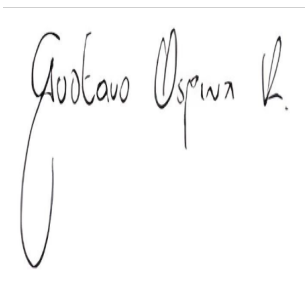
FLUJO DE APROBACIÓN

Fecha de entrega In-Ova: 21/03/2025 02:43 PM

Documentos electrónicos entregados para pago		
PROYECTO	**TIPO DE SOPORTE**	**N° FACTURA**
B. DIGITAL	FACTURA	FE400
SBPM	FACTURA	FE401
B. DIGITAL	FACTURA	FE402
SBPM	FACTURA	FE403

Contrato: 0375-25
Acreedor: JANIUM SAS
NIT: 830141046

QUIEN ENVIA:
Gustavo Adolfo Ospina Ruiz 2.
Enlace
QUIEN REVISA:






Gustavo Adolfo Ospina Ruiz 2. C.C/NIT 1037577751	Ana Isabel Estrada Castro 3. C.C/NIT 1000556765	Isabel Cristian Bernal Vinasco 4. C.C/NIT 32205329	Yakelin Vanegas Morales 5. C.C/NIT 1020395994

INFORME DE SUPERVISIÓN

CONTRATO N° 0375 DE 2025 ENTRE LA BIBLIOTECA PÚBLICA PILOTO DE MEDELLÍN PARA AMÉRICA LATINA Y JANIUM S.A.S. CON NIT: 830.141.046-4

SEGUIMIENTO ADMINISTRATIVO

0403213024

Fecha del informe:	**05 de marzo de 2025**
Tipo de informe:	Parcial
Lugar de ejecución:	Distrito Especial de Ciencia, Tecnología e Innovación de Medellín.
Supervisor (a):	Isabel Cristina Bernal Vinasco
Cédula supervisor (a):	32205329
Apoyo a la supervisión:	Ana Isabel Estrada Castro
Enlaces que participan:	1
Fecha de suscripción Secop II:	23 de enero de 2025
Fecha de inicio Secop II:	24 de enero de 2025
Fecha final Secop II:	31 de mayo de 2025
Otrosí ___ :	No Aplica

Proyecto	Valor Inicial Por Rubro:	(+) Otrosi N° 1	(+) Otrosi N° 2	(-) Liberaciones	Valor actual del contrato	Ejecutado	Disponible
B. DIGITAL	$ 6.509.386	$ 0	$ 0	$ 0	$ 6.509.386	$ 2.603.754	$ 3.905.632
SBPM	$ 52.924.318	$ 0	$ 0	$ 0	$ 52.924.318	$ 21.169.724	$ 31.754.594
					$ 0	$ 0	$ 0
					$ 0	$ 0	$ 0
					$ 0	$ 0	$ 0
Valor Contrato	**$ 59.433.704**	**$ 0**	**$ 0**	**$ 0**	**$ 59.433.704**	**$ 23.773.478**	**$ 35.660.226**

NOVEDADES DEL CONTRATO

Fecha de suspensión:	No aplica.
Fecha de reinicio:	No aplica.
Fecha terminación anticipada:	No aplica.

OBJETO DEL CONTRATO:

Suscripción al soporte, actualización, mantenimiento y alojamiento de los sistemas bibliográficos Janium por parte de la Biblioteca Pública Piloto de Medellín, el Sistema de Bibliotecas Públicas de Medellín y demás proyectos.

SEGUIMIENTO FINANCIERO

Estado actual:	**En Ejecución**
Cumplimiento objeto contractual:	**40,00 %**
Ejecución presupuestal:	**40,00 %**

Valor actual del contrato	Proyecto	Tipo de Soporte	N° Factura / Doc. Soporte	Fecha Soporte	% Ejecución	Valor a Pagar	Saldo Contrato
$ 59.433.704	B. DIGITAL	Factura	FE387	05-feb-2025	00,77 %	$ 460.422,00	$ 58.973.282,00
$ 59.433.704	SBPM	Factura	FE388	05-feb-2025	05,05 %	$ 2.538.463,00	$ 56.434.819,00
$ 59.433.704	SBPM	Factura	FE394	11-feb-2025	18,58 %	$ 8.046.399,00	$ 48.388.420,00
$ 59.433.704	B. DIGITAL	Factura	FE395	11-feb-2025	20,00 %	$ 841.455,00	$ 47.546.965,00
$ 59.433.704	B. DIGITAL	Factura	FE400	03-mar-2025	21,42 %	$ 841.455,00	$ 46.705.510,00
$ 59.433.704	SBPM	Factura	FE401	03-mar-2025	34,95 %	$ 8.046.399,00	$ 38.659.111,00
$ 59.433.704	B. DIGITAL	Factura	FE402	03-mar-2025	35,73 %	$ 460.422,00	$ 38.198.689,00
$ 59.433.704	SBPM	Factura	FE403	03-mar-2025	40,00 %	$ 2.538.463,00	$ 35.660.226,00

Factura	**FE400**
Proyecto:	B. DIGITAL
Subtotal:	$ 707.105
Iva:	$ 134.350
Total a Pagar:	**$ 841.455**

Factura	**FE401**
Proyecto:	SBPM
Subtotal:	$ 6.761.680
Iva:	$ 1.284.719
Total a Pagar:	**$ 8.046.399**

Factura	**FE402**
Proyecto:	B. DIGITAL
Subtotal:	$ 460.422
Iva:	$ 0
Total a Pagar:	**$ 460.422**

Factura	**FE403**
Proyecto:	SBPM
Subtotal:	$ 2.538.463
Iva:	$ 0
Total a Pagar:	**$ 2.538.463**

SEGUIMIENTO TÉCNICO

A continuación, se presentan los resultados de la verificación de las evidencias enviadas por el contratista, recopiladas una vez finalizado el mes FEBRERO de 2025:

1. Informe de Disponibilidad de Sistemas: Los niveles de disponibilidad cumplen con los parámetros establecidos, asegurando la continuidad en los servicios digitales:
- Sistema bibliográfico Janium SBPM – BPP (http://rbmam.janium.net): 99,97%
- Repositorio ENKI – BPP (http://bibliotecapiloto.janium.net): 100%
- Repositorio AHM (http://ahmedellin.janium.net): 99,97%

2. Copias de Seguridad: Realizó los respaldos diarios de las bases de datos de los 3 sistemas contratados, asegurando la integridad y seguridad de la información.

3. Seguimiento de Almacenamiento: Los niveles de uso de almacenamiento se mantienen estables y dentro de los rangos esperados:
- Janium SBPM: 38% ocupado
- Repositorio ENKI BPP: 71% ocupado
- Repositorio AHM: 73% ocupado

4. Soporte y Actualizaciones: Durante el mes se atendieron las siguientes cantidades de tickets de soporte, cumpliendo con los tiempos de atención establecidos:
- Janium SBPM: 64 tickets.
- Janium BPP: 22 tickets.
- Repositorio ENKI BPP: 5 ticket.
- Repositorio AHM: 5 ticket.

5. Seguridad de Sistemas: El contratista envió un informe de ciberseguridad que clasifica los riesgos en niveles alto, medio y bajo. En enero se identificaron librerías con riesgo alto, por lo que se solicitó al contratista un plan de mitigación. En febrero, tras las actualizaciones y correcciones aplicadas, dichos riesgos fueron solucionados. Actualmente, solo persisten riesgos de nivel medio y bajo, que el contratista se comprometió a gestionar trimestralmente.

6. Mejoras al Sistema: Durante el mes, se implementaron actualizaciones para optimizar la eficiencia y funcionalidad del sistema. Entre las principales mejoras se incluyen la corrección de fallos en el OPAC, la incorporación de parámetros para personalización de navegación y la actualización de bibliotecas de JavaScript para fortalecer la seguridad.

7. Capacitaciones: Se tiene claro que el contratista realiza capacitaciones ocasionales o programadas para el personal nuevo y antiguo de Circulación y Préstamos sobre el uso y la operación del sistema.

8. Envío de Respaldos: Se entregó el enlace de descarga de los respaldos de las bases de datos, según lo estipulado en el contrato.

9. Uso de Datos: Se reiteró la prohibición de utilizar los datos recolectados para fines no relacionados con los servicios contratados.

10. Borrado Seguro de Información: No se realizó ningún borrado de datos, ya que la relación contractual se encuentra vigente.

SEGUIMIENTO ASPECTOS ADMINISTRATIVOS DE LA EJECUCIÓN:

* Los pagos al sistema de seguridad social integral al momento de presentar el informe de actividades y/o la facturación fueron verificados y corresponden con el valor a pagar de conformidad con los honorarios fijados.
* En el período reportado no se impusieron multas ni sanciones.

SEGUIMIENTO POLIZAS DEL CONTRATO:

CUMPLIMIENTO

Amparo:	Valor	Vigencia Actual: Desde	Vigencia Actual: Hasta	Fecha aprobación SECOP II: Inicial	Fecha aprobación SECOP II: Modificación
Cumplimiento	$ 11.886.741	23-ene-2025	30-nov-2025	24-ene-2025	No aplica
Pago de salarios, prestaciones sociales legales e indemnizaciones laborales	$ 2.971.685	23-ene-2025	31-may-2028	24-ene-2025	No aplica
Calidad del Servicio	$ 11.886.741	23-ene-2025	30-nov-2025	24-ene-2025	No aplica
Estabilidad de la obra	No aplica	-	-	-	-
Calidad o Buen Funcionamiento	No aplica	-	-	-	-

Aseguradora:	SEGUROS DEL ESTADO S.A
N° de Póliza:	21-44-101462004

RESPONSABILIDAD CIVIL EXTRACONTRACTUAL

Amparo:	Valor	Vigencia Actual: Desde	Vigencia Actual: Hasta	Fecha aprobación SECOP II: Inicial	Fecha aprobación SECOP II: Modificación
Predios labores y operaciones	No aplica	-	-	-	-
Contratistas y subcontratista	No aplica	-	-	-	-
Vehiculos propios y no propios	No aplica	-	-	-	-

Aseguradora:	-
N° de Póliza:	-

ANEXOS AL PRESENTE INFORME:

No	Acta de inicio	No	Certificado Junta central de contadores
No	Acta de suspensión	No	Tarjeta Profesional Revisor Fiscal
No	Acta de reinicio	No	Informe de Gestión entregado por el proveedor (Firmado)
No	Acta de terminación ordinaria	No	Evidencias fotograficas (con Marca de la fecha que fue tomada sin repetir)
No	Contrato	Si	Evidencias pantallazos PC (Marca de la fecha del escritorio)
No	Otrosi N° 1	Si	Evidencias documentos (pdf. word. excel, otros)
No	Otrosi N° 2	No	Evidencias N° de la placa (Compra de Activos BPP)
Si	Factura Electrónica	No	Lista de asistencia (Firmados por asistentes)
No	Documento Soporte	Si	Seguridad Social Vencida + Soporte de Pago
No	Cupon de pago	Si	Certificado Parafiscales (Representante Legal)
No	Cuenta de Cobro	No	Certificado Parafiscales (Revisor Fiscal)
No	Remisiones (con fecha y firma)	No	Otro: _____

Total Anexos:	5

DIAN

FACTURA ELECTRÓNICA DE VENTA

Janium

Representación Gráfica

Datos del Documento

Código Único de Factura - CUFE :
49b7582c9978e769f51887bc50c647e526b05a10eda72ae50db3471953b8d14ab0b7d6a7a9e869c409f07ebe4bf65bbc

Número de Factura: FE-400
Fecha de Emisión: 03/03/2025
Fecha de Vencimiento: 02/04/2025
Tipo de Operación: 10 - Estándar

Forma de pago: Crédito
Medio de Pago: Transferencia Débito Interbancario
Orden de pedido:
Fecha de orden de pedido:

Datos del Emisor / Vendedor

Razón Social: JANIUM SAS
Nombre Comercial: JANIUM SAS
Nit del Emisor: 830141046
Tipo de Contribuyente: Persona Jurídica
Régimen Fiscal: R-99-PN
Responsabilidad tributaria: ZZ - No aplica
Actividad Económica: 6201

País: Colombia
Departamento: Bogotá
Municipio / Ciudad: Bogotá, D.c.
Dirección: CL 93 11 A 28 OF 601
Teléfono / Móvil: 6017960010
Correo: cjh@bbhh.com.co

Datos del Adquiriente / Comprador

Nombre o Razón Social: BIBLIOTECA PÚBLICA PILOTO DE MEDELLÍN PARA AMÉRICA LATINA
Tipo de Documento: NIT
Número Documento: 890980150
Tipo de Contribuyente: Persona Jurídica
Régimen fiscal: R-99-PN
Responsabilidad tributaria: ZZ - No aplica

País: Colombia
Departamento: Antioquia
Municipio / Ciudad: Medellín
Dirección: CARRERA 64 50 32
Teléfono / Móvil: 6044600590
Correo: 890980150@scol.com.co

Detalles de Productos

Nro.	Código	Descripción	U/M	Cantidad	Precio unitario	Descuento detalle	Recargo detalle	IMPUESTOS				Precio unitario de venta
								IVA	%	INC	%	
1	Soporte y Actualización para el Sistema Enki BPP Digital periodo enero a mayo de 2025	Soporte y Actualización para el Sistema Enki BPP Digital periodo enero a mayo de 2025	BW	1,00	$ 707.105,04	$ 0,00	$ 0,00	$ 134.349,96	19.00			$ 707.105,04

Notas Finales

Pago 2 de 5 PRIMER SEMESTRE 2025: CONTRATO No. 2025-0375. Mantenimiento de ENKI con tamaño para licencias ilimitadas de OPAC+ STAFF Soporte y Actualización para el Sistema Enki BPP Digital. Por favor Consignar a la Cuenta Corriente No 073015208 del Banco BBVA.
Linea de negocio:

Datos Totales

Documento generado el:
03/03/2025 16:12:21
Documento validado por la DIAN:
03/03/2025 16:12:22
XML Generado por: Solución Gratuita DIAN
800197268
PDF Generado por: Solución Gratuita DIAN
Nit:800197268

MONEDA	COP
TASA DE CAMBIO	0

Subtotal		707105.04
Descuento detalle		0,00
Recargo detalle		0,00
Total Bruto Factura		707105.04
IVA		134349.96
INC		0,00
Bolsas		0,00
Otros impuestos		0
Total impuesto (=)		134349.96
Total neto factura (=)		841455
Descuento Global (-)		0,00
Recargo Global (+)		0,00
Total factura (=)	**COP $**	$ 841455

Valores informativos

ANTICIPOS	
Anticipos	0

RETENCIONES	
Rete fuente	24748.68
Rete IVA	0,00
Rete ICA	0,00

MONEDA	COP
TASA DE CAMBIO	

Subtotal		707.105,04
Descuento detalle		0,00
Recargo detalle		0,00
Total Bruto Factura		707.105,04
IVA		134.349,96
INC		0,00
Bolsas		0,00
Otros impuestos		0,00
Total impuesto (=)		134.349,96
Total neto factura (=)		841.455,00
Descuento Global (-)		0,00
Recargo Global (+)		0,00
Total factura (=)	**COP $**	$ 841.455,00

Valores informativos

ANTICIPOS	
Anticipos	0,00

RETENCIONES	
Rete fuente	24.748,68
Rete IVA	0,00
Rete ICA	0,00

Numero de Autorización: 18764084891259 Rango desde: 375 Rango hasta: 3000 Vigencia: 2026-06-06

DIAN

FACTURA ELECTRÓNICA DE VENTA

Janium

Representación Gráfica

Datos del Documento

Código Único de Factura - CUFE :
eaa33ddd677ad795a3a0a0ba9ca10f62ea4c2354ea38645301071bfa3029842a258e99be6dc73711016b6ae5f22f692e

Número de Factura: FE-401
Fecha de Emisión: 03/03/2025
Fecha de Vencimiento: 02/04/2025
Tipo de Operación: 10 - Estándar

Forma de pago: Crédito
Medio de Pago: Transferencia Débito Interbancario
Orden de pedido:
Fecha de orden de pedido:

Datos del Emisor / Vendedor

Razón Social: JANIUM SAS
Nombre Comercial: JANIUM SAS
Nit del Emisor: 830141046
Tipo de Contribuyente: Persona Jurídica
Régimen Fiscal: R-99-PN
Responsabilidad tributaria: ZZ - No aplica
Actividad Económica: 6201

País: Colombia
Departamento: Bogotá
Municipio / Ciudad: Bogotá, D.c.
Dirección: CL 93 11 A 28 OF 601
Teléfono / Móvil: 6017960010
Correo: cjh@bbhh.com.co

Datos del Adquiriente / Comprador

Nombre o Razón Social: BIBLIOTECA PÚBLICA PILOTO DE MEDELLÍN PARA AMÉRICA LATINA
Tipo de Documento: NIT
Número Documento: 890980150
Tipo de Contribuyente: Persona Jurídica
Régimen fiscal: R-99-PN
Responsabilidad tributaria: ZZ - No aplica

País: Colombia
Departamento: Antioquia
Municipio / Ciudad: Medellín
Dirección: CARRERA 64 50 32
Teléfono / Móvil: 6044600590
Correo: 890980150@scol.com.co

Detalles de Productos

								IMPUESTOS				Precio unitario de venta
Nro.	Código	Descripción	U/M	Cantidad	Precio unitario	Descuento detalle	Recargo detalle	IVA	%	INC	%	
1	Soporte y Actualización para el Sistema Janium de enero a mayo de 2025	Soporte y Actualización para el Sistema Janium de enero a mayo de 2025	BW	1,00	$ 6.054.575,83	$ 0,00	$ 0,00	$ 1.150.369,41	19.00			$ 6.054.575,83
2	Soporte y Actualización para el Sistema Enki del AHM periodo enero a mayo de 2025	Soporte y Actualización para el Sistema Enki del AHM periodo enero a mayo de 2025	BW	1,00	$ 707.104,00	$ 0,00	$ 0,00	$ 134.349,76	19.00			$ 707.104,00

Notas Finales

Pago 2 de 5 PRIMER SEMESTRE 2025: CONTRATO No. 2025-0375. Mantenimiento de JANIUM ULTIMATE con tamaño para licencias de staff y OPAC ilimitadas Janium Ultimate incluye: Control Bibliográfico, Autoridades, Circulación, Control de Suscripciones, Adquisiciones, OAI /PMH, SIP 2 (1), OPAC ilimitado y Licencia de Staff ILIMITADA. Mantenimiento de ENKI con tamaño para licencias ilimitadas de OPAC+ STAFF Soporte y Actualización para el Sistema Enki del AHM. Por favor Consignar a la Cuenta Corriente No 073015208 del Banco BBVA.
Linea de negocio:

Datos Totales

Documento generado el:
03/03/2025 16:22:45
Documento validado por la DIAN:
03/03/2025 16:22:46
XML Generado por: Solución Gratuita DIAN
800197268
PDF Generado por: Solución Gratuita DIAN
Nit:800197268

MONEDA	COP
TASA DE CAMBIO	0

Subtotal		6761679.83
Descuento detalle		0,00
Recargo detalle		0,00
Total Bruto Factura		6761679.83
IVA		1284719.17
INC		0,00
Bolsas		0,00
Otros impuestos		0
Total impuesto (=)		1284719.17
Total neto factura (=)		8046399
Descuento Global (-)		0,00
Recargo Global (+)		0,00
Total factura (=)	**COP $**	$ 8046399

Valores informativos

ANTICIPOS	
Anticipos	0

RETENCIONES	
Rete fuente	236658.79
Rete IVA	0,00
Rete ICA	0,00

MONEDA	COP
TASA DE CAMBIO	

Subtotal		6.761.679,83
Descuento detalle		0,00
Recargo detalle		0,00
Total Bruto Factura		6.761.679,83
IVA		1.284.719,17
INC		0,00
Bolsas		0,00
Otros impuestos		0,00
Total impuesto (=)		1.284.719,17
Total neto factura (=)		8.046.399,00
Descuento Global (-)		0,00
Recargo Global (+)		0,00
Total factura (=)	**COP $**	$ 8.046.399,00

Valores informativos

ANTICIPOS	
Anticipos	0,00

RETENCIONES	
Rete fuente	236.658,79
Rete IVA	0,00
Rete ICA	0,00

Numero de Autorización: 18764084891259 Rango desde: 375 Rango hasta: 3000 Vigencia: 2026-06-06

DIAN

FACTURA ELECTRÓNICA DE VENTA

Janium

Representación Gráfica

Datos del Documento

Código Único de Factura - CUFE :
acd01558b50f2761d1b250bca1d8ab3eb30031ae73d077416f506e605f23ad69ee8e2a8aebeab5d6efa01734940d860b

Número de Factura: FE-402
Fecha de Emisión: 03/03/2025
Fecha de Vencimiento: 02/04/2025
Tipo de Operación: 10 - Estándar

Forma de pago: Crédito
Medio de Pago: Transferencia Débito Interbancario
Orden de pedido:
Fecha de orden de pedido:

Datos del Emisor / Vendedor

Razón Social: JANIUM SAS
Nombre Comercial: JANIUM SAS
Nit del Emisor: 830141046
Tipo de Contribuyente: Persona Jurídica
Régimen Fiscal: R-99-PN
Responsabilidad tributaria: ZZ - No aplica
Actividad Económica: 6201

País: Colombia
Departamento: Bogotá
Municipio / Ciudad: Bogotá, D.c.
Dirección: CL 93 11 A 28 OF 601
Teléfono / Móvil: 6017960010
Correo: cjh@bbhh.com.co

Datos del Adquiriente / Comprador

Nombre o Razón Social: BIBLIOTECA PÚBLICA PILOTO DE MEDELLÍN PARA AMÉRICA LATINA
Tipo de Documento: NIT
Número Documento: 890980150
Tipo de Contribuyente: Persona Jurídica
Régimen fiscal: R-99-PN
Responsabilidad tributaria: ZZ - No aplica

País: Colombia
Departamento: Antioquia
Municipio / Ciudad: Medellín
Dirección: CARRERA 64 50 32
Teléfono / Móvil: 6044600590
Correo: 890980150@scol.com.co

Detalles de Productos

Nro.	Código	Descripción	U/M	Cantidad	Precio unitario	Descuento detalle	Recargo detalle	IMPUESTOS				Precio unitario de venta
								IVA	%	INC	%	
1	Servicio de almacenamiento de objetos digitales en la nube JaniumNet para la BPP por un espacio de 500 GB por el periodo Enero a Mayo de 2025	Servicio de almacenamiento de objetos digitales en la nube JaniumNet para la BPP por un espacio de 500 GB por el periodo Enero a Mayo de 2025	BW	1,00	$ 460.422,00	$ 0,00	$ 0,00					$ 460.422,00

Notas Finales

Pago 2 de 5 PRIMER SEMESTRE 2025: CONTRATO No. 2025-0375. 500 GB Espacio de almacenamiento en disco adicional anual Servicio (5 MESES) de almacenamiento de objetos digitales en la nube JaniumNet para la BPP, por un espacio de 500 GB. Favor consignar a la cuenta corriente No 073015208 del Banco BBVA.
Linea de negocio:

Datos Totales

Documento generado el:
03/03/2025 16:28:14
Documento validado por la DIAN:
03/03/2025 16:28:15
XML Generado por: Solución Gratuita DIAN
800197268
PDF Generado por: Solución Gratuita DIAN
Nit:800197268

MONEDA	COP
TASA DE CAMBIO	0

Subtotal		460422
Descuento detalle		0,00
Recargo detalle		0,00
Total Bruto Factura		460422
IVA		0,00
INC		0,00
Bolsas		0,00
Otros impuestos		0
Total impuesto (=)		0
Total neto factura (=)		460422
Descuento Global (-)		0,00
Recargo Global (+)		0,00
Total factura (=)	**COP $**	$ 460422

Valores informativos

ANTICIPOS	
Anticipos	0

RETENCIONES	
Rete fuente	16114.77
Rete IVA	0,00
Rete ICA	0,00

MONEDA	COP
TASA DE CAMBIO	

Subtotal		460.422,00
Descuento detalle		0,00
Recargo detalle		0,00
Total Bruto Factura		460.422,00
IVA		0,00
INC		0,00
Bolsas		0,00
Otros impuestos		0,00
Total impuesto (=)		0,00
Total neto factura (=)		460.422,00
Descuento Global (-)		0,00
Recargo Global (+)		0,00
Total factura (=)	**COP $**	$ 460.422,00

Valores informativos

ANTICIPOS	
Anticipos	0,00

RETENCIONES	
Rete fuente	16.114,77
Rete IVA	0,00
Rete ICA	0,00

Numero de Autorización: 18764084891259 Rango desde: 375 Rango hasta: 3000 Vigencia: 2026-06-06

DIAN

FACTURA ELECTRÓNICA DE VENTA

Janium

Representación Gráfica

Datos del Documento

Código Único de Factura - CUFE :
44758d3f29c4152b0abb5da1902bc43bc1be0210dc20f51612e4711d918263d1aa25e2a5a301788d029debc1a03a10af

Número de Factura: FE-403
Fecha de Emisión: 03/03/2025
Fecha de Vencimiento: 02/04/2025
Tipo de Operación: 10 - Estándar
Forma de pago: Crédito
Medio de Pago: Transferencia Débito Interbancario
Orden de pedido:
Fecha de orden de pedido:

Datos del Emisor / Vendedor

Razón Social: JANIUM SAS
Nombre Comercial: JANIUM SAS
Nit del Emisor: 830141046
Tipo de Contribuyente: Persona Jurídica
Régimen Fiscal: R-99-PN
Responsabilidad tributaria: ZZ - No aplica
Actividad Económica: 6201
País: Colombia
Departamento: Bogotá
Municipio / Ciudad: Bogotá, D.c.
Dirección: CL 93 11 A 28 OF 601
Teléfono / Móvil: 6017960010
Correo: cjh@bbhh.com.co

Datos del Adquiriente / Comprador

Nombre o Razón Social: BIBLIOTECA PÚBLICA PILOTO DE MEDELLÍN PARA AMÉRICA LATINA
Tipo de Documento: NIT
Número Documento: 890980150
Tipo de Contribuyente: Persona Jurídica
Régimen fiscal: R-99-PN
Responsabilidad tributaria: ZZ - No aplica
País: Colombia
Departamento: Antioquia
Municipio / Ciudad: Medellín
Dirección: CARRERA 64 50 32
Teléfono / Móvil: 6044600590
Correo: 890980150@scol.com.co

Detalles de Productos

Nro.	Código	Descripción	U/M	Cantidad	Precio unitario	Descuento detalle	Recargo detalle	IMPUESTOS				Precio unitario de venta
								IVA	%	INC	%	
1	Servicio de almacenamiento de objetos digitales en la nube JaniumNet para el SBPM, por un espacio de 500 GB, por el período de enero a mayo 2025	Servicio de almacenamiento de objetos digitales en la nube JaniumNet para el SBPM, por un espacio de 500 GB, por el período de enero a mayo 2025	BW	1,00	$ 460.422,40	$ 0,00	$ 0,00					$ 460.422,40
2	Servicio de almacenamiento de objetos digitales en JaniumNet para el AHM, por un espacio de 1,5 TeraBytes periodo enero a mayo 2025	Servicio de almacenamiento de objetos digitales en JaniumNet para el AHM, por un espacio de 1,5 TeraBytes periodo enero a mayo 2025	BW	3,00	$ 460.422,00	$ 0,00	$ 0,00					$ 1.381.266,00
3	Suscripción Anual Servicio Janium Business Intelligence periodo de enero a mayo de 2025	Suscripción Anual Servicio Janium Business Intelligence periodo de enero a mayo de 2025	BW	0,50	$ 809.797,20	$ 0,00	$ 0,00					$ 404.898,60
4	Workflow para Procesar Imágenes para Acercamiento Progresivo periodo enero a mayo 2025	Workflow para Procesar Imágenes para Acercamiento Progresivo periodo enero a mayo 2025	BW	1,00	$ 291.876,00	$ 0,00	$ 0,00					$ 291.876,00

Notas Finales

Pago 2 de 5 PRIMER SEMESTRE 2025: CONTRATO No. 2025-0375. 500 GB Espacio de almacenamiento en disco adicional anual Servicio (5 MESES) de almacenamiento de objetos digitales en la nube JaniumNet para el SBPM, por un espacio de 500GB. 500 GB Espacio de almacenamiento en disco adicion al anual Servicio (5 MESES) de almacenamiento de objetos digitales en la nube JaniumNet para el AHM, por un espacio de 1,5 TeraBytes. Suscripción anu al a JaniumBI Suscripción (5 MESES) al servicio Business Inteligence de Janium. Workflow para Procesar Imágenes para Acercamiento Progresivo (suscrip ción anual) Módulo de Workflow BPP (5 MESES). Favor consignar a la cuenta corriente No 073015208 del Banco BBVA.
Linea de negocio:

Datos Totales

Documento generado el:
03/03/2025 16:39:09
Documento validado por la DIAN:
03/03/2025 16:39:10
XML Generado por: Solución Gratuita DIAN
800197268
PDF Generado por: Solución Gratuita DIAN Nit:800197268

MONEDA	COP
TASA DE CAMBIO	0

Subtotal	2538463
Descuento detalle	0,00
Recargo detalle	0,00
Total Bruto Factura	2538463
IVA	0,00
INC	0,00
Bolsas	0,00
Otros impuestos	0
Total impuesto (=)	0
Total neto factura (=)	2538463
Descuento Global (-)	0,00
Recargo Global (+)	0,00
Total factura (=) COP $	$ 2538463

Valores informativos

ANTICIPOS	
Anticipos	0

RETENCIONES	
Rete fuente	88846.2
Rete IVA	0,00
Rete ICA	0,00

MONEDA	COP
TASA DE CAMBIO	

Subtotal	2.538.463,00
Descuento detalle	0,00
Recargo detalle	0,00
Total Bruto Factura	2.538.463,00
IVA	0,00
INC	0,00
Bolsas	0,00
Otros impuestos	0,00
Total impuesto (=)	0,00
Total neto factura (=)	2.538.463,00
Descuento Global (-)	0,00
Recargo Global (+)	0,00
Total factura (=) COP $	$ 2.538.463,00

Valores informativos

ANTICIPOS	
Anticipos	0,00

RETENCIONES	
Rete fuente	88.846,20
Rete IVA	0,00
Rete ICA	0,00

Numero de Autorización: 18764084891259 Rango desde: 375 Rango hasta: 3000 Vigencia: 2026-06-06

Janium Technology, S.A. de C.V.

Av. Insurgentes Sur 4342 Int 12 B
Colonia Tlalpan Centro,
Alc. Tlalpan
14000 Ciudad de México
MEXICO

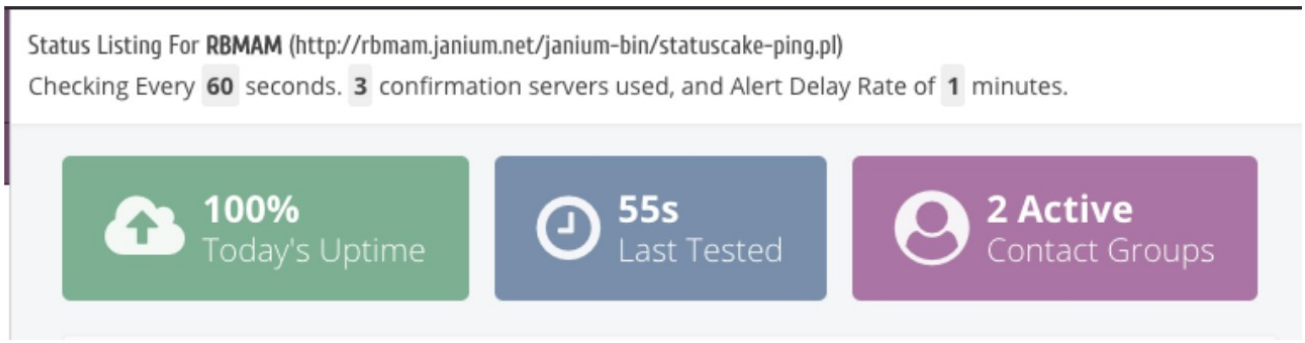
T 52 55 4170-8453
www.janium.com

Ciudad de México, a 03 de marzo de 2025

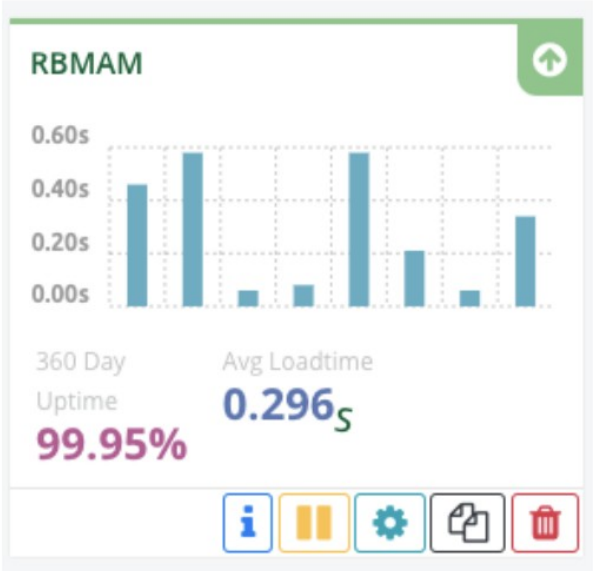
Isabel Cristina Bernal Vinasco
Subdirector de Contenidos y Patrimonio / Biblioteca Pública Piloto

Por este medio entregamos la estadística de disponibilidad del sistema Janium del ***Sistema de Bibliotecas Públicas de Medellín*** correspondiente al mes de febrero del año en curso. Le informo que, para monitorear la disponibilidad del sistema Janium, utilizamos los servicios de StatusCake.

En esta herramienta de monitorización de sitios web se ha configurado el sitio http://rbmam.janium.net como se puede observar en la siguiente imagen:



El sitio http://rbmam.janium.net es monitoreado cada 60 segundos por 3 servidores (ubicados en diferentes zonas geográficas) y genera alertas en caso de fallo en los tiempos de respuesta o falla de disponibilidad del sitio (la alerta se remite a la Gerencia de Soporte Técnico de Janium).



Janium Technology, S.A. de C.V.

Av. Insurgentes Sur 4342 Int 12 B
Colonia Tlalpan Centro,
Alc. Tlalpan
14000 Ciudad de México
MEXICO

T 52 55 4170-8453
www.janium.com

Se anexa el gráfico de Uptime Checks del mes de febrero que muestra el porcentaje de disponibilidad obtenida en este periodo.

Date ↑↓	Uptime ↑↓
February 2025	99.97%

Sin más, le remitimos un cordial saludo.



Luz María Alemán Rentería.
Ejecutivo Soporte Técnico
Janium

Janium Technology, S.A. de C.V.

Av. Insurgentes Sur 4342 Int 12 B
Colonia Tlalpan Centro,
Alc. Tlalpan
14000 Ciudad de México
MEXICO

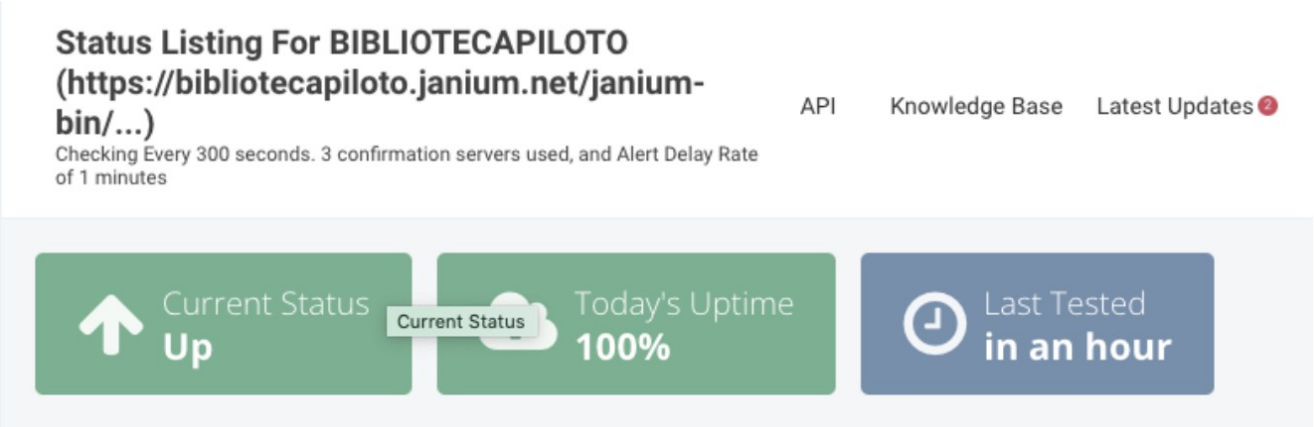
T 52 55 4170-8453
www.janium.com

Ciudad de México, a 03 de marzo de 2025

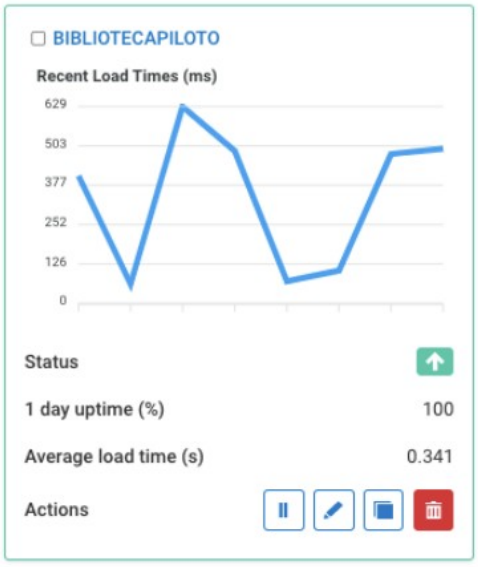
Isabel Cristina Bernal Vinasco
Subdirector de Contenidos y Patrimonio / Biblioteca Pública Piloto

Por este medio entregamos la estadística de disponibilidad del sistema Janium de la ***Biblioteca Pública Piloto*** correspondiente al mes de febrero del año en curso. Le informo que, para monitorear la disponibilidad del sistema Janium, utilizamos los servicios de StatusCake.

En esta herramienta de monitorización de sitios web se ha configurado el sitio http://bibliotecapiloto.janium.net como se puede observar en la siguiente imagen:



El sitio http://bibliotecapiloto.janium.net es monitoreado cada 60 segundos por 3 servidores (ubicados en diferentes zonas geográficas) y genera alertas en caso de fallo en los tiempos de respuesta o falla de disponibilidad del sitio (la alerta se remite a la Gerencia de Soporte Técnico de Janium).



Janium Technology, S.A. de C.V.

Av. Insurgentes Sur 4342 Int 12 B
Colonia Tlalpan Centro,
Alc. Tlalpan
14000 Ciudad de México
MEXICO

T 52 55 4170-8453
www.janium.com

Se anexa el gráfico de Uptime Checks del mes de febrero que muestra el porcentaje de disponibilidad obtenida en este periodo.

Date ↑↓	Uptime ↑↓
February 2025	100%

Sin más, le remitimos un cordial saludo.



Luz María Alemán Rentería.
Ejecutivo Soporte Técnico
Janium

Janium Technology, S.A. de C.V.

Av. Insurgentes Sur 4342 Int 12 B
Colonia Tlalpan Centro,
Alc. Tlalpan
14000 Ciudad de México
MEXICO

T 52 55 4170-8453
www.janium.com

Ciudad de México, a 03 de marzo de 2025

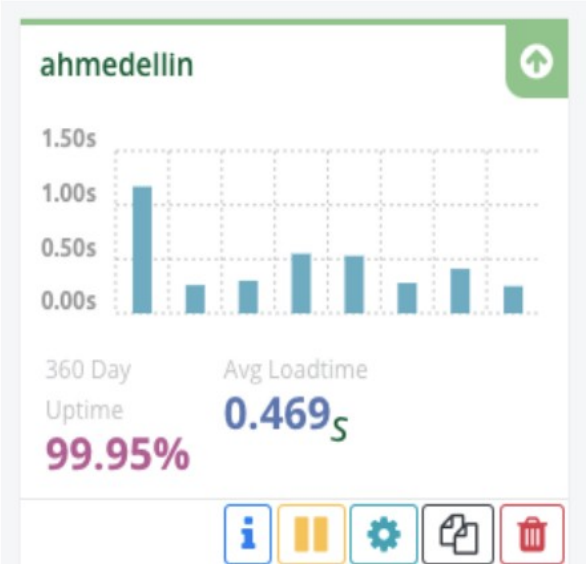
Isabel Cristina Bernal Vinasco
Subdirector de Contenidos y Patrimonio / Biblioteca Pública Piloto

Por este medio entregamos la estadística de disponibilidad del sistema Janium del ***Archivo Histórico de Medellín*** correspondiente al mes de febrero del año en curso. Le informo que, para monitorear la disponibilidad del sistema Janium, utilizamos los servicios de StatusCake.

En esta herramienta de monitorización de sitios web se ha configurado el sitio http://ahmedellin.janium.net como se puede observar en la siguiente imagen:



El sitio http://ahmedellin.janium.net es monitoreado cada 60 segundos por 3 servidores (ubicados en diferentes zonas geográficas) y genera alertas en caso de fallo en los tiempos de respuesta o falla de disponibilidad del sitio (la alerta se remite a la Gerencia de Soporte Técnico de Janium).



Janium Technology, S.A. de C.V.

Av. Insurgentes Sur 4342 Int 12 B
Colonia Tlalpan Centro,
Alc. Tlalpan
14000 Ciudad de México
MEXICO

T 52 55 4170-8453
www.janium.com

Se anexa el gráfico de Uptime Checks del mes de febrero que muestra el porcentaje de disponibilidad obtenida en este periodo.

Date ↑↓	Uptime ↑↓
February 2025	99.97%

Sin más, le remitimos un cordial saludo.



Luz María Alemán Rentería.
Ejecutivo Soporte Técnico
Janium

Janium Technology, S.A. de C.V.

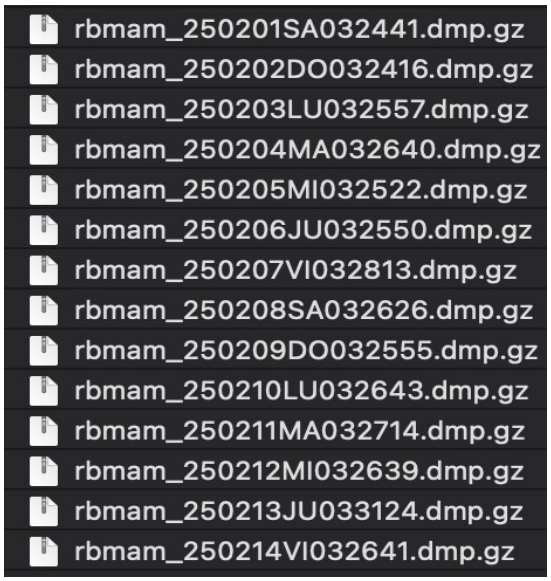
Av. Insurgentes Sur 4342 Int 12 B
Colonia Tlalpan Centro,
Alc. Tlalpan
14000 Ciudad de México
MEXICO

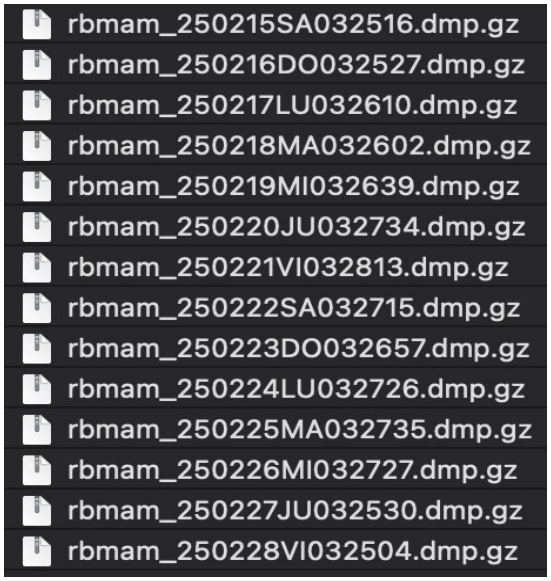
T 52 55 4170-8453
www.janium.com

Ciudad de México, a 03 de marzo de 2024.

Isabel Cristina Bernal Vinasco
Subdirector de Contenidos y Patrimonio / Biblioteca Pública Piloto

Por este medio, mostramos el listado de respaldos diarios de la base de datos del sistema Janium, perteneciente al ***Sistema de Bibliotecas Públicas de Medellín*** correspondiente al mes de febrero del año en curso; que se realiza como parte de las actividades de administración del sistema JaniumNet.





Así mismo me permito informarle, que si usted desea tener acceso a dichos respaldos, puede solicitar las credenciales de acceso en el correo: soporte@janium.com sin más, le remitimos un cordial saludo.

Luz María Alemán Rentería.
Ejecutivo Soporte Técnico
Janium

Janium Technology, S.A. de C.V.

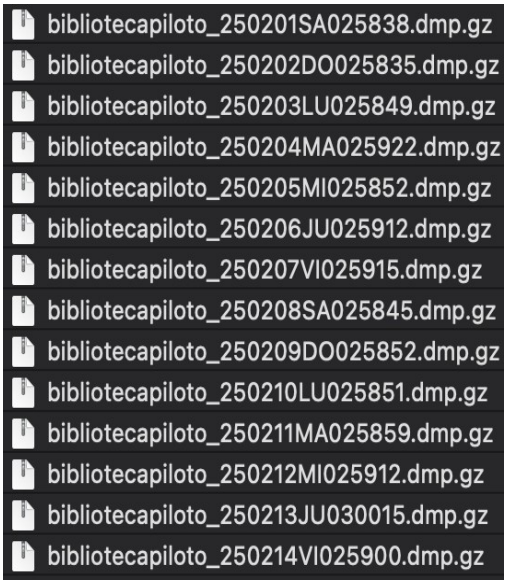
Av. Insurgentes Sur 4342 Int 12 B
Colonia Tlalpan Centro,
Alc. Tlalpan
14000 Ciudad de México
MEXICO

T 52 55 4170-8453
www.janium.com

Ciudad de México, a 03 de marzo de 2025.

