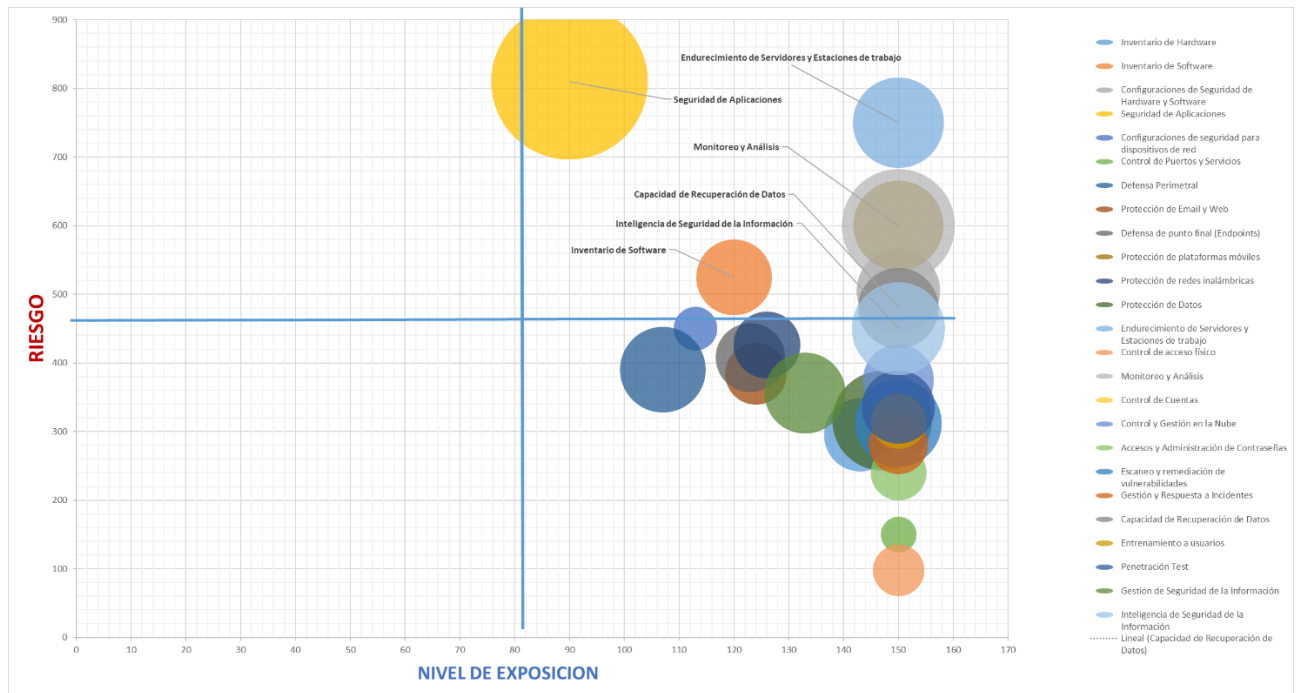
6.1 Matriz de brechas de seguridad de la información