Isabel Cristina Bernal Vinasco
Subdirector de Contenidos y Patrimonio / Biblioteca Pública Piloto

Por este medio, mostramos el listado de respaldos diarios de la base de datos del sistema Janium, perteneciente a la ***Biblioteca Pública Pilloto*** correspondiente al mes de febrero del año en curso; que se realiza como parte de las actividades de administración del sistema JaniumNet.





Así mismo me permito informarle, que si usted desea tener acceso a dichos respaldos, puede solicitar las credenciales de acceso en el correo: soporte@janium.com sin más, le remitimos un cordial saludo.

Luz María Alemán Rentería.
Ejecutivo Soporte Técnico
Janium

Janium Technology, S.A. de C.V.

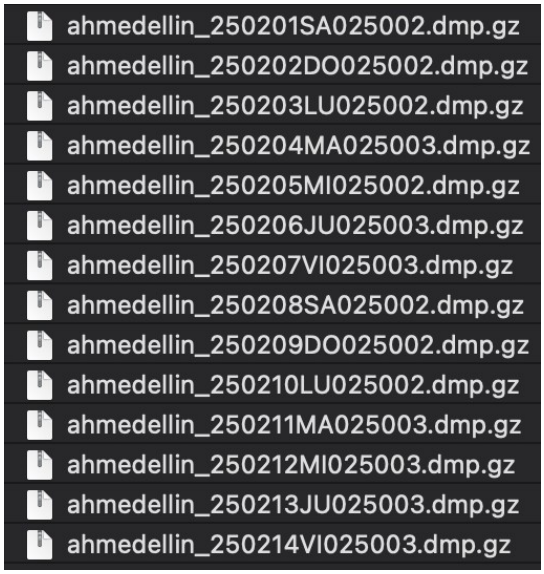
Av. Insurgentes Sur 4342 Int 12 B
Colonia Tlalpan Centro,
Alc. Tlalpan
14000 Ciudad de México
MEXICO

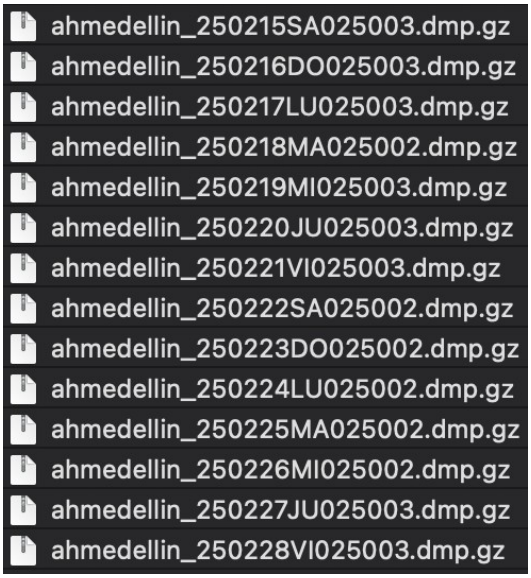
T 52 55 4170-8453
www.janium.com

Ciudad de México, a 03 de marzo de 2025.

Isabel Cristina Bernal Vinasco
Subdirector de Contenidos y Patrimonio / Biblioteca Pública Piloto

Por este medio, mostramos el listado de respaldos diarios de la base de datos del sistema Janium, perteneciente al **Archivo Histórico de Medellín** correspondiente al mes de febrero del año en curso; que se realiza como parte de las actividades de administración del sistema JaniumNet.





Así mismo me permito informarle, que si usted desea tener acceso a dichos respaldos, puede solicitar las credenciales de acceso en el correo: soporte@janium.com sin más, le remitimos un cordial saludo.

Luz María Alemán Rentería.
Ejecutivo Soporte Técnico
Janium

Janium S.A.S.

Calle 93 #11A - 28
Oficina 601 Edificio
Capital Park
Bogotá, Colombia

Tel. (571) 344 17 60
www.janium.com

Ciudad de México a 03 de marzo de 2025.

Isabel Cristina Bernal Vinasco
Subdirector de Contenidos y Patrimonio
Biblioteca Pública Piloto
Presente

El almacenamiento para el Sistema Janium de la Biblioteca Pública Piloto y el Sistema de Bibliotecas Públicas de Medellín tiene actualmente este uso:

- Espacio asignado 259G
- Espacio ocupado 190G

El almacenamiento para el Sistema Enki de la Biblioteca Pública Piloto y el Sistema de Bibliotecas Públicas de Medellín tiene actualmente este uso:

- Espacio asignado 424G
- Espacio ocupado 355G

El almacenamiento para el Sistema Janium del Archivo Histórico de Medellín tiene actualmente este uso:

- Espacio asignado 1.1T
- Espacio ocupado 1.1T

Sin otro particular, envió un cordial saludo.



Zandra Mendoza
Ejecutivo de Soporte
Janium

Janium S.A.S.

Calle 93 #11A - 28
Oficina 601 Edificio
Capital Park
Bogotá, Colombia

Tel. (571) 344 17 60
www.janium.com

Ciudad de México a 03 de marzo de 2025.

Isabel Cristina Bernal Vinasco
Subdirector de Contenidos y Patrimonio
Biblioteca Pública Piloto
Presente

Por este medio hago llegar las soluciones dadas a los tickets recibidos de Febrero de 2025, en nuestra plataforma de ZohoDesk.

Notas:

Se incluyen todos los tickets generados por las unidades de información existentes en AHM, BPP, BPP ENKI y SBPM.

Para el **Archivo Histórico de Medellín**

ID de Ticket	Asunto	Solución	Estado (Ticket)
72798	AHM - Banner catálogo Archivo Histórico de Medellín	Se hace el cambio de banner.	Cerrado
72821	AHMEDELLIN - REPORTE DE DISPONIBILIDAD JANIUMNET ENERO 2025	Se envía reporte de disponibilidad del servicio JaniumNet.	Cerrado
72825	AHMEDELLIN - REPORTE DE RESPALDOS JANIUMNET ENERO 2025	Se envía reporte mensual de respaldos en el servicio JaniumNet.	Cerrado
73314	AHMEDELLIN - Plantilla publicaciones periódicas	Se activa el formato PUB. PER, con los mismos campos que posee el SBPM y se han agregado las etiquetas requeridas. Se crea la ubicación PUBLICACIONES PERIODICAS. El tipo de material TEXTO y el estado Consulta en Sala; ya existían en el Sistema.	Cerrado
73436	AHMEDELLIN - cambio banner catálogo público	Se hace el cambio de banner.	Cerrado

Para el **Enki Biblioteca Pública Piloto**

ID de Ticket	Asunto	Solución	Estado (Ticket)
72937	BPP ENKI - Generar reporte ARCHIVO SONORO	Se envía archivo con reporte solicitado.	Cerrado
72938	BPP ENKI - REGISTROS QUE NO SE VISUALIZAN	El registro no se visualizaba porque le crearon un ejemplar. Se eliminan los ejemplares y ya se visualizan los tres registros.	Cerrado

Janium S.A.S.

Calle 93 #11A - 28
Oficina 601 Edificio
Capital Park
Bogotá, Colombia

Tel. (571) 344 17 60
www.janium.com

ID de Ticket	Asunto	Solución	Estado (Ticket)
72954	BPP ENKI - Generar reporte GRABACION SONORA	Se envía link para la descarga del listado.	Cerrado
72985	BPP ENKI - Eliminar fichas	Se eliminan los registros con las fichas indicadas.	Cerrado
73096	BPP ENKI - Crear cuenta de catalogación Repositorio digital	Se envían datos de acceso.	Cerrado

Para la **Biblioteca Pública Piloto**

ID de Ticket	Asunto	Solución	Estado (Ticket)
72795	BPP - Solicitud de datos mes de enero Colección Infantil.	Se envían las cifras solicitadas.	Cerrado
72796	BPP RATON - Agregar fechas de cierre bibliotecas Ratón de Biblioteca	Se configuran fechas de cierre.	Cerrado
72822	BPP - REPORTE DE DISPONIBILIDAD JANIUMNET ENERO 2025	Se envía reporte de disponibilidad del servicio JaniumNet.	Cerrado
72827	BPP - REPORTE DE RESPALDOS JANIUMNET ENERO 2025	Se envía reporte mensual de respaldos en el servicio JaniumNet.	Cerrado
72834	BPP - CAMBIO FECHA DE VENCIMIENTO USUARIA 1033184378	Se modifica la fecha de vencimiento por la solicitada.	Cerrado
72972	BPP - PROBLEMA EN EL DESPLIEGUE DEL USUARIO EN EL PRESTAMO	El error es en el domicilio, se corrige debido a una tarea automática.	Cerrado
72982	BPP - Eliminar multa	Se elimina la multa indicada.	Cerrado
73000	BPP - CAMBIO DE BIBLIOTECA OPERADOR CIRCULACION	Se hace el cambio de biblioteca en la cuenta indicada.	Cerrado
73065	BPP - Cambiar de estado y generar listado	Se cambia el estado de los materiales y se envía enlace para la descarga del reporte.	Cerrado
73088	BPP - Cambiar de estado y generar listado TRENES	Se cambia el estado de los materiales y se envía enlace para la descarga del reporte.	Cerrado
73089	BPP - Cambiar de estado y generar listado SAN ANTONIO DE PRADO	Se cambia el estado de los materiales y se envía enlace para la descarga del reporte.	Cerrado

Janium S.A.S.

Calle 93 #11A - 28
Oficina 601 Edificio
Capital Park
Bogotá, Colombia

Tel. (571) 344 17 60
www.janium.com

ID de Ticket	Asunto	Solución	Estado (Ticket)
73090	BPP - Solicitud de información Sala Infantil BPP de los últimos trimestres de 2023 y 2024	Se envían enlaces para la descarga de los reportes.	Cerrado
73147	BPP - Cancelar Apartado	De acuerdo con personal de Circulación y préstamos, se procede a cerrar el presente ticket.	Cerrado
73161	BPP RATON - Eliminación de usuario duplicado.	Se eliminan usuarios duplicados.	Cerrado
73202	BPP - Generar reporte y cambiar de estado JZF	Se cambia el estado de los materiales y se envía enlace para la descarga del reporte.	Cerrado
73218	BPP - Generar reporte y cambiar de estado JZF	Se cambia el estado de los materiales y se envía enlace para la descarga del reporte.	Cerrado
73260	BPP - Ampliar privilegios DUPLICAR y BORRAR registros	Se agregan los privilegios solicitados.	Cerrado
73278	BPP - Ocultar y generar listado TRENES	Se hace el cambio de nivel de acceso y se envía enlace para la descarga del reporte.	Cerrado
73280	BPP - Ocultar y generar listado SEDE CENTRAL	Se hace el cambio de nivel de acceso y se envía enlace para la descarga del reporte.	Cerrado
73330	BPP - Cambio de ficha ejemplar	Se hace el cambio solicitado	Cerrado
73453	BPP - Cambio número de ficha ejemplar	Se cambia de ficha al ejemplar.	Cerrado
73458	BPP - Cambiar de estado y generar listado.	Se hace el cambio de estado y nivel de acceso, además se envía enlace para la descarga del listados.	Cerrado

Para el **Sistema de Bibliotecas Públicas de Medellín**

ID de Ticket	Asunto	Solución	Estado (Ticket)
72795	BPP - Solicitud de datos mes de enero Colección Infantil.	Se envían las cifras solicitadas.	Cerrado
72796	BPP RATON - Agregar fechas de cierre bibliotecas Ratón de Biblioteca	Se configuran fechas de cierre.	Cerrado
72822	BPP - REPORTE DE DISPONIBILIDAD JANIUMNET ENERO 2025	Se envía reporte de disponibilidad del servicio JaniumNet.	Cerrado
72827	BPP - REPORTE DE RESPALDOS JANIUMNET ENERO 2025	Se envía reporte mensual de respaldos en el servicio	Cerrado

Janium S.A.S.

Calle 93 #11A - 28
Oficina 601 Edificio
Capital Park
Bogotá, Colombia

Tel. (571) 344 17 60
www.janium.com

ID de Ticket	Asunto	Solución	Estado (Ticket)
		JaniumNet.	
72834	BPP - CAMBIO FECHA DE VENCIMIENTO USUARIA 1033184378	Se modifica la fecha de vencimiento por la solicitada.	Cerrado
72972	BPP - PROBLEMA EN EL DESPLIEGUE DEL USUARIO EN EL PRESTAMO	El error es en el domicilio, se corrige debido a una tarea automática.	Cerrado
72982	BPP - Eliminar multa	Se elimina la multa indicada.	Cerrado
73000	BPP - CAMBIO DE BIBLIOTECA OPERADOR CIRCULACION	Se hace el cambio de biblioteca en la cuenta indicada.	Cerrado
73065	BPP - Cambiar de estado y generar listado	Se cambia el estado de los materiales y se envía enlace para la descarga del reporte.	Cerrado
73088	BPP - Cambiar de estado y generar listado TRENES	Se cambia el estado de los materiales y se envía enlace para la descarga del reporte.	Cerrado
73089	BPP - Cambiar de estado y generar listado SAN ANTONIO DE PRADO	Se cambia el estado de los materiales y se envía enlace para la descarga del reporte.	Cerrado
73090	BPP - Solicitud de información Sala Infantil BPP de los últimos trimestres de 2023 y 2024	Se envían enlaces para la descarga de los reportes.	Cerrado
73147	BPP - Cancelar Apartado	De acuerdo con personal de Circulación y préstamos, se procede a cerrar el presente ticket.	Cerrado
73161	BPP RATON - Eliminación de usuario duplicado.	Se eliminan usuarios duplicados.	Cerrado
73202	BPP - Generar reporte y cambiar de estado JZF	Se cambia el estado de los materiales y se envía enlace para la descarga del reporte.	Cerrado
73218	BPP - Generar reporte y cambiar de estado JZF	Se cambia el estado de los materiales y se envía enlace para la descarga del reporte.	Cerrado
73260	BPP - Ampliar privilegios DUPLICAR y BORRAR registros	Se agregan los privilegios solicitados.	Cerrado
73278	BPP - Ocultar y generar listado TRENES	Se hace el cambio de nivel de acceso y se envía enlace para la descarga del reporte.	Cerrado

Janium S.A.S.

Calle 93 #11A - 28
Oficina 601 Edificio
Capital Park
Bogotá, Colombia

Tel. (571) 344 17 60
www.janium.com

ID de Ticket	Asunto	Solución	Estado (Ticket)
73280	BPP - Ocultar y generar listado SEDE CENTRAL	Se hace el cambio de nivel de acceso y se envía enlace para la descarga del reporte.	Cerrado
73330	BPP - Cambio de ficha ejemplar	Se hace el cambio solicitado	Cerrado
73453	BPP - Cambio número de ficha ejemplar	Se cambia de ficha al ejemplar.	Cerrado
73458	BPP - Cambiar de estado y generar listado.	Se hace el cambio de estado y nivel de acceso, además se envía enlace para la descarga del listados.	Cerrado

Sin otro particular, quedo a sus órdenes.



Zandra Mendoza
Ejecutivo de Soporte
Janium

Janium S.A.S.

Carrera 7 no. 156 – 68
North Point 3 Oficina
1005 Bogotá, Colombia
Tel. (571) 467 4363
www.janium.com

Bogotá, Colombia a 3 de marzo de 2025

Isabel Cristina Bernal Vinasco
Subdirector de Contenidos y Patrimonio
Biblioteca Pública Piloto
P r e s e n t e

Estimada Dra. Bernal:

Le remito un cordial saludo y le hago entrega de los Reportes de seguridad de Febrero de 2025, sobre los sitios:

https://ahmedellin.janium.net
https://bibliotecapiloto.janium.net
https://rbmam.janium.net

Estos reportes han sido generados con las herramientas Tenable Nessus (https://www.tenable.com/products/nessus) y ZAP (https://www.zaproxy.org/blog/2023-10-12-zap-2-14-0/).

Estado actual: No se detectaron alertas de gravedad alta.

Las alertas que presentan los reportes, en su mayoría, son meramente informativos. El compromiso de Janium es atender trimestralmente las alertas que sean de gravedad baja o media; sólo las alertas de gravedad alta serán atendidas de inmediato.

Con esto damos cumplimiento a lo estipulado en el contrato No. 0240 de 2024, sobre el punto “Informe sobre el estado de la seguridad del sistema de información, así como de la infraestructura asociada”.

Atentamente



José Amador Rodríguez Mejía

Gerente de Soporte Técnico

Janium

Outlook

RE: Consulta sobre mitigación de vulnerabilidades detectada

Desde José Amador Rodríguez <jrodriguez@janium.com>
Fecha Lun 2025-02-17 12:56
Para Gustavo Ospina Ruíz <tecnologia@bibliomed.gov.co>
CC Isabel Bernal <subdir.contenidos@bpp.gov.co>

Buenas tardes Gustavo.

Se ejecutó el análisis de vulnerabilidades el pasado 14 de febrero; acá los informes correspondientes:

https://workdrive.janium.com/external/b584ce8b45db90808e0eba6af65918b677a4d5dbefa7b2bfb92f5b1c81a81d3f

Saludos

José Amador Rodríguez Mejía
Gerente de Soporte técnico
número móvil: +52 55 1953 6967
número Bogotá, Colombia = +5713441760 ext. 109
número Medellín, Colombia = +5742040508 ext. 109
número San José, Costa Rica = +50640001849 ext. 109
número Madrid, España = +34911161538 ext. 109
número Ciudad de México, México = +525541708453 ext. 109
número Lima, Perú = +5116419556 ext. 109
número Estados Unidos, California = 1-650-440-4481 ext. 109
número Santiago, Chile = +56228988240 ext. 109
Janium
==========
web: http://www.janium.com
==========

Los datos personales que se faciliten a este email serán tratados de conformidad con el nuevo Reglamento Europeo (UE) 2016/679 de Protección de Datos. La información relativa a los destinatarios de los datos, la finalidad y las medidas de seguridad, así como cualquier información adicional relativa a la protección de sus datos personales podrá consultarla en el siguiente enlace https://www.janium.com/politicas-de-privacidad Ante el responsable del tratamiento podrá ejercer, entre otros, sus derechos de acceso, rectificación, supresión, oposición y limitación de tratamiento.

---- El jue., 13 feb. 2025 15:25:07 -0600, **Gustavo Ospina Ruíz <tecnologia@bibliomed.gov.co>** escribió ----

Cordial saludo, Sr. José.

Agradecemos su pronta respuesta y la información proporcionada sobre esta actualización.

Quedamos atentos a la liberación del release y a los resultados del análisis de seguridad posterior.

Cordialmente,

Gustavo Adolfo Ospina Ruíz
Contratista – Apoyo administrativo TIC's
Sistema de Bibliotecas Públicas de Medellín
Celular: 304 677 5105

Si usted no es el destinatario de este mensaje, le solicitamos abstenerse de divulgarlo en cualquier forma, informarnos del mismo y eliminarlo en forma inmediata. El correo institucional de la Biblioteca Pública Piloto de Medellín contiene datos de carácter confidencial de propiedad de la Institución, cualquier uso de su contenido, sin la aprobación expresa, constituye una violación de la propiedad Intelectual protegida y sancionada por la ley. Hemos verificado de acuerdo con nuestros sistemas que este mensaje no contenga virus ni otros defectos, pero recomendamos que el destinatario también realice las revisiones de seguridad respectiva.

De: José Amador Rodríguez <jrodriguez@janium.com>
Enviado: jueves, 13 de febrero de 2025 12:36
Para: Gustavo Ospina Ruíz <tecnologia@bibliomed.gov.co>
Cc: Subdirección de Contenidos y Patrimonio <subdir.contenidos@bpp.gov.co>
Asunto: Re: Consulta sobre mitigación de vulnerabilidades detectada

Buenas tardes Gustavo.

Me informa Desarrollo lo siguiente:

1. Hemos actualizado las bibliotecas de Javascript de terceros (jquery-validate y DataTables) que presentaban alertas.
2. Como control interno, se instalador en un ambiente de desarrollo, se ejecutaron los análisis de seguridad y ya no se reportan dichas alertas.
3. La alerta de nivel medio no se atenderá de forma inmediata porque el detalle de la vulnerabilidad hace referencia al componente "Cross-Site Scripting (XSS)" y dicho componente no es usado en el sistema Janium.

El release que contiene esta actualización de las bibliotecas de Javascript de terceros se liberará el día de mañana, viernes 14 de febrero.

El día de mañana, después de la liberación del release, se ejecutarán los análisis de seguridad.

Saludos.

José Amador Rodríguez Mejía
Gerente de Soporte técnico
número móvil: +52 55 1953 6967
número Bogotá, Colombia = +5713441760 ext. 109
número Medellín, Colombia = +5742040508 ext. 109
número San José, Costa Rica = +50640001849 ext. 109
número Madrid, España = +34911161538 ext. 109
número Ciudad de México, México = +525541708453 ext. 109
número Lima, Perú = +5116419556 ext. 109
número Estados Unidos, California = 1-650-440-4481 ext. 109
número Santiago, Chile = +56228988240 ext. 109
Janium
==========
web: http://www.janium.com
==========

Los datos personales que se faciliten a este email serán tratados de conformidad con el nuevo Reglamento Europeo (UE) 2016/679 de Protección de Datos. La información relativa a los destinatarios de los datos, la finalidad y las medidas de seguridad, así como cualquier información adicional relativa a la protección de sus

datos personales podrá consultarla en el siguiente enlace https://www.janium.com/politicas-de-privacidad Ante el responsable del tratamiento podrá ejercer, entre otros, sus derechos de acceso, rectificación, supresión, oposición y limitación de tratamiento.

---- El mié., 12 feb. 2025 08:57:31 -0600, **José Amador Rodríguez <jrodriguez@janium.com>** escribió ----

Buenos días Gustavo.

He compartido su correo con la Gerencia de Desarrollo y con el administrador del servicio en la nube JaniumNet para conocer el estado de estas alertas.

Apenas tenga noticias se las informaré.

Saludos.

José Amador Rodríguez Mejía
Gerente de Soporte técnico
número móvil: +52 55 1953 6967
número Bogotá, Colombia = +5713441760 ext. 109
número Medellín, Colombia = +5742040508 ext. 109
número San José, Costa Rica = +50640001849 ext. 109
número Madrid, España = +34911161538 ext. 109
número Ciudad de México, México = +525541708453 ext. 109
número Lima, Perú = +5116419556 ext. 109
número Estados Unidos, California = 1-650-440-4481 ext. 109
número Santiago, Chile = +56228988240 ext. 109
Janium
==========
web: http://www.janium.com
==========

Los datos personales que se faciliten a este email serán tratados de conformidad con el nuevo Reglamento Europeo (UE) 2016/679 de Protección de Datos. La información relativa a los destinatarios de los datos, la finalidad y las medidas de seguridad, así como cualquier información adicional relativa a la protección de sus datos personales podrá consultarla en el siguiente enlace https://www.janium.com/politicas-de-privacidad Ante el responsable del tratamiento podrá ejercer, entre otros, sus derechos de acceso, rectificación, supresión, oposición y limitación de tratamiento.