	CONTROLES	DESCRIPCION	PUNTOS	% MADUREZ	% ESPERADO	% BRECHA
PREVENIR	Control 1	Inventario de Hardware	2	0,40%	8,00%	95,00%
	Control 2	Inventario de Software	6	1,20%	6,00%	80,00%
	Control 3	Configuraciones de Seguridad de Hardware y Software	0	0,00%	12,00%	100,00%
	Control 4	Seguridad de Aplicaciones	10	2,00%	4,00%	50,00%
	Control 5	Configuraciones de seguridad para dispositivos de red	7	1,50%	6,00%	75,00%
	Control 6	Control de Puertos y Servicios	0	0,00%	6,00%	100,00%
	Control 7	Defensa Perimetral	36	7,50%	24,00%	68,80%
	Control 8	Protección de Email y Web	15	3,00%	14,00%	78,60%
	Control 9	Defensa de punto final (Endpoints)	22	4,40%	20,00%	78,00%
	Control 10	Protección de plataformas móviles	0	0,00%	5,70%	100,00%
	Control 11	Protección de redes inalámbricas	10	1,70%	8,60%	80,00%
	Control 12	Protección de Datos	2	0,30%	15,90%	98,20%
	Control 13	Endurecimiento de Servidores y Estaciones de trabajo	0	0,00%	4,20%	100,00%
DETECTAR	Control 14	Control de acceso físico	0	0,00%	6,50%	100,00%
	Control 15	Monitoreo y Análisis	0	0,00%	3,80%	100,00%
	Control 16	Control de Cuentas	0	0,00%	7,00%	100,00%
	Control 17	Control y Gestión en la Nube	0	0,00%	6,50%	100,00%
	Control 18	Accesos y Administración de Contraseñas	0	0,00%	6,10%	100,00%
RESPONDER	Control 19	Escaneo y remediación de vulnerabilidades	0	0,00%	8,40%	100,00%
	Control 20	Gestión y Respuesta a Incidentes	0	0,00%	3,60%	100,00%
PREDECIR	Control 21	Capacidad de Recuperación de Datos	0	0,00%	5,90%	100,00%
	Control 22	Entrenamiento a usuarios	0	0,00%	4,10%	100,00%
GESTIONAR	Control 23	Penetración Test	0	0,00%	3,90%	100,00%
	Control 24	Gestión de Seguridad de la Información	15	1,10%	8,60%	87,50%
	Control 25	Inteligencia de Seguridad de la Información	0	0,00%	1,40%	100,00%
TOTAL			125	23,10%	200,20%	88,46%

6.2 Matriz de Riesgo & Factibilidad

	CONTROLES	DESCRIPCION	NIVEL DE EXPOSICION 0-150 Unidades	RIESGO (Impacto x Probabilidad) 1-900 Unidades	FACTIBILIDAD (Complejidad x Costos) 5 - 15750 Unidades
PREVENIR	Control 1	Inventario de Hardware	143	295	1189
	Control 2	Inventario de Software	120	525	1287
	Control 3	Configuraciones de Seguridad de Hardware y Software	150	505	1568
	Control 4	Seguridad de Aplicaciones	90	810	5498
	Control 5	Configuraciones de seguridad para dispositivos de red	113	450	427
	Control 6	Control de Puertos y Servicios	150	375	285
	Control 7	Defensa Perimetral	107	390	1644
	Control 8	Protección de Email y Web	124	384	859
	Control 9	Defensa de punto final (Endpoints)	123	408	1073
	Control 10	Protección de plataformas móviles	150	600	1809
	Control 11	Protección de redes inalámbricas	126	426	1003
	Control 12	Protección de Datos	147	316	2229
	Control 13	Endurecimiento de Servidores y Estaciones de trabajo	150	750	1855
DETECTAR	Control 14	Control de acceso físico	150	98	594
	Control 15	Monitoreo y Análisis	150	600	2860
	Control 16	Control de Cuentas	150	318	292
	Control 17	Control y Gestión en la Nube	150	375	1132
	Control 18	Accesos y Administración de Contraseñas	150	240	694
RESPONDER	Control 19	Escaneo y remediación de vulnerabilidades	150	312	1685
	Control 20	Gestión y Respuesta a Incidentes	150	281	795
PREDECIR	Control 21	Capacidad de Recuperación de Datos	150	480	1447
	Control 22	Entrenamiento a usuarios	150	315	695
GESTIONAR	Control 23	Penetración Test	150	336	1200
	Control 24	Gestión de Seguridad de la Información	133	356	1475
	Control 25	Inteligencia de Seguridad de la Información	150	450	1950
TOTAL			3476	415,8	1421,8

6.3 Matriz de Riesgo & Nivel de exposición



VII. Conclusiones

- El entorno de seguridad de información de **BELLAS ARTES** se ubica en la categoría de madurez **“BAJA”**. En consecuencia, la estrategia Seguridad de la información, de TI, roles, controles y responsabilidades que corresponden con los escenarios valorados presentan oportunidades de mejora notables.
- En función del estudio realizado a los 25 controles, se obtuvo información precisa sobre cada uno de ellos, se identificó: **(24) controles en estado crítico**, **(1) controles con oportunidades de mejora**, **(0) controles se encuentran debidamente implementados**, **(0) no aplicable**.

- Los controles con oportunidad de mejora críticos cuya brecha es superior al 50% deben ser considerados de forma prioritaria.

No	CONTROLES	OBJETIVO	SANS 6.1	NIST CF	PCI 3.0	ISO 27002:2013	%BRECHA
3	Configuraciones de Seguridad de Hardware y Software	Establecer, implementar, y administrar configuraciones seguras usando una configuración rigurosa y un proceso de control de cambios que permita prevenir ataques.	Control 3	PR-IP	2.2 2.3 6.2 11.5	A.14.2.4 A.14.2.8 A.18.2.3	100,0%
6	Control de Puertos y Servicios	Administrar (rastros/control/corrección) la operación continua de uso de puertos, protocolos, servicios en dispositivos de red para minimizar los espacios de vulnerabilidad disponibles para los atacantes	Control 9	PR-IP	1.4	A.9.1.2 A.13.1.1 A.13.1.2 A.14.1.2	100,0%
10	Protección de plataformas móviles	Minimizar los riesgos expuestos en caso de que las organizaciones permitan utilizar dispositivos móviles en la organización, o que los colaboradores de la organización utilicen los dispositivos móviles para almacenar, procesar o transmitir datos de la organización.					100,0%
13	Endurecimiento de Servidores y Estaciones de trabajo	Capacidades que permitan a las organizaciones implementar buenas prácticas de seguridad de la información en las configuraciones de equipos que serán utilizados en los ambientes de producción.					100,0%
14	Control de acceso físico	Visualizar los controles necesarios en las organizaciones, que permitan controlar el acceso a las áreas de procesamiento, transmisión y almacenamiento de datos críticos de los usuarios de sus servicios.					100,0%
15	Monitoreo y Análisis	Recolección, gestión y análisis de logs de eventos que podrían ayudar a detectar, entender o recuperar de un ataque	Control 6	DE-AE RS-AN	10.1- 10.7	A.12.4.1 - A.12.4.4 A.12.7.1	100,0%
16	Control de Cuentas	Gestión activa del ciclo de vida de cuentas de sistemas y aplicaciones (creación/uso/inactividad/eliminación) con el fin de minimizar que atacantes hagan uso de las mismas	Control 16	PR-AC DE-CM	7.1- 7.3 8.7- 8.8	A.9.1.1 A.9.2.1 - A.9.2.6 A.9.3.1 A.9.4.1 - A.9.4.3 A.11.2.8	100,0%
17	Control y Gestión en la Nube	Buenas prácticas y controles para la protección de la información para los servicios en la nube				ISO/EC 27017	100,0%