---- El mié., 12 feb. 2025 07:56:28 -0600, **Gustavo Ospina Ruíz <tecnologia@bibliomed.gov.co>** escribió ----

Cordial saludo, Sr. José.

Espero que se encuentre muy bien.

Le escribo para consultar sobre las medidas que se han tomado para mitigar las vulnerabilidades detectadas en los sistemas contratados, específicamente en la **librería JavaScript** identificada como vulnerable, utilizada en los portales.

Alertas

Nombre	Nivel de riesgo	Número de Instancias
Librería JS Vulnerable	Alto	2

Según el oficio de seguridad enviado por ustedes, se indica que "*sólo las alertas de gravedad alta serán atendidas de inmediato*". Al revisar los reportes de ZAP, hemos identificado que en cada uno de ellos existen alertas con nivel de riesgo alto. En este sentido, quisiéramos conocer el estado actual del proceso de mitigación de estas vulnerabilidades.

Agradecemos su pronta revisión del tema y quedamos atentos a sus comentarios.

Cordialmente,

Gustavo Adolfo Ospina Ruíz
Contratista – Apoyo administrativo TIC's
Sistema de Bibliotecas Públicas de Medellín
Celular: 304 677 5105

Si usted no es el destinatario de este mensaje, le solicitamos abstenerse de divulgarlo en cualquier forma, informarnos del mismo y eliminarlo en forma inmediata. El correo institucional de la Biblioteca Pública Piloto de Medellín contiene datos de carácter confidencial de propiedad de la Institución, cualquier uso de su contenido, sin la aprobación expresa, constituye una violación de la propiedad Intelectual protegida y sancionada por la ley. Hemos verificado de acuerdo con nuestros sistemas que este mensaje no contenga virus ni otros defectos, pero recomendamos que el destinatario también realice las revisiones de seguridad respectiva.

rbmam.janium.net

Sitios: https://cdn.jsdelivr.net https://rbmam.janium.net http://rbmam.janium.net

Generado a lun, 3 mar 2025 10:59:51

ZAP Versión: 2.16.0

ZAP by Checkmarx

Sumario de Alertas

Nivel de riesgo	Número de Alertas
Alto	0
Medio	4
Bajo	3
Informativo	11

Alertas

Nombre	Nivel de riesgo	Número de Instancias
CSP: script-src unsafe-inline	Medio	8
CSP: style-src unsafe-inline	Medio	8
Cabecera Content Security Policy (CSP) no configurada	Medio	2
Librería JS Vulnerable	Medio	1
Divulgación de Información - Mensajes de Error de Depuración	Bajo	1
Divulgación de Marcas de Tiempo - Unix	Bajo	53
Divulgación de error de aplicación	Bajo	1
Aplicación Web Moderna	Informativo	1
Divulgación de información - Comentarios sospechosos	Informativo	24
Tecnología Detectada - Bootbox.js	Informativo	2
Tecnología Detectada - Bootstrap	Informativo	2
Tecnología Detectada - DataTables	Informativo	2
Tecnología Detectada - Google Font API	Informativo	2
Tecnología Detectada - HSTS	Informativo	2
Tecnología Detectada - Modernizr	Informativo	2
Tecnología Detectada - Moment.js	Informativo	2
Tecnología Detectada - jQuery	Informativo	2
User Agent Fuzzer	Informativo	48

Detalles de la Alerta

Medio	CSP: script-src unsafe-inline
Descripción	Content Security Policy (CSP) es una capa de seguridad añadida que ayuda a detectar y mitigar ciertos tipos de ataques. Incluyendo (pero no limitado a) Cross Site Scripting (XSS), y ataques de inyección de datos. Estos ataques se utilizan, para todo, desde el robo de datos a la desfiguración de sitios o la distribución de malware. CSP proporciona un conjunto de cabeceras HTTP estándar que permiten a los propietarios de sitios web declarar las fuentes de contenido aprobadas que los navegadores deberían poder cargar en esa página. Los tipos cubiertos son JavaScript, CSS, marcos HTML, fuentes, imágenes y objetos incrustables como applets Java, ActiveX y archivos de audio y vídeo.
URL	http://rbmam.janium.net
Método	GET
Ataque	
Evidencia	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net https://fonts.googleapis.com data:; frame-ancestors 'self' https://bibliotecasmedellin.gov.co https://www.bibliotecapiloto.gov.co https://www.medellin.gov.co ; form-action 'self'; frame-src 'self' https://janium.github.io;img-src 'self' https://www.codigos-qr.com blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net; object-src 'self' https://www.youtube.com;
Otra información	script-src incluye unsafe-inline.
URL	https://rbmam.janium.net/
Método	GET
Ataque	
Evidencia	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net https://fonts.googleapis.com data:; frame-ancestors 'self' https://bibliotecasmedellin.gov.co https://www.bibliotecapiloto.gov.co https://www.medellin.gov.co ; form-action 'self'; frame-src 'self' https://janium.github.io;img-src 'self' https://www.codigos-qr.com blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net; object-src 'self' https://www.youtube.com;
Otra información	script-src incluye unsafe-inline.
URL	https://rbmam.janium.net/janium-bin/ayuda.pl?prg=janium_login.pl&ctx=
Método	GET
Ataque	
Evidencia	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net https://fonts.googleapis.com data:; frame-ancestors 'self' https://bibliotecasmedellin.gov.co https://www.bibliotecapiloto.gov.co https://www.medellin.gov.co ; form-action 'self'; frame-src 'self' https://janium.github.io;img-src 'self' https://www.codigos-qr.com blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net; object-src 'self' https://www.youtube.com;
Otra información	script-src incluye unsafe-inline.
URL	https://rbmam.janium.net/janium-bin/busqueda_rapida.pl?Id=20250303102326
Método	GET
Ataque	

Evidencia	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net https://fonts.googleapis.com data:; frame-ancestors 'self' https://bibliotecasmedellin.gov.co https://www.bibliotecapiloto.gov.co https://www.medellin.gov.co ; form-action 'self'; frame-src 'self' https://janium.github.io;img-src 'self' https://www.codigos-qr.com blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net; object-src 'self' https://www.youtube.com;
Otra información	script-src incluye unsafe-inline.
URL	https://rbmam.janium.net/janium-bin/janium_login.pl
Método	GET
Ataque	
Evidencia	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net https://fonts.googleapis.com data:; frame-ancestors 'self' https://bibliotecasmedellin.gov.co https://www.bibliotecapiloto.gov.co https://www.medellin.gov.co ; form-action 'self'; frame-src 'self' https://janium.github.io;img-src 'self' https://www.codigos-qr.com blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net; object-src 'self' https://www.youtube.com;
Otra información	script-src incluye unsafe-inline.
URL	https://rbmam.janium.net/janium-bin/janium_login_error.pl
Método	GET
Ataque	
Evidencia	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net https://fonts.googleapis.com data:; frame-ancestors 'self' https://bibliotecasmedellin.gov.co https://www.bibliotecapiloto.gov.co https://www.medellin.gov.co ; form-action 'self'; frame-src 'self' https://janium.github.io;img-src 'self' https://www.codigos-qr.com blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net; object-src 'self' https://www.youtube.com;
Otra información	script-src incluye unsafe-inline.
URL	https://rbmam.janium.net/janium-bin/password_reset.pl
Método	GET
Ataque	
Evidencia	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net https://fonts.googleapis.com data:; frame-ancestors 'self' https://bibliotecasmedellin.gov.co https://www.bibliotecapiloto.gov.co https://www.medellin.gov.co ; form-action 'self'; frame-src 'self' https://janium.github.io;img-src 'self' https://www.codigos-qr.com blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net; object-src 'self' https://www.youtube.com;
Otra información	script-src incluye unsafe-inline.
URL	https://rbmam.janium.net/janium-bin/password_reset.pl/send
Método	POST
Ataque	
	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net

Evidencia	https://fonts.googleapis.com data:; frame-ancestors 'self' https://bibliotecasmedellin.gov.co https://www.bibliotecapiloto.gov.co https://www.medellin.gov.co ; form-action 'self'; frame-src 'self' https://janium.github.io;img-src 'self' https://www.codigos-qr.com blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net; object-src 'self' https://www.youtube.com;
Otra información	script-src incluye unsafe-inline.
Instancia	8
Solución	Asegúrese de que su servidor web, servidor de aplicación, balanceador de carga, etc. está configurado apropiadamente para establecer la cabecera de Política de Seguridad de Contenido.
Referencia	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693
WASC Id	15
Plugin Id	10055

Medio	**CSP: style-src unsafe-inline**
Descripción	Content Security Policy (CSP) es una capa de seguridad añadida que ayuda a detectar y mitigar ciertos tipos de ataques. Incluyendo (pero no limitado a) Cross Site Scripting (XSS), y ataques de inyección de datos. Estos ataques se utilizan, para todo, desde el robo de datos a la desfiguración de sitios o la distribución de malware. CSP proporciona un conjunto de cabeceras HTTP estándar que permiten a los propietarios de sitios web declarar las fuentes de contenido aprobadas que los navegadores deberían poder cargar en esa página. Los tipos cubiertos son JavaScript, CSS, marcos HTML, fuentes, imágenes y objetos incrustables como applets Java, ActiveX y archivos de audio y vídeo.
URL	http://rbmam.janium.net
Método	GET
Ataque	
Evidencia	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net https://fonts.googleapis.com data:; frame-ancestors 'self' https://bibliotecasmedellin.gov.co https://www.bibliotecapiloto.gov.co https://www.medellin.gov.co ; form-action 'self'; frame-src 'self' https://janium.github.io;img-src 'self' https://www.codigos-qr.com blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net; object-src 'self' https://www.youtube.com;
Otra información	style-src incluye unsafe-inline.
URL	https://rbmam.janium.net/
Método	GET
Ataque	
Evidencia	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net https://fonts.googleapis.com data:; frame-ancestors 'self' https://bibliotecasmedellin.gov.co https://www.bibliotecapiloto.gov.co https://www.medellin.gov.co ; form-action 'self'; frame-src 'self' https://janium.github.io;img-src 'self' https://www.codigos-qr.com blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net; object-src 'self' https://www.youtube.com;
Otra información	style-src incluye unsafe-inline.

URL	https://rbmam.janium.net/janium-bin/ayuda.pl?prg=janium_login.pl&ctx=
Método	GET
Ataque	
Evidencia	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net https://fonts.googleapis.com data:; frame-ancestors 'self' https://bibliotecasmedellin.gov.co https://www.bibliotecapiloto.gov.co https://www.medellin.gov.co ; form-action 'self'; frame-src 'self' https://janium.github.io;img-src 'self' https://www.codigos-qr.com blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net; object-src 'self' https://www.youtube.com;
Otra información	style-src incluye unsafe-inline.
URL	https://rbmam.janium.net/janium-bin/busqueda_rapida.pl?Id=20250303102326
Método	GET
Ataque	
Evidencia	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net https://fonts.googleapis.com data:; frame-ancestors 'self' https://bibliotecasmedellin.gov.co https://www.bibliotecapiloto.gov.co https://www.medellin.gov.co ; form-action 'self'; frame-src 'self' https://janium.github.io;img-src 'self' https://www.codigos-qr.com blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net; object-src 'self' https://www.youtube.com;
Otra información	style-src incluye unsafe-inline.
URL	https://rbmam.janium.net/janium-bin/janium_login.pl
Método	GET
Ataque	
Evidencia	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net https://fonts.googleapis.com data:; frame-ancestors 'self' https://bibliotecasmedellin.gov.co https://www.bibliotecapiloto.gov.co https://www.medellin.gov.co ; form-action 'self'; frame-src 'self' https://janium.github.io;img-src 'self' https://www.codigos-qr.com blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net; object-src 'self' https://www.youtube.com;
Otra información	style-src incluye unsafe-inline.
URL	https://rbmam.janium.net/janium-bin/janium_login_error.pl
Método	GET
Ataque	
Evidencia	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net https://fonts.googleapis.com data:; frame-ancestors 'self' https://bibliotecasmedellin.gov.co https://www.bibliotecapiloto.gov.co https://www.medellin.gov.co ; form-action 'self'; frame-src 'self' https://janium.github.io;img-src 'self' https://www.codigos-qr.com blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net; object-src 'self' https://www.youtube.com;
Otra información	style-src incluye unsafe-inline.
URL	https://rbmam.janium.net/janium-bin/password_reset.pl
Método	GET

Ataque	
Evidencia	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net https://fonts.googleapis.com data:; frame-ancestors 'self' https://bibliotecasmedellin.gov.co https://www.bibliotecapiloto.gov.co https://www.medellin.gov.co ; form-action 'self'; frame-src 'self' https://janium.github.io;img-src 'self' https://www.codigos-qr.com blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net; object-src 'self' https://www.youtube.com;
Otra información	style-src incluye unsafe-inline.
URL	https://rbmam.janium.net/janium-bin/password_reset.pl/send
Método	POST
Ataque	
Evidencia	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net https://fonts.googleapis.com data:; frame-ancestors 'self' https://bibliotecasmedellin.gov.co https://www.bibliotecapiloto.gov.co https://www.medellin.gov.co ; form-action 'self'; frame-src 'self' https://janium.github.io;img-src 'self' https://www.codigos-qr.com blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net; object-src 'self' https://www.youtube.com;
Otra información	style-src incluye unsafe-inline.
Instancia	8
Solución	Asegúrese de que su servidor web, servidor de aplicación, balanceador de carga, etc. está configurado apropiadamente para establecer la cabecera de Política de Seguridad de Contenido.
Referencia	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693
WASC Id	15
Plugin Id	10055

Medio	**Cabecera Content Security Policy (CSP) no configurada**
Descripción	La Política de seguridad de contenido (CSP) es una capa adicional de seguridad que ayuda a detectar y mitigar ciertos tipos de ataques, incluidos Cross Site Scripting (XSS) y ataques de inyección de datos. Estos ataques se utilizan para todo, desde el robo de datos hasta la desfiguración del sitio o la distribución de malware. CSP proporciona un conjunto de encabezados HTTP estándar que permiten a los propietarios de sitios web declarar fuentes de contenido aprobadas que los navegadores deberían poder cargar en esa página; los tipos cubiertos son JavaScript, CSS, marcos HTML, fuentes, imágenes y objetos incrustados como applets de Java, ActiveX, archivos de audio y video.
URL	https://rbmam.janium.net/sitemap.xml
Método	GET
Ataque	
Evidencia	
Otra información	
URL	https://rbmam.janium.net/janium-bin/janium_store.pl?Id=-

Método	POST
Ataque	
Evidencia	
Otra información	
Instancia	2
Solución	Asegúrese de que su servidor web, servidor de aplicaciones, balanceador de carga, etc. esté configurado para establecer la cabecera Content-Security-Policy.
Referencia	https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

Medio	**Librería JS Vulnerable**
Descripción	La librería identificada bootstrap, versión 3.4.1 es vulnerable.
URL	https://rbmam.janium.net/janium/js/bootstrap/bootstrap.min.js
Método	GET
Ataque	
Evidencia	* Bootstrap v3.4.1
Otra información	CVE-2024-6484
Instancia	1
Solución	Actualiza a la última versión de bootstrap.
Referencia	https://nvd.nist.gov/vuln/detail/CVE-2024-6484 https://github.com/rubysec/ruby-advisory-db/blob/master/gems/bootstrap-sass/CVE-2024-6484.yml https://www.herodevs.com/vulnerability-directory/cve-2024-6484 https://github.com/twbs/bootstrap https://github.com/twbs/bootstrap/issues/20631 https://github.com/advisories/GHSA-9mvj-f7w8-pvh2 https://github.com/rubysec/ruby-advisory-db/blob/master/gems/bootstrap/CVE-2024-6484.yml
CWE Id	1395
WASC Id	
Plugin Id	10003

Bajo	**Divulgación de Información - Mensajes de Error de Depuración**
Descripción	La respuesta parecía contener mensajes de error comunes devueltos por plataformas como ASP.NET, y servidores Web como IIS y Apache. Puede configurar la lista de mensajes de depuración comunes.
URL	https://rbmam.janium.net/janium-bin/janium_store.pl?Id=-
Método	POST
Ataque	

Evidencia	Internal Server Error
Otra información	
Instancia	1
Solución	Desactivar los mensajes de depuración antes de pasar a producción.
Referencia	
CWE Id	200
WASC Id	13
Plugin Id	10023

Bajo	**Divulgación de Marcas de Tiempo - Unix**
Descripción	Una marca de tiempo fue revelada por la aplicación/servidor web. - Unix
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1426881987
Otra información	1426881987, que se evalúa como: 2015-03-20 15:06:27.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1431655765
Otra información	1431655765, que se evalúa como: 2015-05-14 21:09:25.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1432725776
Otra información	1432725776, que se evalúa como: 2015-05-27 06:22:56.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1467031594
Otra información	1467031594, que se evalúa como: 2016-06-27 07:46:34.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1476395008
Otra información	1476395008, que se evalúa como: 2016-10-13 16:43:28.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET

Ataque	
Evidencia	1476395009
Otra información	1476395009, que se evalúa como: 2016-10-13 16:43:29.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1495990901
Otra información	1495990901, que se evalúa como: 2017-05-28 12:01:41.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1501505948
Otra información	1501505948, que se evalúa como: 2017-07-31 07:59:08.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1508970993
Otra información	1508970993, que se evalúa como: 2017-10-25 17:36:33.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1518500249
Otra información	1518500249, que se evalúa como: 2018-02-13 00:37:29.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1522805485
Otra información	1522805485, que se evalúa como: 2018-04-03 20:31:25.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1537002063
Otra información	1537002063, que se evalúa como: 2018-09-15 04:01:03.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1541459225

Otra información	1541459225, que se evalúa como: 2018-11-05 18:07:05.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1546045734
Otra información	1546045734, que se evalúa como: 2018-12-28 20:08:54.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1548603684
Otra información	1548603684, que se evalúa como: 2019-01-27 10:41:24.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1549556828
Otra información	1549556828, que se evalúa como: 2019-02-07 11:27:08.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1555081692
Otra información	1555081692, que se evalúa como: 2019-04-12 10:08:12.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1575990012
Otra información	1575990012, que se evalúa como: 2019-12-10 10:00:12.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1595750129
Otra información	1595750129, que se evalúa como: 2020-07-26 02:55:29.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1607167915
Otra información	1607167915, que se evalúa como: 2020-12-05 06:31:55.

URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1610612736
Otra información	1610612736, que se evalúa como: 2021-01-14 03:25:36.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1610612737
Otra información	1610612737, que se evalúa como: 2021-01-14 03:25:37.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1654270250
Otra información	1654270250, que se evalúa como: 2022-06-03 10:30:50.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1694076839
Otra información	1694076839, que se evalúa como: 2023-09-07 03:53:59.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1695183700
Otra información	1695183700, que se evalúa como: 2023-09-19 23:21:40.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1701076831
Otra información	1701076831, que se evalúa como: 2023-11-27 04:20:31.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1731405415
Otra información	1731405415, que se evalúa como: 2024-11-12 04:56:55.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET

Ataque	
Evidencia	1732584193
Otra información	1732584193, que se evalúa como: 2024-11-25 20:23:13.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1744830464
Otra información	1744830464, que se evalúa como: 2025-04-16 14:07:44.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1744830465
Otra información	1744830465, que se evalúa como: 2025-04-16 14:07:45.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1747873779
Otra información	1747873779, que se evalúa como: 2025-05-21 19:29:39.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1750603025
Otra información	1750603025, que se evalúa como: 2025-06-22 09:37:05.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1779033703
Otra información	1779033703, que se evalúa como: 2026-05-17 11:01:43.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1816402316
Otra información	1816402316, que se evalúa como: 2027-07-23 23:11:56.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	

Evidencia	1836072691
Otra información	1836072691, que se evalúa como: 2028-03-07 15:11:31.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1856431235
Otra información	1856431235, que se evalúa como: 2028-10-29 06:20:35.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1859775393
Otra información	1859775393, que se evalúa como: 2028-12-06 23:16:33.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1879048192
Otra información	1879048192, que se evalúa como: 2029-07-18 00:49:52.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1879048193
Otra información	1879048193, que se evalúa como: 2029-07-18 00:49:53.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1894007588
Otra información	1894007588, que se evalúa como: 2030-01-07 04:13:08.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1899447441
Otra información	1899447441, que se evalúa como: 2030-03-11 03:17:21.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1914138554
Otra	

información	1914138554, que se evalúa como: 2030-08-28 04:09:14.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1925078388
Otra información	1925078388, que se evalúa como: 2031-01-01 18:59:48.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1933667412
Otra información	1933667412, que se evalúa como: 2031-04-11 04:50:12.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1955562222
Otra información	1955562222, que se evalúa como: 2031-12-20 14:43:42.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1986661051
Otra información	1986661051, que se evalúa como: 2032-12-14 13:17:31.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1996064986
Otra información	1996064986, que se evalúa como: 2033-04-02 09:29:46.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	2003034995
Otra información	2003034995, que se evalúa como: 2033-06-22 01:36:35.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	2007800933
Otra información	2007800933, que se evalúa como: 2033-08-16 05:28:53.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js

Método	GET
Ataque	
Evidencia	2013265920
Otra información	2013265920, que se evalúa como: 2033-10-18 11:32:00.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	2013265921
Otra información	2013265921, que se evalúa como: 2033-10-18 11:32:01.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	2024104815
Otra información	2024104815, que se evalúa como: 2034-02-20 22:20:15.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	2053994217
Otra información	2053994217, que se evalúa como: 2035-02-01 20:56:57.
Instancia	53
Solución	Confirmar que los datos encontrados de información sobre la marca de tiempo no son sensibles, ni se pueden usar en patrones explotables de divulgación.
Referencia	https://cwe.mitre.org/data/definitions/200.html
CWE Id	200
WASC Id	13
Plugin Id	10096

Bajo	**Divulgación de error de aplicación**
Descripción	Esta página contiene un mensaje de error/advertencia que podría revelar información sensible como la ubicación del archivo que produjo la excepción no controlada. Esta información puede ser usada para lanzas futuros ataques contra la aplicación web. La alerta podría ser una falso positivo si el mensaje de error es encontrado dentro de una página de documentación.
URL	https://rbmam.janium.net/janium-bin/janium_store.pl?Id=-
Método	POST
Ataque	
Evidencia	HTTP/1.1 500 Internal Server Error
Otra información	
Instancia	1

Solución	Revisar el código de fuente de esta página. Implementación de páginas de error personalizadas. Considerar implementar un mecanismos para proveer una única referencia/identificación de error para el cliente (navegador) mientras insertando los detalles en el sitio del navegador y no exponiéndolos al usuario.
Referencia	
CWE Id	200
WASC Id	13
Plugin Id	90022

Informativo	**Aplicación Web Moderna**
Descripción	La aplicación parece ser una aplicación web moderna. Si necesita explorarla automáticamente, el Ajax Spider puede ser más eficaz que el estándar.
URL	https://rbmam.janium.net/janium-bin/busqueda_rapida.pl?Id=20250303102326
Método	GET
Ataque	
Evidencia	 Búsqueda avanzada
Otra información	Se han encontrado enlaces que no tienen atributos href tradicionales, lo que indica que se trata de una aplicación web moderna.
Instancia	1
Solución	Se trata de una alerta informativa, por lo que no es necesario realizar ningún cambio.
Referencia	
CWE Id	
WASC Id	
Plugin Id	10109