18	Accesos y Administración de Contraseñas	Procesos y herramientas utilizados para rastrear/controlar/prevenir/corregir el uso, la asignación y la configuración de privilegios administrativos en computadoras, redes y aplicaciones.	Control 5	PR-AC	2.1 7.1-7.3 8.1-8.3 8.7	A.9.1.1 A.9.2.2 - A.9.2.6 A.9.3.1 A.9.4.1 - A.9.4.4	100,0%
19	Escaneo y remediación de vulnerabilidades	Adquisición, evaluación y toma de acción continua, de información nueva que permita identificar vulnerabilidades, remediar, y minimizar el espacio por el cual un atacante puede ingresar a la red.	Control 4	ID-RA DE-CM RS-MI	6.1 6.2 11.2	A.12.6.1 A.14.2.8	100,0%
20	Gestión y Respuesta a Incidentes	Proteger la información de la organización, así como su reputación, mediante el desarrollo e implementación de infraestructura de respuesta a incidentes, para un descubrimiento rápido de ataques, y una efectiva contingencia del daño, erradicando la presencia del atacante y restaurando la integridad de la red y los sistemas	Control 19	DE-AE RS-RP	12.10	A.6.1.3 A.7.2.1 A.16.1.2 A.16.1.4 - A.16.1.7	100,0%
21	Capacidad de Recuperación de Datos	Los procesos y herramientas usados para proveer una metodología adecuada de recuperación de información crítica	Control 10	RC-RP	4.3 9.5-9.7	A.10.1.1 A.12.3.1	100,0%
22	Entrenamiento a usuarios	Para todos los roles y funciones de la organización, identificar las necesidades de conocimiento, destreza y habilidades para aportar en la defensa de la empresa, desarrollando y ejecutando un plan integral de evaluación, identificación de brechas, y remediación, mediante programas organizacionales de planificación, entrenamiento, y concientización	Control 17	PR-AT	12.6	A.7.2.2	100,0%
23	Penetración Test	Pruebas para determinar la fortaleza general de las defensas de la organización (la tecnología, los procesos y las personas) simulando los objetivos y las acciones que realizaría un atacante	Control 20	RS-IM RC-IM	11.3	A.14.2.8 A.18.2.1 A.18.2.3	100,0%
25	Inteligencia de Seguridad de la Información	Identificación de fuentes de información que permitan a las organizaciones conocer el estado de amenazas, y ser proactivos en las defensas y decisiones que se deben tomar, minimizando el impacto causado por posibles ataques dirigidos.					100,0%

12	Protección de Datos	Los procesos y herramientas usados para prevenir una filtración, mitigando sus efectos y asegurando la privacidad e integridad de información crítica acorde a las directrices formales y procesos aprobados.	Control 13,14	PR-DS PR-AC	1.3- 1.4 3.6 4.1- 4.3 7.1- 7.3 8.7	A.8.3.1 A.9.1.1 A.10.1.1 - A.10.1.2 A.13.2.3 A.18.1.5	98,2%
1	Inventario de Hardware	Administración activa que permita conocer e inventariar solo los dispositivos autorizados que forman parte o deben pertenecer a la red, y bloquear el acceso al resto.	Control 1	ID-AM	2.4	A.8.1.1 A.9.1.2 A.13.1.1	95,0%
24	Gestión de Seguridad de la Información	Validar la existencia de implementación de seguridad de la información en las organizaciones, no solo como un rol; como un todo que dependiendo de la organización puede ser un equipo, presupuesto, y recursos tecnológicos debidamente dimensionados					87,5%
2	Inventario de Software	Administración activa que permita conocer e inventariar todo el software de la red, no solo el instalado, si no el que se puede ejecutar	Control 2	ID-AM		A.12.5.1 A.12.6.2	80,0%
11	Protección de redes inalámbricas	Los procesos y las herramientas usadas para rastrear/controlar/prevenir/corregir el uso seguro de redes inalámbricas en la red local (LAN) , access points, etc.	Control 15	PR-AC	4.3 11.1	A.10.1.1 A.12.4.1 A.12.7.1	80,0%
8	Protección de Email y Web	Minimizar la superficie de ataque y las oportunidades de los atacantes para manipular el comportamiento humano mediante la interacción con navegadores web y correo electrónico	Control 7	PR-PT			78,6%
9	Defensa de punto final (Endpoints)	Controlar la instalación, propagación y ejecución de código malicioso en diferentes puntos de la organización, mientras se optimiza la habilidad de defensa, recolección de información y se aplican acciones correctivas	Control 8	PR-PT DE-CM	5.1- 5.4	A.8.3.1 A.12.2.1 A.13.2.3	78,0%
5	Configuraciones de seguridad para dispositivos de red	Establecer, implementar y administrar activamente (rastros/reportes/corrección) las configuraciones seguras de los dispositivos de red, usando gestión de configuraciones seguras y un proceso de control de cambios.	Control 11	PR-IP	1.1- 1.2 2.2 6.2	A.9.1.2 A.13.1.1 A.13.1.3	75,0%