Informativo	**Divulgación de información - Comentarios sospechosos**
Descripción	La respuesta parece contener comentarios sospechosos que pueden ayudar a un atacante. N scripts o archivos se refieren a todo el contenido, no solo a los comentarios.
URL	http://rbmam.janium.net
Método	GET
Ataque	
Evidencia	bug
Otra información	Se utilizó el siguiente patrón: \bBUG\b y se detectó en el elemento que comienza por: "<scrip workaround.js"></script>", ver campo de evidencia para el comentario/snippet sospechoso.
URL	https://rbmam.janium.net/janium-bin/ayuda.pl?prg=janium_login.pl&ctx=
Método	GET
Ataque	
Evidencia	bug
Otra información	Se utilizó el siguiente patrón: \bBUG\b y se detectó en el elemento que comienza por: "<scrip workaround.js"></script>", ver campo de evidencia para el comentario/snippet sospechoso.
URL	https://rbmam.janium.net/janium-bin/busqueda_rapida.pl?Id=20250303102326
Método	GET
Ataque	
Evidencia	bug
Otra	Se utilizó el siguiente patrón: \bBUG\b y se detectó en el elemento que comienza por: "<scrip

información	workaround.js"></script>", ver campo de evidencia para el comentario/snippet sospechoso.
URL	https://rbmam.janium.net/janium-bin/janium_login.pl
Método	GET
Ataque	
Evidencia	bug
Otra información	Se utilizó el siguiente patrón: \bBUG\b y se detectó en el elemento que comienza por: "<scrip workaround.js"></script>", ver campo de evidencia para el comentario/snippet sospechoso.
URL	https://rbmam.janium.net/janium-bin/janium_login_error.pl
Método	GET
Ataque	
Evidencia	bug
Otra información	Se utilizó el siguiente patrón: \bBUG\b y se detectó en el elemento que comienza por: "<scrip workaround.js"></script>", ver campo de evidencia para el comentario/snippet sospechoso.
URL	https://rbmam.janium.net/janium/js/adminlte/app.min.js
Método	GET
Ataque	
Evidencia	todo
Otra información	Se utilizó el siguiente patrón: \bTODO\b y se detectó en el elemento que comienza por: "if("u ("AdminLTE requires jQuery");!function(i){"use strict";function s(t,e){if(this.elem", ver campo d
URL	https://rbmam.janium.net/janium/js/bootstrap/ie10-viewport-bug-workaround.js
Método	GET
Ataque	
Evidencia	bug
Otra información	Se utilizó el siguiente patrón: \bBUG\b y se detectó en el elemento que comienza por: " * IE1 bug", ver campo de evidencia para el comentario/snippet sospechoso.
URL	https://rbmam.janium.net/janium/js/janium/janium.js
Método	GET
Ataque	
Evidencia	from
Otra información	Se utilizó el siguiente patrón: \bFROM\b y se detectó en el elemento que comienza por: " pla de evidencia para el comentario/snippet sospechoso.
URL	https://rbmam.janium.net/janium/js/janium/quick_search.js
Método	GET
Ataque	
Evidencia	select
Otra información	Se utilizó el siguiente patrón: \bSELECT\b y se detectó 5 veces, la primera en el elemento qu otro_catalogo_escape"]').val();", véase el campo de pruebas para el comentario/snippet sosp
URL	https://rbmam.janium.net/janium/js/jquery/jquery.min.js
Método	GET
Ataque	
Evidencia	username
Otra información	Se utilizó el siguiente patrón: \bUSERNAME\b y se detectó en el elemento que comienza por module&&"object"==typeof module.exports?module.exports=e.document?t(e,!0):function(", ve sospechoso.

URL	https://rbmam.janium.net/janium/js/jquery/plugin/bootbox.min.js
Método	GET
Ataque	
Evidencia	select
Otra información	Se utilizó el siguiente patrón: \bSELECT\b y se detectó en el elemento que comienza por: "!fu define&&define.amd?define(["jquery"],o):"object"==typeof exports?module.exports=o", ver ca sospechoso.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/bootstrap-notify.min.js
Método	GET
Ataque	
Evidencia	from
Otra información	Se utilizó el siguiente patrón: \bFROM\b y se detectó en el elemento que comienza por: "!fun define(["jquery"],t):t("object"==typeof exports?require("jquery"):jQuery)}(fu", ver campo de evi
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables-natural.js
Método	GET
Ataque	
Evidencia	from
Otra información	Se utilizó el siguiente patrón: \bFROM\b y se detectó 3 veces, la primera en el elemento que by using 'natural-nohtml' such as", véase el campo de pruebas para el comentario/snippet so
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	Bug
Otra información	Se utilizó el siguiente patrón: \bBUG\b y se detectó en el elemento que comienza por: "!functi =typeof module)module.exports=e();else if("function"==typeof define&&defin", ver campo de e
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	bUGS
Otra información	Se utilizó el siguiente patrón: \bBUGS\b y se detectó en el elemento que comienza por: " "Ro "AAEAAAARAQAABAAQR0RFRqWLoiAAAdWAAAACWEdQT1Pk1zcKAAHX2AAAZixHU1V ver campo de evidencia para el comentario/snippet sospechoso.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	Select
Otra información	Se utilizó el siguiente patrón: \bSELECT\b y se detectó 8 veces, la primera en el elemento qu DataTables 2.2.2, AutoFill 2.7.0, Buttons 3.2.2, Column visibility 3.2.2, HTML5 export 3.2.2, " /snippet sospechoso.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	TODO
Otra información	Se utilizó el siguiente patrón: \bTODO\b y se detectó en el elemento que comienza por: "!fun ("object"==typeof exports&&"object"==typeof module)module.exports=i();else if(", ver campo

URL	https://rbmam.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	user
Otra información	Se utilizó el siguiente patrón: \bUSER\b y se detectó en el elemento que comienza por: "!func amd?define(["jquery","datatables.net"],function(e){return s(e,window,docu", ver campo de evi
URL	https://rbmam.janium.net/janium/js/jquery/plugin/jquery.placeholder.min.js
Método	GET
Ataque	
Evidencia	select
Otra información	Se utilizó el siguiente patrón: \bSELECT\b y se detectó en el elemento que comienza por: "!fu define(["jquery"],a):a("object"==typeof module&&module.exports?require("jquer", ver campo d
URL	https://rbmam.janium.net/janium/js/jquery/plugin/jquery.validate.min.js
Método	GET
Ataque	
Evidencia	select
Otra información	Se utilizó el siguiente patrón: \bSELECT\b y se detectó en el elemento que comienza por: "!fu define(["jquery"],a):"object"==typeof module&&module.exports?module.exports=a", ver campo sospechoso.
URL	https://rbmam.janium.net/janium/js/jquery/plugin/select2.full.min.js
Método	GET
Ataque	
Evidencia	query
Otra información	Se utilizó el siguiente patrón: \bQUERY\b y se detectó en el elemento que comienza por: "!fu define(["jquery"],n):"object"==typeof module&&module.exports?module.exports=f", ver campo sospechoso.
URL	https://rbmam.janium.net/janium/js/modernizr/modernizr-respond.min.js
Método	GET
Ataque	
Evidencia	query
Otra información	Se utilizó el siguiente patrón: \bQUERY\b y se detectó en el elemento que comienza por: "/*! polyfill * Copyright 2013 Scott Jehl", ver campo de evidencia para el comentario/snippet sosp
URL	https://rbmam.janium.net/janium/js/modernizr/modernizr-respond.min.js
Método	GET
Ataque	
Evidencia	select
Otra información	Se utilizó el siguiente patrón: \bSELECT\b y se detectó en el elemento que comienza por: ";w cssText=a}function D(a,b){return C(n.join(a+";")+(b||""))}function E(a,b){retu", ver campo de ev
URL	https://rbmam.janium.net/janium/js/moment/moment.min.js
Método	GET
Ataque	
Evidencia	from
Otra información	Se utilizó el siguiente patrón: \bFROM\b y se detectó en el elemento que comienza por: "!func =typeof module?module.exports=t():"function"==typeof define&&define.amd?def", ver campo sospechoso.

Instancia	24
Solución	Eliminar todos los comentarios que muestren información que pueda ayudar a un atacante y
Referencia	
CWE Id	200
WASC Id	13
Plugin Id	10027

Informativo	**Tecnología Detectada - Bootbox.js**
Descripción	Las siguientes "JavaScript libraries" tecnologías han sido identificadas: Bootbox.js. Descrita como: Bootbox.js is a small JavaScript library which allows you to create custom modal dialogs using Bootstrap modals, without having to worry about creating, managing, or removing any of the required DOM elements or JavaScript event handlers.
URL	http://rbmam.janium.net
Método	GET
Ataque	
Evidencia	bootbox.min.js
Otra información	
URL	https://rbmam.janium.net/janium-bin/janium_login.pl
Método	GET
Ataque	
Evidencia	bootbox.min.js
Otra información	
Instancia	2
Solución	
Referencia	https://bootboxjs.com/
CWE Id	
WASC Id	13
Plugin Id	10004

Informativo	**Tecnología Detectada - Bootstrap**
Descripción	Las siguientes "UI frameworks" tecnologías han sido identificadas: Bootstrap. Descrita como: Bootstrap is a free and open-source CSS framework directed at responsive, mobile-first front-end web development. It contains CSS and JavaScript-based design templates for typography, forms, buttons, navigation, and other interface components.
URL	http://rbmam.janium.net
Método	GET
Ataque	
Evidencia	bootstrap-notify.min.js
Otra información	El CPE siguiente está asociado con la tecnología identificada: cpe:2.3:a:getbootstrap:bootstrap:*:*:*:*:*:*:*:* Las siguientes versiones están asociadas con la tecnología: 10
URL	https://rbmam.janium.net/janium-bin/janium_login.pl

Método	GET
Ataque	
Evidencia	bootstrap-notify.min.js
Otra información	El CPE siguiente está asociado con la tecnología identificada: cpe:2.3:a:getbootstrap:bootstrap:*:*:*:*:*:*:*:* Las siguientes versiones están asociadas con la tecnología: 10
Instancia	2
Solución	
Referencia	https://getbootstrap.com
CWE Id	
WASC Id	13
Plugin Id	10004

Informativo	**Tecnología Detectada - DataTables**
Descripción	Las siguientes "JavaScript libraries" tecnologías han sido identificadas: DataTables. Descrita como: DataTables is a plug-in for the jQuery Javascript library adding advanced features like pagination, instant search, themes, and more to any HTML table.
URL	http://rbmam.janium.net
Método	GET
Ataque	
Evidencia	datatables.min.js
Otra información	El CPE siguiente está asociado con la tecnología identificada: cpe:2.3:a:datatables:datatables.net:*:*:*:*:*:*:*:*
URL	https://rbmam.janium.net/janium-bin/janium_login.pl
Método	GET
Ataque	
Evidencia	datatables.min.js
Otra información	El CPE siguiente está asociado con la tecnología identificada: cpe:2.3:a:datatables:datatables.net:*:*:*:*:*:*:*:*
Instancia	2
Solución	
Referencia	https://datatables.net
CWE Id	
WASC Id	13
Plugin Id	10004

Informativo	**Tecnología Detectada - Google Font API**
Descripción	Las siguientes "Font scripts" tecnologías han sido identificadas: Google Font API. Descrita como: Google Font API is a web service that supports open-source font files that can be used on your web designs.
URL	http://rbmam.janium.net
Método	GET
Ataque	

Evidencia	fonts.googleapis.com
Otra información	
URL	https://rbmam.janium.net/janium-bin/janium_login.pl
Método	GET
Ataque	
Evidencia	fonts.googleapis.com
Otra información	
Instancia	2
Solución	
Referencia	https://google.com/fonts
CWE Id	
WASC Id	13
Plugin Id	10004

Informativo	**Tecnología Detectada - HSTS**
Descripción	Las siguientes "Security" tecnologías han sido identificadas: HSTS. Descrita como: HTTP Strict Transport Security (HSTS) informs browsers that the site should only be accessed using HTTPS.
URL	http://rbmam.janium.net
Método	GET
Ataque	
Evidencia	Strict-Transport-Security
Otra información	
URL	https://rbmam.janium.net/sitemap.xml
Método	GET
Ataque	
Evidencia	Strict-Transport-Security
Otra información	
Instancia	2
Solución	
Referencia	https://www.rfc-editor.org/rfc/rfc6797#section-6.1
CWE Id	
WASC Id	13
Plugin Id	10004

Informativo	**Tecnología Detectada - Modernizr**
Descripción	Las siguientes "JavaScript libraries" tecnologías han sido identificadas: Modernizr. Descrita como: Modernizr is a JavaScript library that detects the features available in a user's browser.

URL	http://rbmam.janium.net
Método	GET
Ataque	
Evidencia	modernizr/modernizr-respond.min.js
Otra información	
URL	https://rbmam.janium.net/janium-bin/janium_login.pl
Método	GET
Ataque	
Evidencia	modernizr/modernizr-respond.min.js
Otra información	
Instancia	2
Solución	
Referencia	https://modernizr.com
CWE Id	
WASC Id	13
Plugin Id	10004

Informativo	**Tecnología Detectada - Moment.js**
Descripción	Las siguientes "JavaScript libraries" tecnologías han sido identificadas: Moment.js. Descrita como: Moment.js is a free and open-source JavaScript library that removes the need to use the native JavaScript Date object directly.
URL	http://rbmam.janium.net
Método	GET
Ataque	
Evidencia	moment.min.js
Otra información	El CPE siguiente está asociado con la tecnología identificada: cpe:2.3:a:momentjs:moment:*:*:*:*:*:*:*:*
URL	https://rbmam.janium.net/janium-bin/janium_login.pl
Método	GET
Ataque	
Evidencia	moment.min.js
Otra información	El CPE siguiente está asociado con la tecnología identificada: cpe:2.3:a:momentjs:moment:*:*:*:*:*:*:*:*
Instancia	2
Solución	
Referencia	https://momentjs.com
CWE Id	
WASC Id	13
Plugin Id	10004

Informativo	**Tecnología Detectada - jQuery**
	Las siguientes "JavaScript libraries" tecnologías han sido identificadas: jQuery.

Descripción	Descrita como: jQuery is a JavaScript library which is a free, open-source software designed to simplify HTML DOM tree traversal and manipulation, as well as event handling, CSS animation, and Ajax.
URL	http://rbmam.janium.net
Método	GET
Ataque	
Evidencia	jquery
Otra información	El CPE siguiente está asociado con la tecnología identificada: cpe:2.3:a:jquery:jquery:*:*:*:*:*:*:*:*
URL	https://rbmam.janium.net/janium-bin/janium_login.pl
Método	GET
Ataque	
Evidencia	jquery
Otra información	El CPE siguiente está asociado con la tecnología identificada: cpe:2.3:a:jquery:jquery:*:*:*:*:*:*:*:*
Instancia	2
Solución	
Referencia	https://jquery.com
CWE Id	
WASC Id	13
Plugin Id	10004

Informativo	**User Agent Fuzzer**
Descripción	Compare las diferencias en la respuesta según el fuzzeo de User Agent (por ejemplo, sitios móviles, acceso como un motor de búsqueda). Compara el código de estado de la respuesta y el hash del cuerpo de la respuesta con la respuesta original.
URL	http://rbmam.janium.net
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidencia	
Otra información	
URL	http://rbmam.janium.net
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidencia	
Otra información	
URL	http://rbmam.janium.net
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidencia	
Otra información	

URL	http://rbmam.janium.net
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidencia	
Otra información	
URL	http://rbmam.janium.net
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidencia	
Otra información	
URL	http://rbmam.janium.net
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidencia	
Otra información	
URL	http://rbmam.janium.net
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidencia	
Otra información	
URL	http://rbmam.janium.net
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidencia	
Otra información	
URL	http://rbmam.janium.net
Método	GET
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidencia	
Otra información	
URL	http://rbmam.janium.net
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidencia	
Otra información	

URL	http://rbmam.janium.net
Método	GET
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidencia	
Otra información	
URL	http://rbmam.janium.net
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidencia	
Otra información	
URL	http://rbmam.janium.net/
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidencia	
Otra información	
URL	http://rbmam.janium.net/
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidencia	
Otra información	
URL	http://rbmam.janium.net/
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidencia	
Otra información	
URL	http://rbmam.janium.net/
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidencia	
Otra información	
URL	http://rbmam.janium.net/
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidencia	
Otra información	
URL	http://rbmam.janium.net/

Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidencia	
Otra información	
URL	http://rbmam.janium.net/
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidencia	
Otra información	
URL	http://rbmam.janium.net/
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidencia	
Otra información	
URL	http://rbmam.janium.net/
Método	GET
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidencia	
Otra información	
URL	http://rbmam.janium.net/
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidencia	
Otra información	
URL	http://rbmam.janium.net/
Método	GET
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidencia	
Otra información	
URL	http://rbmam.janium.net/
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidencia	
Otra información	
URL	http://rbmam.janium.net/robots.txt

Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidencia	
Otra información	
URL	http://rbmam.janium.net/robots.txt
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidencia	
Otra información	
URL	http://rbmam.janium.net/robots.txt
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidencia	
Otra información	
URL	http://rbmam.janium.net/robots.txt
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidencia	
Otra información	
URL	http://rbmam.janium.net/robots.txt
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidencia	
Otra información	
URL	http://rbmam.janium.net/robots.txt
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidencia	
Otra información	
URL	http://rbmam.janium.net/robots.txt
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidencia	
Otra información	
URL	http://rbmam.janium.net/robots.txt
Método	GET

Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidencia	
Otra información	
URL	http://rbmam.janium.net/robots.txt
Método	GET
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidencia	
Otra información	
URL	http://rbmam.janium.net/robots.txt
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidencia	
Otra información	
URL	http://rbmam.janium.net/robots.txt
Método	GET
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidencia	
Otra información	
URL	http://rbmam.janium.net/robots.txt
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidencia	
Otra información	
URL	http://rbmam.janium.net/sitemap.xml
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidencia	
Otra información	
URL	http://rbmam.janium.net/sitemap.xml
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidencia	
Otra información	
URL	http://rbmam.janium.net/sitemap.xml
Método	GET

Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidencia	
Otra información	
URL	http://rbmam.janium.net/sitemap.xml
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidencia	
Otra información	
URL	http://rbmam.janium.net/sitemap.xml
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidencia	
Otra información	
URL	http://rbmam.janium.net/sitemap.xml
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidencia	
Otra información	
URL	http://rbmam.janium.net/sitemap.xml
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidencia	
Otra información	
URL	http://rbmam.janium.net/sitemap.xml
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidencia	
Otra información	
URL	http://rbmam.janium.net/sitemap.xml
Método	GET
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidencia	
Otra información	
URL	http://rbmam.janium.net/sitemap.xml
Método	GET
	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4

Ataque	(KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidencia	
Otra información	
URL	http://rbmam.janium.net/sitemap.xml
Método	GET
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidencia	
Otra información	
URL	http://rbmam.janium.net/sitemap.xml
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidencia	
Otra información	
Instancia	48
Solución	
Referencia	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	10104

bibliotecapiloto.janium.net

Sitios: https://bibliotecapiloto.janium.net http://bibliotecapiloto.janium.net

Generado a lun, 3 mar 2025 10:21:24

ZAP Versión: 2.16.0

ZAP by Checkmarx

Sumario de Alertas

Nivel de riesgo	Número de Alertas
Alto	0
Medio	4
Bajo	3
Informativo	10

Alertas

Nombre	Nivel de riesgo	Número de Instancias
CSP: script-src unsafe-inline	Medio	6
CSP: style-src unsafe-inline	Medio	6
Cabecera Content Security Policy (CSP) no configurada	Medio	2
Librería JS Vulnerable	Medio	1
Divulgación de Información - Mensajes de Error de Depuración	Bajo	1
Divulgación de Marcas de Tiempo - Unix	Bajo	53
Divulgación de error de aplicación	Bajo	1
Divulgación de información - Comentarios sospechosos	Informativo	19
Tecnología Detectada - Bootbox.js	Informativo	2
Tecnología Detectada - Bootstrap	Informativo	2
Tecnología Detectada - DataTables	Informativo	2
Tecnología Detectada - Google Font API	Informativo	2
Tecnología Detectada - HSTS	Informativo	2
Tecnología Detectada - Modernizr	Informativo	2
Tecnología Detectada - Moment.js	Informativo	2
Tecnología Detectada - jQuery	Informativo	2
User Agent Fuzzer	Informativo	36

Detalles de la Alerta

Medio	CSP: script-src unsafe-inline
Descripción	Content Security Policy (CSP) es una capa de seguridad añadida que ayuda a detectar y mitigar ciertos tipos de ataques. Incluyendo (pero no limitado a) Cross Site Scripting (XSS), y ataques de inyección de datos. Estos ataques se utilizan, para todo, desde el robo de datos a la desfiguración de sitios o la distribución de malware. CSP proporciona un conjunto de cabeceras HTTP estándar que permiten a los propietarios de sitios web declarar las fuentes de contenido aprobadas que los navegadores deberían poder cargar en esa página. Los tipos cubiertos son JavaScript, CSS, marcos HTML, fuentes, imágenes y objetos incrustables como applets Java, ActiveX y archivos de audio y vídeo.
URL	http://bibliotecapiloto.janium.net
Método	GET
Ataque	
Evidencia	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net https://fonts.googleapis.com data:; frame-ancestors 'self' https://www.bibliotecapiloto.gov.co; form-action 'self'; frame-src 'self' https://janium.github.io;img-src 'self' blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net;
Otra información	script-src incluye unsafe-inline.
URL	https://bibliotecapiloto.janium.net/
Método	GET
Ataque	
Evidencia	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net https://fonts.googleapis.com data:; frame-ancestors 'self' https://www.bibliotecapiloto.gov.co; form-action 'self'; frame-src 'self' https://janium.github.io;img-src 'self' blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net;
Otra información	script-src incluye unsafe-inline.
URL	https://bibliotecapiloto.janium.net/janium-bin/janium_login.pl
Método	GET
Ataque	
Evidencia	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net https://fonts.googleapis.com data:; frame-ancestors 'self' https://www.bibliotecapiloto.gov.co; form-action 'self'; frame-src 'self' https://janium.github.io;img-src 'self' blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net;
Otra información	script-src incluye unsafe-inline.
URL	https://bibliotecapiloto.janium.net/janium-bin/janium_login_error.pl
Método	GET
Ataque	
Evidencia	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net https://fonts.googleapis.com data:; frame-ancestors 'self' https://www.bibliotecapiloto.gov.co; form-action 'self'; frame-src 'self' https://janium.github.io;img-src 'self' blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net;
Otra	

información	script-src incluye unsafe-inline.
URL	https://bibliotecapiloto.janium.net/janium-bin/password_reset.pl
Método	GET
Ataque	
Evidencia	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net https://fonts.googleapis.com data:; frame-ancestors 'self' https://www.bibliotecapiloto.gov.co; form-action 'self'; frame-src 'self' https://janium.github.io;img-src 'self' blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net;
Otra información	script-src incluye unsafe-inline.
URL	https://bibliotecapiloto.janium.net/janium-bin/password_reset.pl/send
Método	POST
Ataque	
Evidencia	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net https://fonts.googleapis.com data:; frame-ancestors 'self' https://www.bibliotecapiloto.gov.co; form-action 'self'; frame-src 'self' https://janium.github.io;img-src 'self' blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net;
Otra información	script-src incluye unsafe-inline.
Instancia	6
Solución	Asegúrese de que su servidor web, servidor de aplicación, balanceador de carga, etc. está configurado apropiadamente para establecer la cabecera de Política de Seguridad de Contenido.
Referencia	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693
WASC Id	15
Plugin Id	10055