7	Defensa Perimetral	Detectar/prevenir/corregir el flujo de información que se transfiere entre diferentes redes con un enfoque de protección de datos	Control 12	DE-DP	1.1- 1.3 8.3 10.8 11.4	A.9.1.2 A.12.4.1 A.12.7.1 A.13.1.1 A.13.1.3 A.13.2.3	68,8%
4	Seguridad de Aplicaciones	Gestionar el ciclo de vida de todas las aplicaciones desarrolladas por la empresa, con el fin de prevenir, detectar, y corregir brechas de seguridad	Control 18	PR-IP	6.3 6.5- 6.7	A.9.4.5 A.12.1.4 A.14.2.1 A.14.2.6 - A.14.2.8	50,0%

VIII. Recomendaciones sobre hallazgos relevantes

Sobre **Gestión de seguridad de la información**

Un SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

Para el caso de entidades públicas de Colombia existe “El Modelo de Seguridad y Privacidad de la Información – MSPI”, que imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital.

Para que las entidades públicas incorporen la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y, en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

Sé encuentra alineado con el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y La Guía para la Administración del Riesgo y el Diseño Controles en entidades Públicas, este modelo pertenece al habilitador transversal de Seguridad y Privacidad, de la Política de Gobierno Digital. Y Se desarrolla mediante el Documento Maestro del Modelo de Seguridad y Privacidad de la Información y sus guías de orientación. Lo debe desarrollar el líder o encargado de Seguridad de la Información con el apoyo de toda la estructura organizacional.

Sobre **Monitoreo y análisis**

El Centro de Operaciones de Seguridad (SOC por sus siglas en inglés) brinda monitoreo a la red de datos, monitoreo a servidores, transacciones de bases de datos, diagnóstico de vulnerabilidades técnicas, pruebas de intrusión, administración de riesgos y alertas de amenazas de forma temprana.

Entre los servicios de un SOC están:

- Vigilancia permanente, acción inmediata (monitoreo y análisis).
- Visibilidad de amenazas en la red interna, sistemas en la nube.
- Consultoría y acompañamiento (consultoría especializada).
- Detección de amenazas de forma temprana.
- Análisis de vulnerabilidades.
- Pruebas de Ethical Hacking.
- Hardening de configuraciones
- **Atención y respuesta a incidentes.**
- Acceso a fuentes de inteligencia.

Sobre el **Endurecimiento y Configuraciones de Seguridad de Hardware y Software:**

El endurecimiento del sistema es un proceso para asegurar un sistema informático o un servidor eliminando los riesgos de ciberataques. El proceso consiste en eliminar o desactivar las aplicaciones del sistema, las cuentas de usuario y otras características en las que se pueden infiltrar los ciberatacantes para acceder a la red. Estas características, a veces conocidas como la superficie de ataque, a menudo sirven como puntos de entrada para las actividades cibernéticas maliciosas o los hackers.

El endurecimiento del sistema es importante porque la superficie de ataque de la red de una empresa o un individuo es uno de los lugares más vulnerables a los ciberataques. A través de los puntos de entrada de la superficie de ataque, los hackers, el malware y otras ciberamenazas pueden acceder a la información sensible de una organización. Con el endurecimiento del sistema, las empresas pueden reducir su vulnerabilidad a las ciberamenazas y la probabilidad de que una ciberamenaza acceda a su red.

Hay cinco tipos de hardening del sistema que ayudan a asegurar los elementos críticos de un sistema informático que los ciberatacantes suelen explotar, como las aplicaciones de software, el sistema operativo, el firmware, las bases de datos y las redes. Para llevar a cabo el endurecimiento del sistema con éxito, asegúrese de tener en cuenta las cinco categorías. Estos son los cinco tipos principales de hardening del sistema:

1. Endurecimiento del servidor

El endurecimiento del servidor se refiere a la protección de los puertos, las funciones, los datos y los permisos de un servidor. Un servidor es un ordenador potente que ofrece recursos, servicios o almacenamiento de datos a otros dispositivos en una red autorizada. Las técnicas para el endurecimiento del servidor incluyen la desactivación de los puertos USB cuando se enciende el sistema, la actualización periódica o la aplicación de parches en el software del servidor y la creación de contraseñas más fuertes para todos los usuarios autorizados a acceder al servidor.