Medio	**CSP: style-src unsafe-inline**
Descripción	Content Security Policy (CSP) es una capa de seguridad añadida que ayuda a detectar y mitigar ciertos tipos de ataques. Incluyendo (pero no limitado a) Cross Site Scripting (XSS), y ataques de inyección de datos. Estos ataques se utilizan, para todo, desde el robo de datos a la desfiguración de sitios o la distribución de malware. CSP proporciona un conjunto de cabeceras HTTP estándar que permiten a los propietarios de sitios web declarar las fuentes de contenido aprobadas que los navegadores deberían poder cargar en esa página. Los tipos cubiertos son JavaScript, CSS, marcos HTML, fuentes, imágenes y objetos incrustables como applets Java, ActiveX y archivos de audio y vídeo.
URL	http://bibliotecapiloto.janium.net
Método	GET
Ataque	
Evidencia	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net https://fonts.googleapis.com data:; frame-ancestors 'self' https://www.bibliotecapiloto.gov.co; form-action 'self'; frame-src 'self' https://janium.github.io;img-src 'self' blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net;

Otra información	style-src incluye unsafe-inline.
URL	https://bibliotecapiloto.janium.net/
Método	GET
Ataque	
Evidencia	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net https://fonts.googleapis.com data:; frame-ancestors 'self' https://www.bibliotecapiloto.gov.co; form-action 'self'; frame-src 'self' https://janium.github.io;img-src 'self' blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net;
Otra información	style-src incluye unsafe-inline.
URL	https://bibliotecapiloto.janium.net/janium-bin/janium_login.pl
Método	GET
Ataque	
Evidencia	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net https://fonts.googleapis.com data:; frame-ancestors 'self' https://www.bibliotecapiloto.gov.co; form-action 'self'; frame-src 'self' https://janium.github.io;img-src 'self' blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net;
Otra información	style-src incluye unsafe-inline.
URL	https://bibliotecapiloto.janium.net/janium-bin/janium_login_error.pl
Método	GET
Ataque	
Evidencia	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net https://fonts.googleapis.com data:; frame-ancestors 'self' https://www.bibliotecapiloto.gov.co; form-action 'self'; frame-src 'self' https://janium.github.io;img-src 'self' blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net;
Otra información	style-src incluye unsafe-inline.
URL	https://bibliotecapiloto.janium.net/janium-bin/password_reset.pl
Método	GET
Ataque	
Evidencia	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net https://fonts.googleapis.com data:; frame-ancestors 'self' https://www.bibliotecapiloto.gov.co; form-action 'self'; frame-src 'self' https://janium.github.io;img-src 'self' blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net;
Otra información	style-src incluye unsafe-inline.
URL	https://bibliotecapiloto.janium.net/janium-bin/password_reset.pl/send
Método	POST
Ataque	
	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net

Evidencia	https://fonts.googleapis.com data:; frame-ancestors 'self' https://www.bibliotecapiloto.gov.co; form-action 'self'; frame-src 'self' https://janium.github.io;img-src 'self' blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net;
Otra información	style-src incluye unsafe-inline.
Instancia	6
Solución	Asegúrese de que su servidor web, servidor de aplicación, balanceador de carga, etc. está configurado apropiadamente para establecer la cabecera de Política de Seguridad de Contenido.
Referencia	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693
WASC Id	15
Plugin Id	10055

Medio	**Cabecera Content Security Policy (CSP) no configurada**
Descripción	La Política de seguridad de contenido (CSP) es una capa adicional de seguridad que ayuda a detectar y mitigar ciertos tipos de ataques, incluidos Cross Site Scripting (XSS) y ataques de inyección de datos. Estos ataques se utilizan para todo, desde el robo de datos hasta la desfiguración del sitio o la distribución de malware. CSP proporciona un conjunto de encabezados HTTP estándar que permiten a los propietarios de sitios web declarar fuentes de contenido aprobadas que los navegadores deberían poder cargar en esa página; los tipos cubiertos son JavaScript, CSS, marcos HTML, fuentes, imágenes y objetos incrustados como applets de Java, ActiveX, archivos de audio y video.
URL	https://bibliotecapiloto.janium.net/sitemap.xml
Método	GET
Ataque	
Evidencia	
Otra información	
URL	https://bibliotecapiloto.janium.net/janium-bin/janium_store.pl?Id=-
Método	POST
Ataque	
Evidencia	
Otra información	
Instancia	2
Solución	Asegúrese de que su servidor web, servidor de aplicaciones, balanceador de carga, etc. esté configurado para establecer la cabecera Content-Security-Policy.
Referencia	https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
CWE Id	693
WASC Id	15

Plugin Id	10038

Medio	Librería JS Vulnerable
Descripción	La librería identificada bootstrap, versión 3.4.1 es vulnerable.
URL	https://bibliotecapiloto.janium.net/janium/js/bootstrap/bootstrap.min.js
Método	GET
Ataque	
Evidencia	* Bootstrap v3.4.1
Otra información	CVE-2024-6484
Instancia	1
Solución	Actualiza a la última versión de bootstrap.
Referencia	https://nvd.nist.gov/vuln/detail/CVE-2024-6484 https://github.com/rubysec/ruby-advisory-db/blob/master/gems/bootstrap-sass/CVE-2024-6484.yml https://www.herodevs.com/vulnerability-directory/cve-2024-6484 https://github.com/twbs/bootstrap https://github.com/twbs/bootstrap/issues/20631 https://github.com/advisories/GHSA-9mvj-f7w8-pvh2 https://github.com/rubysec/ruby-advisory-db/blob/master/gems/bootstrap/CVE-2024-6484.yml
CWE Id	1395
WASC Id	
Plugin Id	10003

Bajo	Divulgación de Información - Mensajes de Error de Depuración
Descripción	La respuesta parecía contener mensajes de error comunes devueltos por plataformas como ASP.NET, y servidores Web como IIS y Apache. Puede configurar la lista de mensajes de depuración comunes.
URL	https://bibliotecapiloto.janium.net/janium-bin/janium_store.pl?Id=-
Método	POST
Ataque	
Evidencia	Internal Server Error
Otra información	
Instancia	1
Solución	Desactivar los mensajes de depuración antes de pasar a producción.
Referencia	
CWE Id	200
WASC Id	13
Plugin Id	10023

Bajo	Divulgación de Marcas de Tiempo - Unix
Descripción	Una marca de tiempo fue revelada por la aplicación/servidor web. - Unix
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1426881987

Otra información	1426881987, que se evalúa como: 2015-03-20 15:06:27.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1431655765
Otra información	1431655765, que se evalúa como: 2015-05-14 21:09:25.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1432725776
Otra información	1432725776, que se evalúa como: 2015-05-27 06:22:56.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1467031594
Otra información	1467031594, que se evalúa como: 2016-06-27 07:46:34.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1476395008
Otra información	1476395008, que se evalúa como: 2016-10-13 16:43:28.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1476395009
Otra información	1476395009, que se evalúa como: 2016-10-13 16:43:29.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1495990901
Otra información	1495990901, que se evalúa como: 2017-05-28 12:01:41.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1501505948
Otra información	1501505948, que se evalúa como: 2017-07-31 07:59:08.

URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1508970993
Otra información	1508970993, que se evalúa como: 2017-10-25 17:36:33.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1518500249
Otra información	1518500249, que se evalúa como: 2018-02-13 00:37:29.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1522805485
Otra información	1522805485, que se evalúa como: 2018-04-03 20:31:25.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1537002063
Otra información	1537002063, que se evalúa como: 2018-09-15 04:01:03.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1541459225
Otra información	1541459225, que se evalúa como: 2018-11-05 18:07:05.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1546045734
Otra información	1546045734, que se evalúa como: 2018-12-28 20:08:54.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1548603684
Otra información	1548603684, que se evalúa como: 2019-01-27 10:41:24.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET

Ataque	
Evidencia	1549556828
Otra información	1549556828, que se evalúa como: 2019-02-07 11:27:08.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1555081692
Otra información	1555081692, que se evalúa como: 2019-04-12 10:08:12.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1575990012
Otra información	1575990012, que se evalúa como: 2019-12-10 10:00:12.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1595750129
Otra información	1595750129, que se evalúa como: 2020-07-26 02:55:29.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1607167915
Otra información	1607167915, que se evalúa como: 2020-12-05 06:31:55.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1610612736
Otra información	1610612736, que se evalúa como: 2021-01-14 03:25:36.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1610612737
Otra información	1610612737, que se evalúa como: 2021-01-14 03:25:37.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	

Evidencia	1654270250
Otra información	1654270250, que se evalúa como: 2022-06-03 10:30:50.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1694076839
Otra información	1694076839, que se evalúa como: 2023-09-07 03:53:59.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1695183700
Otra información	1695183700, que se evalúa como: 2023-09-19 23:21:40.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1701076831
Otra información	1701076831, que se evalúa como: 2023-11-27 04:20:31.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1731405415
Otra información	1731405415, que se evalúa como: 2024-11-12 04:56:55.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1732584193
Otra información	1732584193, que se evalúa como: 2024-11-25 20:23:13.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1744830464
Otra información	1744830464, que se evalúa como: 2025-04-16 14:07:44.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1744830465
Otra	

información	1744830465, que se evalúa como: 2025-04-16 14:07:45.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1747873779
Otra información	1747873779, que se evalúa como: 2025-05-21 19:29:39.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1750603025
Otra información	1750603025, que se evalúa como: 2025-06-22 09:37:05.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1779033703
Otra información	1779033703, que se evalúa como: 2026-05-17 11:01:43.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1816402316
Otra información	1816402316, que se evalúa como: 2027-07-23 23:11:56.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1836072691
Otra información	1836072691, que se evalúa como: 2028-03-07 15:11:31.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1856431235
Otra información	1856431235, que se evalúa como: 2028-10-29 06:20:35.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1859775393
Otra información	1859775393, que se evalúa como: 2028-12-06 23:16:33.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js

Método	GET
Ataque	
Evidencia	1879048192
Otra información	1879048192, que se evalúa como: 2029-07-18 00:49:52.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1879048193
Otra información	1879048193, que se evalúa como: 2029-07-18 00:49:53.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1894007588
Otra información	1894007588, que se evalúa como: 2030-01-07 04:13:08.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1899447441
Otra información	1899447441, que se evalúa como: 2030-03-11 03:17:21.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1914138554
Otra información	1914138554, que se evalúa como: 2030-08-28 04:09:14.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1925078388
Otra información	1925078388, que se evalúa como: 2031-01-01 18:59:48.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1933667412
Otra información	1933667412, que se evalúa como: 2031-04-11 04:50:12.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET

Ataque	
Evidencia	1955562222
Otra información	1955562222, que se evalúa como: 2031-12-20 14:43:42.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1986661051
Otra información	1986661051, que se evalúa como: 2032-12-14 13:17:31.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1996064986
Otra información	1996064986, que se evalúa como: 2033-04-02 09:29:46.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	2003034995
Otra información	2003034995, que se evalúa como: 2033-06-22 01:36:35.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	2007800933
Otra información	2007800933, que se evalúa como: 2033-08-16 05:28:53.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	2013265920
Otra información	2013265920, que se evalúa como: 2033-10-18 11:32:00.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	2013265921
Otra información	2013265921, que se evalúa como: 2033-10-18 11:32:01.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	2024104815

Otra información	2024104815, que se evalúa como: 2034-02-20 22:20:15.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	2053994217
Otra información	2053994217, que se evalúa como: 2035-02-01 20:56:57.
Instancia	53
Solución	Confirmar que los datos encontrados de información sobre la marca de tiempo no son sensibles, ni se pueden usar en patrones explotables de divulgación.
Referencia	https://cwe.mitre.org/data/definitions/200.html
CWE Id	200
WASC Id	13
Plugin Id	10096

Bajo	**Divulgación de error de aplicación**
Descripción	Esta página contiene un mensaje de error/advertencia que podría revelar información sensible como la ubicación del archivo que produjo la excepción no controlada. Esta información puede ser usada para lanzas futuros ataques contra la aplicación web. La alerta podría ser una falso positivo si el mensaje de error es encontrado dentro de una página de documentación.
URL	https://bibliotecapiloto.janium.net/janium-bin/janium_store.pl?Id=-
Método	POST
Ataque	
Evidencia	HTTP/1.1 500 Internal Server Error
Otra información	
Instancia	1
Solución	Revisar el código de fuente de esta página. Implementación de páginas de error personalizadas. Considerar implementar un mecanismos para proveer una única referencia/identificación de error para el cliente (navegador) mientras insertando los detalles en el sitio del navegador y no exponiéndolos al usuario.
Referencia	
CWE Id	200
WASC Id	13
Plugin Id	90022

Informativo	**Divulgación de información - Comentarios sospechosos**
Descripción	La respuesta parece contener comentarios sospechosos que pueden ayudar a un atacante. M scripts o archivos se refieren a todo el contenido, no solo a los comentarios.
URL	http://bibliotecapiloto.janium.net
Método	GET
Ataque	
Evidencia	bug
Otra información	Se utilizó el siguiente patrón: \bBUG\b y se detectó en el elemento que comienza por: "<scrip workaround.js"></script>", ver campo de evidencia para el comentario/snippet sospechoso.
URL	https://bibliotecapiloto.janium.net/janium-bin/janium_login.pl

Método	GET
Ataque	
Evidencia	bug
Otra información	Se utilizó el siguiente patrón: \bBUG\b y se detectó en el elemento que comienza por: "<scrip workaround.js"></script>", ver campo de evidencia para el comentario/snippet sospechoso.
URL	https://bibliotecapiloto.janium.net/janium-bin/janium_login_error.pl
Método	GET
Ataque	
Evidencia	bug
Otra información	Se utilizó el siguiente patrón: \bBUG\b y se detectó en el elemento que comienza por: "<scrip workaround.js"></script>", ver campo de evidencia para el comentario/snippet sospechoso.
URL	https://bibliotecapiloto.janium.net/janium/js/adminlte/app.min.js
Método	GET
Ataque	
Evidencia	todo
Otra información	Se utilizó el siguiente patrón: \bTODO\b y se detectó en el elemento que comienza por: "if("u ("AdminLTE requires jQuery");!function(i){"use strict";function s(t,e){if(this.elem", ver campo d
URL	https://bibliotecapiloto.janium.net/janium/js/bootstrap/ie10-viewport-bug-workaround.js
Método	GET
Ataque	
Evidencia	bug
Otra información	Se utilizó el siguiente patrón: \bBUG\b y se detectó en el elemento que comienza por: " * IE1 bug", ver campo de evidencia para el comentario/snippet sospechoso.
URL	https://bibliotecapiloto.janium.net/janium/js/janium/janium.js
Método	GET
Ataque	
Evidencia	from
Otra información	Se utilizó el siguiente patrón: \bFROM\b y se detectó en el elemento que comienza por: " pla de evidencia para el comentario/snippet sospechoso.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/jquery.min.js
Método	GET
Ataque	
Evidencia	username
Otra información	Se utilizó el siguiente patrón: \bUSERNAME\b y se detectó en el elemento que comienza por module&&"object"==typeof module.exports?module.exports=e.document?t(e,!0):function(", ve sospechoso.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/bootbox.min.js
Método	GET
Ataque	
Evidencia	select
Otra información	Se utilizó el siguiente patrón: \bSELECT\b y se detectó en el elemento que comienza por: "!fu define&&define.amd?define(["jquery"],o):"object"==typeof exports?module.exports=o", ver ca sospechoso.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/bootstrap-notify.min.js
Método	GET

Ataque	
Evidencia	from
Otra información	Se utilizó el siguiente patrón: \bFROM\b y se detectó en el elemento que comienza por: "!fun define(["jquery"],t):t("object"==typeof exports?require("jquery"):jQuery)}(fu", ver campo de evi
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	Bug
Otra información	Se utilizó el siguiente patrón: \bBUG\b y se detectó en el elemento que comienza por: "!functi =typeof module)module.exports=e();else if("function"==typeof define&&defin", ver campo de e
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	bUGS
Otra información	Se utilizó el siguiente patrón: \bBUGS\b y se detectó en el elemento que comienza por: " "Ro "AAEAAAARAQAABAAQR0RFRqWLoiAAAdWAAAACWEdQT1Pk1zcKAAHX2AAAZixHU1V ver campo de evidencia para el comentario/snippet sospechoso.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	Select
Otra información	Se utilizó el siguiente patrón: \bSELECT\b y se detectó 8 veces, la primera en el elemento qu DataTables 2.2.2, AutoFill 2.7.0, Buttons 3.2.2, Column visibility 3.2.2, HTML5 export 3.2.2, ", /snippet sospechoso.
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	TODO
Otra información	Se utilizó el siguiente patrón: \bTODO\b y se detectó en el elemento que comienza por: "!func ("object"==typeof exports&&"object"==typeof module)module.exports=i();else if(", ver campo
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	user
Otra información	Se utilizó el siguiente patrón: \bUSER\b y se detectó en el elemento que comienza por: "!func amd?define(["jquery","datatables.net"],function(e){return s(e,window,docu", ver campo de evi
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/jquery.placeholder.min.js
Método	GET
Ataque	
Evidencia	select
Otra información	Se utilizó el siguiente patrón: \bSELECT\b y se detectó en el elemento que comienza por: "!fu define(["jquery"],a):a("object"==typeof module&&module.exports?require("jquer", ver campo
URL	https://bibliotecapiloto.janium.net/janium/js/jquery/plugin/jquery.validate.min.js
Método	GET

Ataque	
Evidencia	select
Otra información	Se utilizó el siguiente patrón: \bSELECT\b y se detectó en el elemento que comienza por: "!fu define(["jquery"],a):"object"==typeof module&&module.exports?module.exports=a", ver campo sospechoso.
URL	https://bibliotecapiloto.janium.net/janium/js/modernizr/modernizr-respond.min.js
Método	GET
Ataque	
Evidencia	query
Otra información	Se utilizó el siguiente patrón: \bQUERY\b y se detectó en el elemento que comienza por: "/*! polyfill * Copyright 2013 Scott Jehl", ver campo de evidencia para el comentario/snippet sosp
URL	https://bibliotecapiloto.janium.net/janium/js/modernizr/modernizr-respond.min.js
Método	GET
Ataque	
Evidencia	select
Otra información	Se utilizó el siguiente patrón: \bSELECT\b y se detectó en el elemento que comienza por: ";w cssText=a}function D(a,b){return C(n.join(a+";")+(b||""))}function E(a,b){retu", ver campo de ev
URL	https://bibliotecapiloto.janium.net/janium/js/moment/moment.min.js
Método	GET
Ataque	
Evidencia	from
Otra información	Se utilizó el siguiente patrón: \bFROM\b y se detectó en el elemento que comienza por: "!func =typeof module?module.exports=t():"function"==typeof define&&define.amd?def", ver campo sospechoso.
Instancia	19
Solución	Eliminar todos los comentarios que muestren información que pueda ayudar a un atacante y
Referencia	
CWE Id	200
WASC Id	13
Plugin Id	10027

Informativo	**Tecnología Detectada - Bootbox.js**
Descripción	Las siguientes "JavaScript libraries" tecnologías han sido identificadas: Bootbox.js. Descrita como: Bootbox.js is a small JavaScript library which allows you to create custom modal dialogs using Bootstrap modals, without having to worry about creating, managing, or removing any of the required DOM elements or JavaScript event handlers.
URL	http://bibliotecapiloto.janium.net
Método	GET
Ataque	
Evidencia	bootbox.min.js
Otra información	
URL	https://bibliotecapiloto.janium.net/janium-bin/janium_login.pl
Método	GET

Ataque	
Evidencia	bootbox.min.js
Otra información	
Instancia	2
Solución	
Referencia	https://bootboxjs.com/
CWE Id	
WASC Id	13
Plugin Id	10004

Informativo	**Tecnología Detectada - Bootstrap**
Descripción	Las siguientes "UI frameworks" tecnologías han sido identificadas: Bootstrap. Descrita como: Bootstrap is a free and open-source CSS framework directed at responsive, mobile-first front-end web development. It contains CSS and JavaScript-based design templates for typography, forms, buttons, navigation, and other interface components.
URL	http://bibliotecapiloto.janium.net
Método	GET
Ataque	
Evidencia	bootstrap-notify.min.js
Otra información	El CPE siguiente está asociado con la tecnología identificada: cpe:2.3:a:getbootstrap:bootstrap:*:*:*:*:*:*:*:* Las siguientes versiones están asociadas con la tecnología: 10
URL	https://bibliotecapiloto.janium.net/janium-bin/janium_login.pl
Método	GET
Ataque	
Evidencia	bootstrap-notify.min.js
Otra información	El CPE siguiente está asociado con la tecnología identificada: cpe:2.3:a:getbootstrap:bootstrap:*:*:*:*:*:*:*:* Las siguientes versiones están asociadas con la tecnología: 10
Instancia	2
Solución	
Referencia	https://getbootstrap.com
CWE Id	
WASC Id	13
Plugin Id	10004

Informativo	**Tecnología Detectada - DataTables**
Descripción	Las siguientes "JavaScript libraries" tecnologías han sido identificadas: DataTables. Descrita como: DataTables is a plug-in for the jQuery Javascript library adding advanced features like pagination, instant search, themes, and more to any HTML table.
URL	http://bibliotecapiloto.janium.net
Método	GET
Ataque	
Evidencia	datatables.min.js

Otra información	El CPE siguiente está asociado con la tecnología identificada: cpe:2.3:a:datatables: datatables.net:*:*:*:*:*:*:*:*
URL	https://bibliotecapiloto.janium.net/janium-bin/janium_login.pl
Método	GET
Ataque	
Evidencia	datatables.min.js
Otra información	El CPE siguiente está asociado con la tecnología identificada: cpe:2.3:a:datatables: datatables.net:*:*:*:*:*:*:*:*
Instancia	2
Solución	
Referencia	https://datatables.net
CWE Id	
WASC Id	13
Plugin Id	10004

Informativo	**Tecnología Detectada - Google Font API**
Descripción	Las siguientes "Font scripts" tecnologías han sido identificadas: Google Font API. Descrita como: Google Font API is a web service that supports open-source font files that can be used on your web designs.
URL	http://bibliotecapiloto.janium.net
Método	GET
Ataque	
Evidencia	fonts.googleapis.com
Otra información	
URL	https://bibliotecapiloto.janium.net/janium-bin/janium_login.pl
Método	GET
Ataque	
Evidencia	fonts.googleapis.com
Otra información	
Instancia	2
Solución	
Referencia	https://google.com/fonts
CWE Id	
WASC Id	13
Plugin Id	10004

Informativo	**Tecnología Detectada - HSTS**
Descripción	Las siguientes "Security" tecnologías han sido identificadas: HSTS. Descrita como: HTTP Strict Transport Security (HSTS) informs browsers that the site should only be accessed using HTTPS.

URL	http://bibliotecapiloto.janium.net
Método	GET
Ataque	
Evidencia	Strict-Transport-Security
Otra información	
URL	https://bibliotecapiloto.janium.net/
Método	GET
Ataque	
Evidencia	Strict-Transport-Security
Otra información	
Instancia	2
Solución	
Referencia	https://www.rfc-editor.org/rfc/rfc6797#section-6.1
CWE Id	
WASC Id	13
Plugin Id	10004

Informativo	**Tecnología Detectada - Modernizr**
Descripción	Las siguientes "JavaScript libraries" tecnologías han sido identificadas: Modernizr. Descrita como: Modernizr is a JavaScript library that detects the features available in a user's browser.
URL	http://bibliotecapiloto.janium.net
Método	GET
Ataque	
Evidencia	modernizr/modernizr-respond.min.js
Otra información	
URL	https://bibliotecapiloto.janium.net/janium-bin/janium_login.pl
Método	GET
Ataque	
Evidencia	modernizr/modernizr-respond.min.js
Otra información	
Instancia	2
Solución	
Referencia	https://modernizr.com
CWE Id	
WASC Id	13
Plugin Id	10004

Informativo	**Tecnología Detectada - Moment.js**
	Las siguientes "JavaScript libraries" tecnologías han sido identificadas: Moment.js.

Descripción	Descrita como: Moment.js is a free and open-source JavaScript library that removes the need to use the native JavaScript Date object directly.
URL	http://bibliotecapiloto.janium.net
Método	GET
Ataque	
Evidencia	moment.min.js
Otra información	El CPE siguiente está asociado con la tecnología identificada: cpe:2.3:a:momentjs:moment:*:*:*:*:*:*:*:*
URL	https://bibliotecapiloto.janium.net/janium-bin/janium_login.pl
Método	GET
Ataque	
Evidencia	moment.min.js
Otra información	El CPE siguiente está asociado con la tecnología identificada: cpe:2.3:a:momentjs:moment:*:*:*:*:*:*:*:*
Instancia	2
Solución	
Referencia	https://momentjs.com
CWE Id	
WASC Id	13
Plugin Id	10004

Informativo	**Tecnología Detectada - jQuery**
Descripción	Las siguientes "JavaScript libraries" tecnologías han sido identificadas: jQuery. Descrita como: jQuery is a JavaScript library which is a free, open-source software designed to simplify HTML DOM tree traversal and manipulation, as well as event handling, CSS animation, and Ajax.
URL	http://bibliotecapiloto.janium.net
Método	GET
Ataque	
Evidencia	jquery
Otra información	El CPE siguiente está asociado con la tecnología identificada: cpe:2.3:a:jquery:jquery:*:*:*:*:*:*:*:*
URL	https://bibliotecapiloto.janium.net/janium-bin/janium_login.pl
Método	GET
Ataque	
Evidencia	jquery
Otra información	El CPE siguiente está asociado con la tecnología identificada: cpe:2.3:a:jquery:jquery:*:*:*:*:*:*:*:*
Instancia	2
Solución	
Referencia	https://jquery.com
CWE Id	

WASC Id	13
Plugin Id	10004

Informativo	User Agent Fuzzer
Descripción	Compare las diferencias en la respuesta según el fuzzeo de User Agent (por ejemplo, sitios móviles, acceso como un motor de búsqueda). Compara el código de estado de la respuesta y el hash del cuerpo de la respuesta con la respuesta original.
URL	http://bibliotecapiloto.janium.net
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidencia	
Otra información	
URL	http://bibliotecapiloto.janium.net
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidencia	
Otra información	
URL	http://bibliotecapiloto.janium.net
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidencia	
Otra información	
URL	http://bibliotecapiloto.janium.net
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidencia	
Otra información	
URL	http://bibliotecapiloto.janium.net
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidencia	
Otra información	
URL	http://bibliotecapiloto.janium.net
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidencia	
Otra información	
URL	http://bibliotecapiloto.janium.net

Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidencia	
Otra información	
URL	http://bibliotecapiloto.janium.net
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidencia	
Otra información	
URL	http://bibliotecapiloto.janium.net
Método	GET
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidencia	
Otra información	
URL	http://bibliotecapiloto.janium.net
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidencia	
Otra información	
URL	http://bibliotecapiloto.janium.net
Método	GET
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidencia	
Otra información	
URL	http://bibliotecapiloto.janium.net
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidencia	
Otra información	
URL	http://bibliotecapiloto.janium.net/robots.txt
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidencia	
Otra información	
URL	http://bibliotecapiloto.janium.net/robots.txt

Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidencia	
Otra información	
URL	http://bibliotecapiloto.janium.net/robots.txt
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidencia	
Otra información	
URL	http://bibliotecapiloto.janium.net/robots.txt
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidencia	
Otra información	
URL	http://bibliotecapiloto.janium.net/robots.txt
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidencia	
Otra información	
URL	http://bibliotecapiloto.janium.net/robots.txt
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidencia	
Otra información	
URL	http://bibliotecapiloto.janium.net/robots.txt
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidencia	
Otra información	
URL	http://bibliotecapiloto.janium.net/robots.txt
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidencia	
Otra información	
URL	http://bibliotecapiloto.janium.net/robots.txt
Método	GET

Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidencia	
Otra información	
URL	http://bibliotecapiloto.janium.net/robots.txt
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidencia	
Otra información	
URL	http://bibliotecapiloto.janium.net/robots.txt
Método	GET
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidencia	
Otra información	
URL	http://bibliotecapiloto.janium.net/robots.txt
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidencia	
Otra información	
URL	http://bibliotecapiloto.janium.net/sitemap.xml
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidencia	
Otra información	
URL	http://bibliotecapiloto.janium.net/sitemap.xml
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidencia	
Otra información	
URL	http://bibliotecapiloto.janium.net/sitemap.xml
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidencia	
Otra información	
URL	http://bibliotecapiloto.janium.net/sitemap.xml
Método	GET

Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidencia	
Otra información	
URL	http://bibliotecapiloto.janium.net/sitemap.xml
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidencia	
Otra información	
URL	http://bibliotecapiloto.janium.net/sitemap.xml
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidencia	
Otra información	
URL	http://bibliotecapiloto.janium.net/sitemap.xml
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidencia	
Otra información	
URL	http://bibliotecapiloto.janium.net/sitemap.xml
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidencia	
Otra información	
URL	http://bibliotecapiloto.janium.net/sitemap.xml
Método	GET
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidencia	
Otra información	
URL	http://bibliotecapiloto.janium.net/sitemap.xml
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidencia	
Otra información	
URL	http://bibliotecapiloto.janium.net/sitemap.xml
Método	GET

Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidencia	
Otra información	
URL	http://bibliotecapiloto.janium.net/sitemap.xml
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidencia	
Otra información	
Instancia	36
Solución	
Referencia	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	10104

ahmedellin.janium.net

Sitios: https://ahmedellin.janium.net http://ahmedellin.janium.net

Generado a lun, 3 mar 2025 10:04:12

ZAP Versión: 2.16.0

ZAP by Checkmarx

Sumario de Alertas

Nivel de riesgo	Número de Alertas
Alto	0
Medio	4
Bajo	3
Informativo	10

Alertas

Nombre	Nivel de riesgo	Número de Instancias
CSP: script-src unsafe-inline	Medio	6
CSP: style-src unsafe-inline	Medio	6
Cabecera Content Security Policy (CSP) no configurada	Medio	2
Librería JS Vulnerable	Medio	1
Divulgación de Información - Mensajes de Error de Depuración	Bajo	1
Divulgación de Marcas de Tiempo - Unix	Bajo	53
Divulgación de error de aplicación	Bajo	1
Divulgación de información - Comentarios sospechosos	Informativo	19
Tecnología Detectada - Bootbox.js	Informativo	2
Tecnología Detectada - Bootstrap	Informativo	2
Tecnología Detectada - DataTables	Informativo	2
Tecnología Detectada - Google Font API	Informativo	2
Tecnología Detectada - HSTS	Informativo	2
Tecnología Detectada - Modernizr	Informativo	2
Tecnología Detectada - Moment.js	Informativo	2
Tecnología Detectada - jQuery	Informativo	2
User Agent Fuzzer	Informativo	36

Detalles de la Alerta

Medio	CSP: script-src unsafe-inline
Descripción	Content Security Policy (CSP) es una capa de seguridad añadida que ayuda a detectar y mitigar ciertos tipos de ataques. Incluyendo (pero no limitado a) Cross Site Scripting (XSS), y ataques de inyección de datos. Estos ataques se utilizan, para todo, desde el robo de datos a la desfiguración de sitios o la distribución de malware. CSP proporciona un conjunto de cabeceras HTTP estándar que permiten a los propietarios de sitios web declarar las fuentes de contenido aprobadas que los navegadores deberían poder cargar en esa página. Los tipos cubiertos son JavaScript, CSS, marcos HTML, fuentes, imágenes y objetos incrustables como applets Java, ActiveX y archivos de audio y vídeo.
URL	http://ahmedellin.janium.net
Método	GET
Ataque	
Evidencia	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net https://fonts.googleapis.com data:; frame-ancestors 'self'; form-action 'self'; frame-src 'self' https://janium.github.io;img-src 'self' blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net;
Otra información	script-src incluye unsafe-inline.
URL	https://ahmedellin.janium.net/
Método	GET
Ataque	
Evidencia	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net https://fonts.googleapis.com data:; frame-ancestors 'self'; form-action 'self'; frame-src 'self' https://janium.github.io;img-src 'self' blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net;
Otra información	script-src incluye unsafe-inline.
URL	https://ahmedellin.janium.net/janium-bin/janium_login.pl
Método	GET
Ataque	
Evidencia	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net https://fonts.googleapis.com data:; frame-ancestors 'self'; form-action 'self'; frame-src 'self' https://janium.github.io;img-src 'self' blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net;
Otra información	script-src incluye unsafe-inline.
URL	https://ahmedellin.janium.net/janium-bin/janium_login_error.pl
Método	GET
Ataque	
Evidencia	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net https://fonts.googleapis.com data:; frame-ancestors 'self'; form-action 'self'; frame-src 'self' https://janium.github.io;img-src 'self' blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net;
Otra información	script-src incluye unsafe-inline.

URL	https://ahmedellin.janium.net/janium-bin/password_reset.pl
Método	GET
Ataque	
Evidencia	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net https://fonts.googleapis.com data:; frame-ancestors 'self'; form-action 'self'; frame-src 'self' https://janium.github.io;img-src 'self' blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net;
Otra información	script-src incluye unsafe-inline.
URL	https://ahmedellin.janium.net/janium-bin/password_reset.pl/send
Método	POST
Ataque	
Evidencia	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net https://fonts.googleapis.com data:; frame-ancestors 'self'; form-action 'self'; frame-src 'self' https://janium.github.io;img-src 'self' blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net;
Otra información	script-src incluye unsafe-inline.
Instancia	6
Solución	Asegúrese de que su servidor web, servidor de aplicación, balanceador de carga, etc. está configurado apropiadamente para establecer la cabecera de Política de Seguridad de Contenido.
Referencia	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693
WASC Id	15
Plugin Id	10055

Medio	**CSP: style-src unsafe-inline**
Descripción	Content Security Policy (CSP) es una capa de seguridad añadida que ayuda a detectar y mitigar ciertos tipos de ataques. Incluyendo (pero no limitado a) Cross Site Scripting (XSS), y ataques de inyección de datos. Estos ataques se utilizan, para todo, desde el robo de datos a la desfiguración de sitios o la distribución de malware. CSP proporciona un conjunto de cabeceras HTTP estándar que permiten a los propietarios de sitios web declarar las fuentes de contenido aprobadas que los navegadores deberían poder cargar en esa página. Los tipos cubiertos son JavaScript, CSS, marcos HTML, fuentes, imágenes y objetos incrustables como applets Java, ActiveX y archivos de audio y vídeo.
URL	http://ahmedellin.janium.net
Método	GET
Ataque	
Evidencia	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net https://fonts.googleapis.com data:; frame-ancestors 'self'; form-action 'self'; frame-src 'self' https://janium.github.io;img-src 'self' blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net;
Otra	

información	style-src incluye unsafe-inline.
URL	https://ahmedellin.janium.net/
Método	GET
Ataque	
Evidencia	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net https://fonts.googleapis.com data:; frame-ancestors 'self'; form-action 'self'; frame-src 'self' https://janium.github.io;img-src 'self' blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net;
Otra información	style-src incluye unsafe-inline.
URL	https://ahmedellin.janium.net/janium-bin/janium_login.pl
Método	GET
Ataque	
Evidencia	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net https://fonts.googleapis.com data:; frame-ancestors 'self'; form-action 'self'; frame-src 'self' https://janium.github.io;img-src 'self' blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net;
Otra información	style-src incluye unsafe-inline.
URL	https://ahmedellin.janium.net/janium-bin/janium_login_error.pl
Método	GET
Ataque	
Evidencia	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net https://fonts.googleapis.com data:; frame-ancestors 'self'; form-action 'self'; frame-src 'self' https://janium.github.io;img-src 'self' blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net;
Otra información	style-src incluye unsafe-inline.
URL	https://ahmedellin.janium.net/janium-bin/password_reset.pl
Método	GET
Ataque	
Evidencia	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net https://fonts.googleapis.com data:; frame-ancestors 'self'; form-action 'self'; frame-src 'self' https://janium.github.io;img-src 'self' blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net;
Otra información	style-src incluye unsafe-inline.
URL	https://ahmedellin.janium.net/janium-bin/password_reset.pl/send
Método	POST
Ataque	
Evidencia	default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net; font-src 'self' https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net https://fonts.googleapis.com data:; frame-ancestors 'self'; form-action 'self'; frame-src 'self'

	https://janium.github.io;img-src 'self' blob: data:; script-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net;
Otra información	style-src incluye unsafe-inline.
Instancia	6
Solución	Asegúrese de que su servidor web, servidor de aplicación, balanceador de carga, etc. está configurado apropiadamente para establecer la cabecera de Política de Seguridad de Contenido.
Referencia	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693
WASC Id	15
Plugin Id	10055

Medio	**Cabecera Content Security Policy (CSP) no configurada**
Descripción	La Política de seguridad de contenido (CSP) es una capa adicional de seguridad que ayuda a detectar y mitigar ciertos tipos de ataques, incluidos Cross Site Scripting (XSS) y ataques de inyección de datos. Estos ataques se utilizan para todo, desde el robo de datos hasta la desfiguración del sitio o la distribución de malware. CSP proporciona un conjunto de encabezados HTTP estándar que permiten a los propietarios de sitios web declarar fuentes de contenido aprobadas que los navegadores deberían poder cargar en esa página; los tipos cubiertos son JavaScript, CSS, marcos HTML, fuentes, imágenes y objetos incrustados como applets de Java, ActiveX, archivos de audio y video.
URL	https://ahmedellin.janium.net/sitemap.xml
Método	GET
Ataque	
Evidencia	
Otra información	
URL	https://ahmedellin.janium.net/janium-bin/janium_store.pl?Id=-
Método	POST
Ataque	
Evidencia	
Otra información	
Instancia	2
Solución	Asegúrese de que su servidor web, servidor de aplicaciones, balanceador de carga, etc. esté configurado para establecer la cabecera Content-Security-Policy.
Referencia	https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
CWE Id	693
WASC Id	15

Plugin Id	10038

Medio	**Librería JS Vulnerable**
Descripción	La librería identificada bootstrap, versión 3.4.1 es vulnerable.
URL	https://ahmedellin.janium.net/janium/js/bootstrap/bootstrap.min.js
Método	GET
Ataque	
Evidencia	* Bootstrap v3.4.1
Otra información	CVE-2024-6484
Instancia	1
Solución	Actualiza a la última versión de bootstrap.
Referencia	https://nvd.nist.gov/vuln/detail/CVE-2024-6484 https://github.com/rubysec/ruby-advisory-db/blob/master/gems/bootstrap-sass/CVE-2024-6484.yml https://www.herodevs.com/vulnerability-directory/cve-2024-6484 https://github.com/twbs/bootstrap https://github.com/twbs/bootstrap/issues/20631 https://github.com/advisories/GHSA-9mvj-f7w8-pvh2 https://github.com/rubysec/ruby-advisory-db/blob/master/gems/bootstrap/CVE-2024-6484.yml
CWE Id	1395
WASC Id	
Plugin Id	10003

Bajo	**Divulgación de Información - Mensajes de Error de Depuración**
Descripción	La respuesta parecía contener mensajes de error comunes devueltos por plataformas como ASP.NET, y servidores Web como IIS y Apache. Puede configurar la lista de mensajes de depuración comunes.
URL	https://ahmedellin.janium.net/janium-bin/janium_store.pl?Id=-
Método	POST
Ataque	
Evidencia	Internal Server Error
Otra información	
Instancia	1
Solución	Desactivar los mensajes de depuración antes de pasar a producción.
Referencia	
CWE Id	200
WASC Id	13
Plugin Id	10023

Bajo	**Divulgación de Marcas de Tiempo - Unix**
Descripción	Una marca de tiempo fue revelada por la aplicación/servidor web. - Unix
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1426881987

Otra información	1426881987, que se evalúa como: 2015-03-20 15:06:27.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1431655765
Otra información	1431655765, que se evalúa como: 2015-05-14 21:09:25.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1432725776
Otra información	1432725776, que se evalúa como: 2015-05-27 06:22:56.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1467031594
Otra información	1467031594, que se evalúa como: 2016-06-27 07:46:34.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1476395008
Otra información	1476395008, que se evalúa como: 2016-10-13 16:43:28.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1476395009
Otra información	1476395009, que se evalúa como: 2016-10-13 16:43:29.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1495990901
Otra información	1495990901, que se evalúa como: 2017-05-28 12:01:41.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1501505948
Otra información	1501505948, que se evalúa como: 2017-07-31 07:59:08.

URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1508970993
Otra información	1508970993, que se evalúa como: 2017-10-25 17:36:33.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1518500249
Otra información	1518500249, que se evalúa como: 2018-02-13 00:37:29.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1522805485
Otra información	1522805485, que se evalúa como: 2018-04-03 20:31:25.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1537002063
Otra información	1537002063, que se evalúa como: 2018-09-15 04:01:03.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1541459225
Otra información	1541459225, que se evalúa como: 2018-11-05 18:07:05.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1546045734
Otra información	1546045734, que se evalúa como: 2018-12-28 20:08:54.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1548603684
Otra información	1548603684, que se evalúa como: 2019-01-27 10:41:24.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET

Ataque	
Evidencia	1549556828
Otra información	1549556828, que se evalúa como: 2019-02-07 11:27:08.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1555081692
Otra información	1555081692, que se evalúa como: 2019-04-12 10:08:12.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1575990012
Otra información	1575990012, que se evalúa como: 2019-12-10 10:00:12.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1595750129
Otra información	1595750129, que se evalúa como: 2020-07-26 02:55:29.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1607167915
Otra información	1607167915, que se evalúa como: 2020-12-05 06:31:55.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1610612736
Otra información	1610612736, que se evalúa como: 2021-01-14 03:25:36.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1610612737
Otra información	1610612737, que se evalúa como: 2021-01-14 03:25:37.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	

Evidencia	1654270250
Otra información	1654270250, que se evalúa como: 2022-06-03 10:30:50.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1694076839
Otra información	1694076839, que se evalúa como: 2023-09-07 03:53:59.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1695183700
Otra información	1695183700, que se evalúa como: 2023-09-19 23:21:40.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1701076831
Otra información	1701076831, que se evalúa como: 2023-11-27 04:20:31.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1731405415
Otra información	1731405415, que se evalúa como: 2024-11-12 04:56:55.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1732584193
Otra información	1732584193, que se evalúa como: 2024-11-25 20:23:13.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1744830464
Otra información	1744830464, que se evalúa como: 2025-04-16 14:07:44.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1744830465
Otra	

información	1744830465, que se evalúa como: 2025-04-16 14:07:45.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1747873779
Otra información	1747873779, que se evalúa como: 2025-05-21 19:29:39.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1750603025
Otra información	1750603025, que se evalúa como: 2025-06-22 09:37:05.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1779033703
Otra información	1779033703, que se evalúa como: 2026-05-17 11:01:43.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1816402316
Otra información	1816402316, que se evalúa como: 2027-07-23 23:11:56.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1836072691
Otra información	1836072691, que se evalúa como: 2028-03-07 15:11:31.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1856431235
Otra información	1856431235, que se evalúa como: 2028-10-29 06:20:35.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1859775393
Otra información	1859775393, que se evalúa como: 2028-12-06 23:16:33.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js

Método	GET
Ataque	
Evidencia	1879048192
Otra información	1879048192, que se evalúa como: 2029-07-18 00:49:52.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1879048193
Otra información	1879048193, que se evalúa como: 2029-07-18 00:49:53.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1894007588
Otra información	1894007588, que se evalúa como: 2030-01-07 04:13:08.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1899447441
Otra información	1899447441, que se evalúa como: 2030-03-11 03:17:21.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1914138554
Otra información	1914138554, que se evalúa como: 2030-08-28 04:09:14.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1925078388
Otra información	1925078388, que se evalúa como: 2031-01-01 18:59:48.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1933667412
Otra información	1933667412, que se evalúa como: 2031-04-11 04:50:12.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET

Ataque	
Evidencia	1955562222
Otra información	1955562222, que se evalúa como: 2031-12-20 14:43:42.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1986661051
Otra información	1986661051, que se evalúa como: 2032-12-14 13:17:31.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	1996064986
Otra información	1996064986, que se evalúa como: 2033-04-02 09:29:46.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	2003034995
Otra información	2003034995, que se evalúa como: 2033-06-22 01:36:35.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	2007800933
Otra información	2007800933, que se evalúa como: 2033-08-16 05:28:53.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	2013265920
Otra información	2013265920, que se evalúa como: 2033-10-18 11:32:00.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	2013265921
Otra información	2013265921, que se evalúa como: 2033-10-18 11:32:01.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	2024104815

Otra información	2024104815, que se evalúa como: 2034-02-20 22:20:15.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	2053994217
Otra información	2053994217, que se evalúa como: 2035-02-01 20:56:57.
Instancia	53
Solución	Confirmar que los datos encontrados de información sobre la marca de tiempo no son sensibles, ni se pueden usar en patrones explotables de divulgación.
Referencia	https://cwe.mitre.org/data/definitions/200.html
CWE Id	200
WASC Id	13
Plugin Id	10096