2. Endurecimiento de aplicaciones de software

Con el endurecimiento de las aplicaciones de software, los usuarios u organizaciones añaden o actualizan las medidas de seguridad en todos los programas y aplicaciones de su red. Estas aplicaciones o software pueden incluir navegadores web, procesadores de texto o programas de hojas de cálculo. Los usuarios que implementan el endurecimiento de las aplicaciones de software actualizan los códigos de sus aplicaciones o añaden más tácticas de ciberseguridad basadas en el software.

3. Endurecimiento del sistema operativo

El endurecimiento del sistema operativo (OS) se refiere al proceso de asegurar los sistemas operativos de los dispositivos finales, como ordenadores o teléfonos móviles, dentro de su red. En informática, un sistema operativo es un tipo específico de software que maneja las funciones básicas de un dispositivo, como permitir que los programas se inicien y se ejecuten. Las tácticas para llevar a cabo el endurecimiento del sistema operativo incluyen la instalación o actualización de parches y la reducción del número de personas con autorización para el sistema operativo de su empresa.

Aunque están relacionados entre sí, el endurecimiento del sistema operativo y el de las aplicaciones de software son procesos distintos. El endurecimiento de las aplicaciones de software hace hincapié en la seguridad de los programas de terceros, es decir, del software creado por una empresa diferente a la que fabricó su dispositivo. El endurecimiento del sistema operativo, por su parte, se centra en mejorar la seguridad del software base que permite el funcionamiento de esas aplicaciones de terceros.

4. Endurecimiento de la base de datos

Con el endurecimiento de la base de datos, los usuarios aseguran tanto su base de datos digital como su sistema de gestión de bases de datos (DBMS). Una base de datos es el espacio de almacenamiento de la información valiosa de su organización a la que se accede digitalmente a través de los dispositivos o sistemas de su red. El SGBD, por su parte, es el software con el que los usuarios se relacionan cuando quieren acceder, almacenar, modificar o evaluar la información almacenada en una base de datos. Las estrategias para el endurecimiento de la base de datos incluyen la desactivación de las

funciones de la base de datos que no se necesitan, el cifrado de los recursos de la base de datos y la reducción de los privilegios de los usuarios.

5. Endurecimiento de la red

El endurecimiento de la red se refiere al proceso de asegurar los canales y sistemas de comunicación entre los servidores, los dispositivos finales y otra tecnología que opera en una red compartida. Dado que todos estos sistemas y dispositivos interactúan regularmente entre sí, una posible vulnerabilidad en uno de ellos podría llevar a la vulnerabilidad de toda la red. Las empresas o los particulares pueden mejorar el endurecimiento de la red instalando sistemas de detección de intrusos que adviertan la actividad sospechosa, estableciendo cortafuegos y cifrando el tráfico de la red.

Sobre **Escaneo y remediación de vulnerabilidades y Penetration Test:**

Es necesario llevar a cabo de forma continua (frecuentemente) la evaluación y mitigación de vulnerabilidades, ejercicios éticos (**Ethical Hacking**), para probar las deficiencias de seguridad en los activos críticos (*personas, procesos y tecnología*) de la compañía, valiéndose de técnicas y tácticas similares a las que usan los criminales; esto con el fin de identificar las brechas y cerrarlas antes que los criminales las encuentren, exploten y causen daños lamentables para la organización.

Sobre **Entrenamiento a usuarios:**

Evaluar el comportamiento de los colaboradores (factor humano) en una organización, ante los ataques más habituales en el campo de la ingeniería social, tratando de esta forma de identificar puntos fuertes y débiles sobre las políticas de seguridad, así como su nivel de conocimiento de forma automatizada con el valor agregado de contar con un esquema de concientización inmediata e indicadores de efectividad.

Los tipos de ataque pueden ser muy variados:

- Herramientas automatizadas que recogen correos electrónicos desde los buscadores web.
- Búsquedas en redes sociales de información publicada por los empleados, colaboradores, etc.
- Llamadas telefónicas suplantando personas clave, soportes, help desk, etc.
- Acceso físico a instalaciones validando controles de acceso desde el exterior y el interior.
- Ataques de Phishing.
- Etc.

Sobre **Protección de Datos (DLP)**

Un DLP es una herramienta que tiene como finalidad prevenir las fugas de información cuyo origen está dentro de la propia organización, de una manera activa y sin perder productividad. Estas herramientas suelen incorporar inteligencia artificial que les permite aprender sobre el tipo de documentos confidenciales que se utilizan y qué acciones llevan a cabo los usuarios sobre los mismos, para volverse cada vez más efectivas en la prevención de fugas de información.

Los DLP monitorizan la red de la organización para evitar las fugas de información antes de que se lleguen a producir. Una vez que detectan una posible fuga, alertan al usuario para que sea consciente de que la acción que está realizando atenta contra la confidencialidad de la empresa o contra una política de seguridad que vela por ella. Estas acciones tienen como objetivo concienciar a los miembros de la organización.

La monitorización de recursos por parte de un DLP no se limita exclusivamente a la red interna de la organización, ya que estas herramientas son capaces de extender su supervisión a dispositivos móviles, tanto Android como iOS. Los DLP son capaces de comprobar a qué correos corporativos se ha accedido. Además, tienen capacidad de comprobar y detener la transmisión de datos confidenciales desde la organización a aplicaciones de almacenamiento en la nube o redes sociales.

Para que la implantación de un DLP en la organización sea lo más sencilla posible, incorporan plantillas preconfiguradas según distintas normas o estándares como el RGPD, LPI, LSSI o PCI-DSS.

Otras funciones destacables de estas herramientas son:

- Las políticas creadas se pueden aplicar de diferente manera como, por ejemplo, por segmento de red, puerta de enlace, grupo de usuarios, etc. Cada organización podrá utilizar la que mejor se adapte a sus necesidades.
- La administración de estas herramientas se encuentra centralizada, lo que permite una gestión más sencilla y ágil.
- Inspección de múltiples tipos de ficheros y protocolos independientemente de que la información se transmita cifrada o no.
- Añaden marcas de agua, tanto visibles como invisibles a los ficheros para que en caso de fuga de información se pueda identificar a su responsable.

Los DLP son un tipo de herramientas que pueden prevenir muchas fugas de información en cualquier empresa y por consiguiente, la pérdida de reputación o incluso ser objeto de sanciones administrativas por incumplimiento normativo.

Sobre **Control y gestión en la nube**

La nube está modificando las operaciones de todo tipo de organizaciones, sin importar tamaño, industria o ubicación geográfica, con el objetivo de proteger los entornos informáticos cloud, así como sus aplicaciones y datos almacenados en la nube.

Desde su origen, la seguridad en la nube o ciberseguridad consta de las siguientes categorías:

- Seguridad de datos.
- Gestión de identidades y accesos (IAM, por sus siglas en inglés).
- Gobernanza (políticas de prevención, detección y mitigación de amenazas).
- Planificación de la retención de datos (DR) y la continuidad del negocio (BC).
- Cumplimiento legal.

IX. Plan de proyectos recomendados

A continuación, se detallan los proyectos recomendados (**ordenados en función del nivel de riesgo**), para mejorar el nivel de madurez relacionado con seguridad de la información, en concordancia con los hallazgos identificados en **Bellas Artes**.