Bajo	**Divulgación de error de aplicación**
Descripción	Esta página contiene un mensaje de error/advertencia que podría revelar información sensible como la ubicación del archivo que produjo la excepción no controlada. Esta información puede ser usada para lanzas futuros ataques contra la aplicación web. La alerta podría ser una falso positivo si el mensaje de error es encontrado dentro de una página de documentación.
URL	https://ahmedellin.janium.net/janium-bin/janium_store.pl?Id=-
Método	POST
Ataque	
Evidencia	HTTP/1.1 500 Internal Server Error
Otra información	
Instancia	1
Solución	Revisar el código de fuente de esta página. Implementación de páginas de error personalizadas. Considerar implementar un mecanismos para proveer una única referencia/identificación de error para el cliente (navegador) mientras insertando los detalles en el sitio del navegador y no exponiéndolos al usuario.
Referencia	
CWE Id	200
WASC Id	13
Plugin Id	90022

Informativo	**Divulgación de información - Comentarios sospechosos**
Descripción	La respuesta parece contener comentarios sospechosos que pueden ayudar a un atacante. N scripts o archivos se refieren a todo el contenido, no solo a los comentarios.
URL	http://ahmedellin.janium.net
Método	GET
Ataque	
Evidencia	bug
Otra información	Se utilizó el siguiente patrón: \bBUG\b y se detectó en el elemento que comienza por: "<scrip workaround.js"></script>", ver campo de evidencia para el comentario/snippet sospechoso.
URL	https://ahmedellin.janium.net/janium-bin/janium_login.pl

Método	GET
Ataque	
Evidencia	bug
Otra información	Se utilizó el siguiente patrón: \bBUG\b y se detectó en el elemento que comienza por: "<scrip workaround.js"></script>", ver campo de evidencia para el comentario/snippet sospechoso.
URL	https://ahmedellin.janium.net/janium-bin/janium_login_error.pl
Método	GET
Ataque	
Evidencia	bug
Otra información	Se utilizó el siguiente patrón: \bBUG\b y se detectó en el elemento que comienza por: "<scrip workaround.js"></script>", ver campo de evidencia para el comentario/snippet sospechoso.
URL	https://ahmedellin.janium.net/janium/js/adminlte/app.min.js
Método	GET
Ataque	
Evidencia	todo
Otra información	Se utilizó el siguiente patrón: \bTODO\b y se detectó en el elemento que comienza por: "if("u ("AdminLTE requires jQuery");!function(i){"use strict";function s(t,e){if(this.elem", ver campo d
URL	https://ahmedellin.janium.net/janium/js/bootstrap/ie10-viewport-bug-workaround.js
Método	GET
Ataque	
Evidencia	bug
Otra información	Se utilizó el siguiente patrón: \bBUG\b y se detectó en el elemento que comienza por: " * IE1 bug", ver campo de evidencia para el comentario/snippet sospechoso.
URL	https://ahmedellin.janium.net/janium/js/janium/janium.js
Método	GET
Ataque	
Evidencia	from
Otra información	Se utilizó el siguiente patrón: \bFROM\b y se detectó en el elemento que comienza por: " pla de evidencia para el comentario/snippet sospechoso.
URL	https://ahmedellin.janium.net/janium/js/jquery/jquery.min.js
Método	GET
Ataque	
Evidencia	username
Otra información	Se utilizó el siguiente patrón: \bUSERNAME\b y se detectó en el elemento que comienza por module&&"object"==typeof module.exports?module.exports=e.document?t(e,!0):function(", ve sospechoso.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/bootbox.min.js
Método	GET
Ataque	
Evidencia	select
Otra información	Se utilizó el siguiente patrón: \bSELECT\b y se detectó en el elemento que comienza por: "!fu define&&define.amd?define(["jquery"],o):"object"==typeof exports?module.exports=o", ver ca sospechoso.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/bootstrap-notify.min.js
Método	GET

Ataque	
Evidencia	from
Otra información	Se utilizó el siguiente patrón: \bFROM\b y se detectó en el elemento que comienza por: "!fun define(["jquery"],t):t("object"==typeof exports?require("jquery"):jQuery)}(fu", ver campo de evi
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	Bug
Otra información	Se utilizó el siguiente patrón: \bBUG\b y se detectó en el elemento que comienza por: "!functi =typeof module)module.exports=e();else if("function"==typeof define&&defin", ver campo de e
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	bUGS
Otra información	Se utilizó el siguiente patrón: \bBUGS\b y se detectó en el elemento que comienza por: " "Ro "AAEAAAARAQAABAAQR0RFRqWLoiAAAdWAAAACWEdQT1Pk1zcKAAHX2AAAZixHU1V ver campo de evidencia para el comentario/snippet sospechoso.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	Select
Otra información	Se utilizó el siguiente patrón: \bSELECT\b y se detectó 8 veces, la primera en el elemento qu DataTables 2.2.2, AutoFill 2.7.0, Buttons 3.2.2, Column visibility 3.2.2, HTML5 export 3.2.2, ", /snippet sospechoso.
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	TODO
Otra información	Se utilizó el siguiente patrón: \bTODO\b y se detectó en el elemento que comienza por: "!func ("object"==typeof exports&&"object"==typeof module)module.exports=i();else if(", ver campo
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/datatables.min.js
Método	GET
Ataque	
Evidencia	user
Otra información	Se utilizó el siguiente patrón: \bUSER\b y se detectó en el elemento que comienza por: "!func amd?define(["jquery","datatables.net"],function(e){return s(e,window,docu", ver campo de evi
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/jquery.placeholder.min.js
Método	GET
Ataque	
Evidencia	select
Otra información	Se utilizó el siguiente patrón: \bSELECT\b y se detectó en el elemento que comienza por: "!fu define(["jquery"],a):a("object"==typeof module&&module.exports?require("jquer", ver campo d
URL	https://ahmedellin.janium.net/janium/js/jquery/plugin/jquery.validate.min.js
Método	GET

Ataque	
Evidencia	select
Otra información	Se utilizó el siguiente patrón: \bSELECT\b y se detectó en el elemento que comienza por: "!fu define(["jquery"],a):"object"==typeof module&&module.exports?module.exports=a", ver campo sospechoso.
URL	https://ahmedellin.janium.net/janium/js/modernizr/modernizr-respond.min.js
Método	GET
Ataque	
Evidencia	query
Otra información	Se utilizó el siguiente patrón: \bQUERY\b y se detectó en el elemento que comienza por: "/*! polyfill * Copyright 2013 Scott Jehl", ver campo de evidencia para el comentario/snippet sosp
URL	https://ahmedellin.janium.net/janium/js/modernizr/modernizr-respond.min.js
Método	GET
Ataque	
Evidencia	select
Otra información	Se utilizó el siguiente patrón: \bSELECT\b y se detectó en el elemento que comienza por: ";w cssText=a}function D(a,b){return C(n.join(a+";")+(b||""))}function E(a,b){retu", ver campo de ev
URL	https://ahmedellin.janium.net/janium/js/moment/moment.min.js
Método	GET
Ataque	
Evidencia	from
Otra información	Se utilizó el siguiente patrón: \bFROM\b y se detectó en el elemento que comienza por: "!func =typeof module?module.exports=t():"function"==typeof define&&define.amd?def", ver campo sospechoso.
Instancia	19
Solución	Eliminar todos los comentarios que muestren información que pueda ayudar a un atacante y
Referencia	
CWE Id	200
WASC Id	13
Plugin Id	10027

Informativo	**Tecnología Detectada - Bootbox.js**
Descripción	Las siguientes "JavaScript libraries" tecnologías han sido identificadas: Bootbox.js. Descrita como: Bootbox.js is a small JavaScript library which allows you to create custom modal dialogs using Bootstrap modals, without having to worry about creating, managing, or removing any of the required DOM elements or JavaScript event handlers.
URL	http://ahmedellin.janium.net
Método	GET
Ataque	
Evidencia	bootbox.min.js
Otra información	
URL	https://ahmedellin.janium.net/janium-bin/janium_login.pl
Método	GET

Ataque	
Evidencia	bootbox.min.js
Otra información	
Instancia	2
Solución	
Referencia	https://bootboxjs.com/
CWE Id	
WASC Id	13
Plugin Id	10004

Informativo	**Tecnología Detectada - Bootstrap**
Descripción	Las siguientes "UI frameworks" tecnologías han sido identificadas: Bootstrap. Descrita como: Bootstrap is a free and open-source CSS framework directed at responsive, mobile-first front-end web development. It contains CSS and JavaScript-based design templates for typography, forms, buttons, navigation, and other interface components.
URL	http://ahmedellin.janium.net
Método	GET
Ataque	
Evidencia	bootstrap-notify.min.js
Otra información	El CPE siguiente está asociado con la tecnología identificada: cpe:2.3:a:getbootstrap:bootstrap:*:*:*:*:*:*:*:* Las siguientes versiones están asociadas con la tecnología: 10
URL	https://ahmedellin.janium.net/janium-bin/password_reset.pl
Método	GET
Ataque	
Evidencia	bootstrap-notify.min.js
Otra información	El CPE siguiente está asociado con la tecnología identificada: cpe:2.3:a:getbootstrap:bootstrap:*:*:*:*:*:*:*:*
Instancia	2
Solución	
Referencia	https://getbootstrap.com
CWE Id	
WASC Id	13
Plugin Id	10004

Informativo	**Tecnología Detectada - DataTables**
Descripción	Las siguientes "JavaScript libraries" tecnologías han sido identificadas: DataTables. Descrita como: DataTables is a plug-in for the jQuery Javascript library adding advanced features like pagination, instant search, themes, and more to any HTML table.
URL	http://ahmedellin.janium.net
Método	GET
Ataque	
Evidencia	datatables.min.js

Otra información	El CPE siguiente está asociado con la tecnología identificada: cpe:2.3:a:datatables:datatables.net:*:*:*:*:*:*:*:*
URL	https://ahmedellin.janium.net/janium-bin/janium_login.pl
Método	GET
Ataque	
Evidencia	datatables.min.js
Otra información	El CPE siguiente está asociado con la tecnología identificada: cpe:2.3:a:datatables:datatables.net:*:*:*:*:*:*:*:*
Instancia	2
Solución	
Referencia	https://datatables.net
CWE Id	
WASC Id	13
Plugin Id	10004

Informativo	**Tecnología Detectada - Google Font API**
Descripción	Las siguientes "Font scripts" tecnologías han sido identificadas: Google Font API. Descrita como: Google Font API is a web service that supports open-source font files that can be used on your web designs.
URL	http://ahmedellin.janium.net
Método	GET
Ataque	
Evidencia	fonts.googleapis.com
Otra información	
URL	https://ahmedellin.janium.net/janium-bin/janium_login.pl
Método	GET
Ataque	
Evidencia	fonts.googleapis.com
Otra información	
Instancia	2
Solución	
Referencia	https://google.com/fonts
CWE Id	
WASC Id	13
Plugin Id	10004

Informativo	**Tecnología Detectada - HSTS**
Descripción	Las siguientes "Security" tecnologías han sido identificadas: HSTS. Descrita como: HTTP Strict Transport Security (HSTS) informs browsers that the site should only be accessed using HTTPS.

URL	http://ahmedellin.janium.net
Método	GET
Ataque	
Evidencia	Strict-Transport-Security
Otra información	
URL	https://ahmedellin.janium.net/robots.txt
Método	GET
Ataque	
Evidencia	Strict-Transport-Security
Otra información	
Instancia	2
Solución	
Referencia	https://www.rfc-editor.org/rfc/rfc6797#section-6.1
CWE Id	
WASC Id	13
Plugin Id	10004

Informativo	**Tecnología Detectada - Modernizr**
Descripción	Las siguientes "JavaScript libraries" tecnologías han sido identificadas: Modernizr. Descrita como: Modernizr is a JavaScript library that detects the features available in a user's browser.
URL	http://ahmedellin.janium.net
Método	GET
Ataque	
Evidencia	modernizr/modernizr-respond.min.js
Otra información	
URL	https://ahmedellin.janium.net/janium-bin/janium_login.pl
Método	GET
Ataque	
Evidencia	modernizr/modernizr-respond.min.js
Otra información	
Instancia	2
Solución	
Referencia	https://modernizr.com
CWE Id	
WASC Id	13
Plugin Id	10004

Informativo	**Tecnología Detectada - Moment.js**
	Las siguientes "JavaScript libraries" tecnologías han sido identificadas: Moment.js.

Descripción	Descrita como: Moment.js is a free and open-source JavaScript library that removes the need to use the native JavaScript Date object directly.
URL	http://ahmedellin.janium.net
Método	GET
Ataque	
Evidencia	moment.min.js
Otra información	El CPE siguiente está asociado con la tecnología identificada: cpe:2.3:a:momentjs:moment:*:*:*:*:*:*:*:*
URL	https://ahmedellin.janium.net/janium-bin/janium_login.pl
Método	GET
Ataque	
Evidencia	moment.min.js
Otra información	El CPE siguiente está asociado con la tecnología identificada: cpe:2.3:a:momentjs:moment:*:*:*:*:*:*:*:*
Instancia	2
Solución	
Referencia	https://momentjs.com
CWE Id	
WASC Id	13
Plugin Id	10004

Informativo	**Tecnología Detectada - jQuery**
Descripción	Las siguientes "JavaScript libraries" tecnologías han sido identificadas: jQuery. Descrita como: jQuery is a JavaScript library which is a free, open-source software designed to simplify HTML DOM tree traversal and manipulation, as well as event handling, CSS animation, and Ajax.
URL	http://ahmedellin.janium.net
Método	GET
Ataque	
Evidencia	jquery
Otra información	El CPE siguiente está asociado con la tecnología identificada: cpe:2.3:a:jquery:jquery:*:*:*:*:*:*:*:*
URL	https://ahmedellin.janium.net/janium-bin/password_reset.pl
Método	GET
Ataque	
Evidencia	jquery
Otra información	El CPE siguiente está asociado con la tecnología identificada: cpe:2.3:a:jquery:jquery:*:*:*:*:*:*:*:*
Instancia	2
Solución	
Referencia	https://jquery.com
CWE Id	

WASC Id	13
Plugin Id	10004

Informativo	User Agent Fuzzer
Descripción	Compare las diferencias en la respuesta según el fuzzeo de User Agent (por ejemplo, sitios móviles, acceso como un motor de búsqueda). Compara el código de estado de la respuesta y el hash del cuerpo de la respuesta con la respuesta original.
URL	http://ahmedellin.janium.net
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidencia	
Otra información	
URL	http://ahmedellin.janium.net
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidencia	
Otra información	
URL	http://ahmedellin.janium.net
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidencia	
Otra información	
URL	http://ahmedellin.janium.net
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidencia	
Otra información	
URL	http://ahmedellin.janium.net
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidencia	
Otra información	
URL	http://ahmedellin.janium.net
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidencia	
Otra información	
URL	http://ahmedellin.janium.net

Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidencia	
Otra información	
URL	http://ahmedellin.janium.net
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidencia	
Otra información	
URL	http://ahmedellin.janium.net
Método	GET
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidencia	
Otra información	
URL	http://ahmedellin.janium.net
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidencia	
Otra información	
URL	http://ahmedellin.janium.net
Método	GET
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidencia	
Otra información	
URL	http://ahmedellin.janium.net
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidencia	
Otra información	
URL	http://ahmedellin.janium.net/robots.txt
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidencia	
Otra información	
URL	http://ahmedellin.janium.net/robots.txt

Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidencia	
Otra información	
URL	http://ahmedellin.janium.net/robots.txt
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidencia	
Otra información	
URL	http://ahmedellin.janium.net/robots.txt
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidencia	
Otra información	
URL	http://ahmedellin.janium.net/robots.txt
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidencia	
Otra información	
URL	http://ahmedellin.janium.net/robots.txt
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidencia	
Otra información	
URL	http://ahmedellin.janium.net/robots.txt
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidencia	
Otra información	
URL	http://ahmedellin.janium.net/robots.txt
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidencia	
Otra información	
URL	http://ahmedellin.janium.net/robots.txt
Método	GET

Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidencia	
Otra información	
URL	http://ahmedellin.janium.net/robots.txt
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidencia	
Otra información	
URL	http://ahmedellin.janium.net/robots.txt
Método	GET
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidencia	
Otra información	
URL	http://ahmedellin.janium.net/robots.txt
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidencia	
Otra información	
URL	http://ahmedellin.janium.net/sitemap.xml
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidencia	
Otra información	
URL	http://ahmedellin.janium.net/sitemap.xml
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidencia	
Otra información	
URL	http://ahmedellin.janium.net/sitemap.xml
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidencia	
Otra información	
URL	http://ahmedellin.janium.net/sitemap.xml
Método	GET

Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidencia	
Otra información	
URL	http://ahmedellin.janium.net/sitemap.xml
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidencia	
Otra información	
URL	http://ahmedellin.janium.net/sitemap.xml
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidencia	
Otra información	
URL	http://ahmedellin.janium.net/sitemap.xml
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidencia	
Otra información	
URL	http://ahmedellin.janium.net/sitemap.xml
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidencia	
Otra información	
URL	http://ahmedellin.janium.net/sitemap.xml
Método	GET
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidencia	
Otra información	
URL	http://ahmedellin.janium.net/sitemap.xml
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidencia	
Otra información	
URL	http://ahmedellin.janium.net/sitemap.xml
Método	GET

Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidencia	
Otra información	
URL	http://ahmedellin.janium.net/sitemap.xml
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidencia	
Otra información	
Instancia	36
Solución	
Referencia	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	10104

Janium S.A.S.

Calle 93 #11A - 28
Oficina 601 Edificio
Capital Park
Bogotá, Colombia

Tel. (571) 344 17 60
www.janium.com

Ciudad de México a 03 de marzo de 2025.

Isabel Cristina Bernal Vinasco
Subdirectora de Contenidos y Patrimonio
Biblioteca Pública Piloto
Presente

Por este medio hago de su conocimiento las mejoras realizadas en el sistema Janium de Febrero de 2025.

2025-02-27 v2023 rafe298196

- Se corrige condición que podía provocar un fallo en el OPAC cuando un registro no contaba con información en etiquetas configuradas para despliegue.

2025-02-25 v2023 rf670b89c9

- Se añaden parámetros de contexto de sesión durante la construcción de las barras de navegación para posibilitar una personalización más precisa de las mismas.

2025-02-13 v2023 r785288daf

- Se actualizan bibliotecas de Javascript de terceros que han implementado cambios para enfrentar posibles riesgos de seguridad.

Sin otro particular, quedo a sus órdenes.



Zandra Mendoza
Ejecutivo de Soporte
Janium

Janium S.A.S.

Carrera 7 no. 156 – 68
North Point 3 Oficina
1005 Bogotá, Colombia
Tel. (571) 467 4363
www.janium.com

Bogotá, Colombia a 3 de marzo de 2025

Isabel Cristina Bernal Vinasco
Subdirector de Contenidos y Patrimonio
Biblioteca Pública Piloto
P r e s e n t e

Estimada Dra. Bernal:

Le remito un cordial saludo y le hago entrega del enlace donde se encuentran almacenados los respaldos de las bases de datos correspondientes a Febrero de 2025 para los sitios:

https://ahmedellin.janium.net
https://bibliotecapiloto.janium.net
https://rbmam.janium.net

El enlace es:

https://workdrive.janium.com/external/7c0a11163a36cc3bca6a58fb173bb1334a240c8385c70c1a82ffac663e37f46a

Este enlace está protegido con contraseña (la cual es la acordada previamente y que por seguridad no se coloca en este oficio) y tiene fecha de caducidad para el 10 de marzo de 2025 a las 23:59 horas.

Con esto damos cumplimiento a lo estipulado en el contrato No. 0240 de 2024, sobre el punto “Envío de los datos de respaldo en los primeros 10 días del mes vencido”.

Atentamente



José Amador Rodríguez Mejía

Gerente de Soporte Técnico

Janium

Janium S.A.S.

Calle 93 # 11A – 28 Of. 601
Edificio Capital Park
Bogotá, Colombia
Pbx. (57 1) 344 1760
Cel. (57) 321 499 9867
www.janium.com

Bogotá, 03 marzo de 2025

Señores
BIBLIOTECA PÚBLICA PILOTO DE MEDELLÍN PARA AMÉRICA LATINA
Medellín

ALEX YESID BELALCAZAR GUERRERO, identificado con cédula de ciudadanía No. 79.628.043 de Bogotá en mi calidad de representante legal de la Sociedad **JANIUM S.A.S.** sociedad domiciliada en la ciudad de Bogotá D.C identificada con **NIT. 830.141.046-4**, certifico que a la fecha y en particular durante los seis (6) meses anteriores a la fecha de expedición de esta certificación, la sociedad se encuentra al día en las obligaciones con los sistemas de salud, riesgos profesionales, pensiones y aportes a cajas de compensación familiar, Instituto Colombiano de Bienestar Familiar y Servicio Nacional de Aprendizaje.

Con relación a la "Planilla Integrada de Autoliquidación de Aportes" a través de la cual se efectuaron los pagos respectivos al periodo de cotización en Salud del Mes de **FEBRERO 2025** y en Pensión del Mes de **ENERO 2025,** informamos: (i) El número de radicación es el **84020748** y (ii) El número de autorización es el **1256031402.**

Esta certificación se expide a solicitud del interesado y en cumplimiento del artículo 50, de la ley 789 de 2002.



ALEX YESID BELALCAZAR GUERRERO
REPRESENTANTE LEGAL
JANIUM S.A.S.
Nit. 830.141.046 – 4

compensar | miplanilla.com

REPORTE RESUMEN DE PAGO

Información básica de la planilla

Empresa:	Janium S.A.S	**NIT:**	830141046
Tipo Planilla:	E	**Periodo liquidación Pensiones:**	enero 2025
Sucursal o Dependencia:	PRINCIPAL	**Periodo liquidación Salud:**	febrero 2025
Número de Radicación:	84020748	**Total a pagar:**	$8,917,800
Fecha de vencimiento:	12/02/2025	**Total de empleados:**	4
Fecha de Pago:	10/02/2025	**Número de Administradoras:**	10

Detalles del pago

Razón social recaudo:	Compensar OI	**Nit recaudo:**	9998600669427
Descripción:	MiPlanilla.com Pago Proteccion Social	**Medio de Pago:**	Pago Electronico por PSE
Banco:	BANCO BBVA COLOMBIA S.A.	**Número Autorización:**	1256031402
Estado de la transacción:	Transacción aprobada		

Código	NIT	Administradoras	Num. Afiliados	*Número de incapacidad por riesgos laborales	Valor descontado en incapacidad y/o licencia	Total Pagado
14-23	860011153	POSITIVA COMPANIA DE SEGUROS	4		$0	$151,200
230301	800224808	Porvenir	1		$0	$1,953,400
25-14	900336004	Administradora Colombiana de Pensiones -	3		$0	$2,946,000
CCF03	890900842	Comfenalco Antioquia Caja de Compensacion Fliar	1		$0	$232,000
CCF24	860066942	Compensar Caja de Compensacion Fliar	3		$0	$926,000
EPS005	800251440	Sanitas EPS	2		$0	$1,525,100
EPS008	860066942	Compensar EPS	1		$0	$377,600
EPS010	800088702	EPS Sura	1		$0	$232,000
PAICBF	899999239	ICBF Instituto Colombiano de Bienestar Familiar	1		$0	$344,700
PASENA	899999034	SENA	1		$0	$229,800
						$8,917,800

***Si descontó incapacidades o notas crédito debe informar a la administradora correspondiente los descuentos.**

Este documento está clasificado como PRIVADO por parte de Compensar Operador de Información