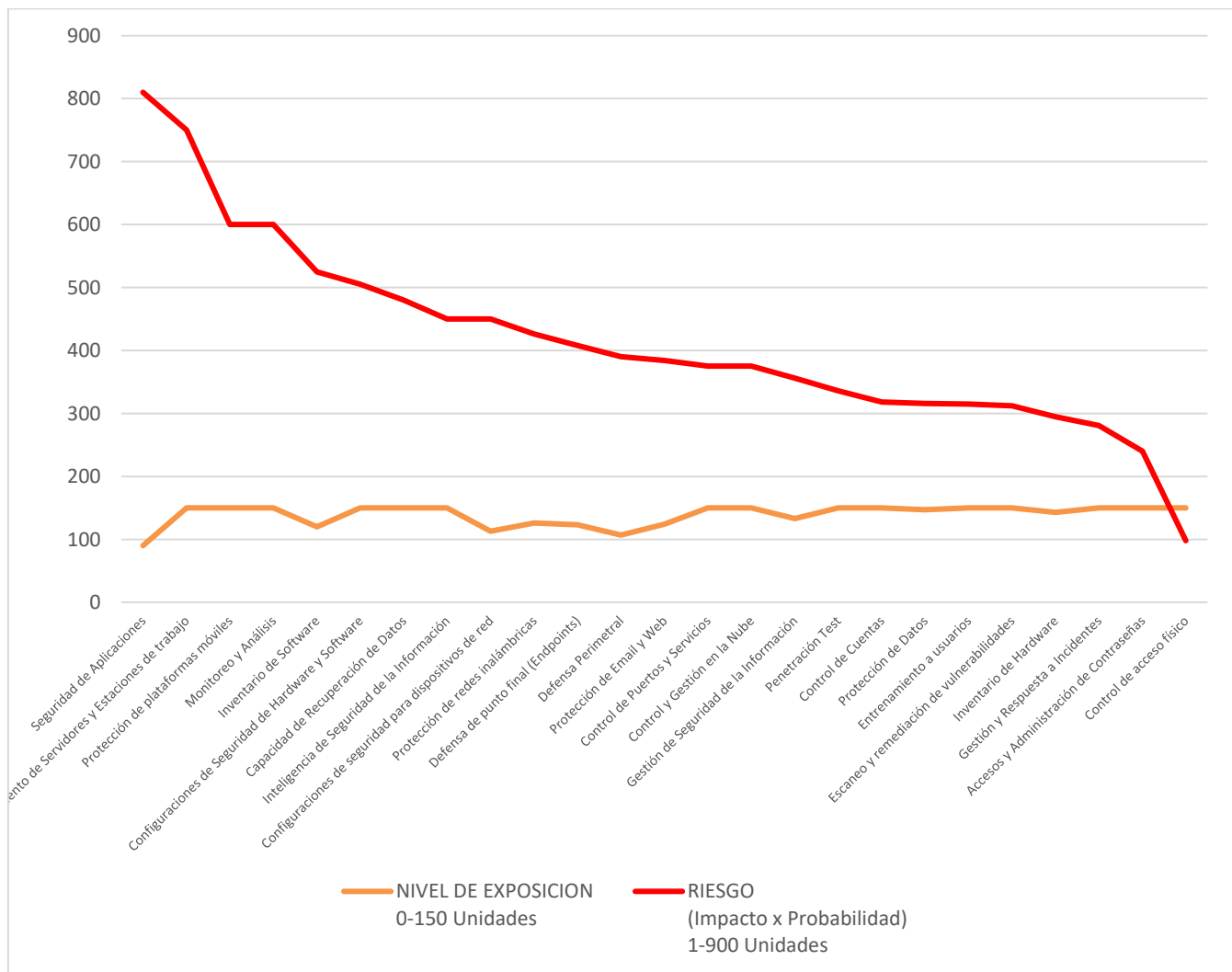


Ilustración 1 - Orden en función del nivel de riesgo de mayor a menor

Dentro del proceso de mejora recomendado, GMS pone a su disposición el personal profesional necesario para concretar los alcances de cada uno de los proyectos propuestos en función del presupuesto y prioridad que defina **BELLAS ARTES** dentro de su planificación.

⚠ NOTA IMPORTANTE: Se recomienda actualizar mínimo cada 6 meses el *Análisis de Nivel de Madurez*, en función de mantener las métricas del proceso de mejora continua vigentes.