AUDITORIA AL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION

INFORME DEFINITIVO

ADRIANA GIRALDO RAMIREZ
Jefe Control Interno

FELIPE ANDRES RESTREPO ZUUAGA

Contratista apoyo - Oficina de Control Interno

OFICINA DE CONTROL INTERNO

Octubre de 2019

ANM-OCI-047-2019

TABLA DE CONTENIDO

1. OBJETIVO GENERAL 3

2. OBJETIVOS ESPECIFICOS 3

3. ALCANCE 3

4. METODOLOGÍA 3

5. RESULTADOS 4

5.1 Controles evaluados del Anexo A de la norma ISO 27001 4

5.1.1 Política de Seguridad de la Información: 4

5.1.2 Organización de la Seguridad de la Información: 4

5.1.3 Gestión de Activos: 5

5.1.4 Controles de Acceso: 5

5.1.5 Criptografía: 16

5.1.6 Códigos maliciosos: 17

5.1.7 Copias de respaldo: 18

5.1.8 5.1.8 Gestión de la vulnerabilidad técnica: 18

5.1.9 Seguridad en las comunicaciones: 19

5.1.10 Adquisición, desarrollo y mantenimiento de sistemas: 22

5.1.11 Gestión de incidentes de Seguridad de la Información: 26

5.1.12 Gestión de la continuidad del negocio: 26

6. OPORTUNIDADES DE MEJORA 27

1. OBJETIVO GENERAL

Evaluar el estado y nivel de madurez del Sistema de Gestión de Seguridad de la Información que tiene implementado la Agencia Nacional de Minería.

2. OBJETIVOS ESPECIFICOS

Verificar algunos de los controles que están en el Anexo A de la norma ISO 27001:2013 y que deben estar implementados para poder soportar el SGSI

3. ALCANCE

La Oficina de Control Interno en su rol de evaluación y seguimiento, realizó la verificación de los controles que soportan el Sistema de Gestión de Seguridad de la Información, con corte de septiembre 2019.

4. METODOLOGÍA

La Oficina de Control Interno con el fin de verificar el cumplimiento de la política nacional de Gobierno Digital, realizó la evaluación al Sistema de Gestión de Seguridad de la Información, teniendo como objetivo la evaluación de los controles del anexo A de la norma ISO 27001.

Soportados en la estrategia de mejora continua (Planear, Hacer, Verificar y Actuar), tomamos cada uno de los controles para proceder a evaluarlos teniendo como herramientas la realización de entrevistas, pruebas de recorrido, reuniones y el uso de técnicas asistidas para evaluar los tres pilares de seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

Se evaluaron todos los dominios de la norma, excepto el de seguridad de los recursos humanos, y en el informe sólo hacemos referencia a aquellos, en los cuales vemos oportunidades de mejora o la necesidad de su implementación. Dicha evaluación se efectuaron a través de entrevistas a los encargados de los procesos, recolección de pruebas documentales y pruebas a través de la VPN, en un periodo de tiempo del 15 de agosto al 30 de septiembre de 2019.

Para la elaboración del presente informe se tendrán en cuenta los términos definidos en el procedimiento EVA1-P-001 Versión 2 denominado Auditoría Interna, que establece lo siguiente:

"**EVIDENCIAS DE AUDITORÍA**: Registros, declaraciones de hechos o cualquier otra información que es pertinente para los criterios de auditoría y que es verificable. Definición tomada de la Norma Técnica Colombiana NTC-ISO 9000:2015, Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC)". La evidencia de auditoría puede ser cualitativa o cuantitativa, es utilizada en auditoría para determinar cuándo se cumple con el criterio de auditoría. La evidencia de auditoría se basa en la realización de entrevistas, revisión de documentos, observación de actividades y condiciones, resultados de mediciones y pruebas.

"NO CONFORMIDAD: *Incumplimiento de un requisito. Definición tomada de la Norma Técnica Colombiana NTC-ISO 9000:2015, Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC)".* Se constituye, cuando existe evidencia objetiva del incumplimiento. Para lo cual debe plantearse una ACCIÓN CORRECTIVA, con la implementación de un plan de mejoramiento interno, que se ejecutable y medible, el cual debe radicarse en el Sistema de Información ISOLUCION de la Agencia Nacional de Minería.

"*OPORTUNIDAD DE MEJORA:* Son oportunidades detectadas que permiten ofrecer una mejora sustancial a los procesos, productos, servicios, procedimientos, instructivos ambiente de trabajo, entre otros.". Para lo cual debe planear una ACCIÓN DE MEJORA, con la implementación de un plan de mejoramiento interno, que se ejecutable y medible, el cual debe radicarse en ISOLUCION.

El informe preliminar se remitió a la Jefe de la Oficina de Tecnología en información mediante memorando 201911002266043 del 10 de Octubre de 2019, donde se expresa un plazo de 5 días para su controversia. Una vez vencido el término y no a ver recibido informar se libera el siguiente informe definitivo.

5. RESULTADOS

De acuerdo a los resultados obtenidos en la evaluación realizada al estado y nivel de madurez del Sistema de Gestión de Seguridad de la Información, que a la fecha tiene implementado la Agencia Nacional de Minería, podemos concluir que el Sistema de Gestión de Seguridad de la Información, se encuentra en una **ETAPA TEMPRANA DE IMPLEMENTACIÓN**, esto debido a que hay controles del Anexo A de la norma ISO 27001:2013, que no funcionan de manera adecuada y otros controles que no están implementados.

5.1 Controles evaluados del Anexo A de la norma ISO 27001

5.1.1 Política de Seguridad de la Información:

La Agencia Nacional de Minería, cuenta con la Política de Seguridad de la información, la cual fue establecida por la resolución 104 del 2 de marzo de 2018, en el capítulo 4. En esta política se hace referencia al Manual de Seguridad, en el cual hay controles, que aún no se encuentran implementados, algunos de ellos son el cifrado en las comunicaciones, se observan deficiencias en controles, también se ha evidenciado deficiencia en el contenido y la estructura de algunas políticas.

- En el tema de activos de información se presentan debilidades pues no están inventariados, y no están clasificados con respecto al nivel de riesgo.
- No se evidenció un documento escrito en el cual se determine que los empleados, contratistas y proveedores están obligados a cumplir la política del Seguridad de la Información y más aún deban ser participantes activos del Sistema de Gestión de Seguridad de la Información.

5.1.2 Organización de la Seguridad de la Información:

Se evidencia compromiso de la alta dirección con el SGSI, pues se ha asignado el presupuesto para el rol de Oficial de Seguridad de la Información, se tiene definido la adquisición de herramientas para seguridad de la información, se le ha dado un espacio al Oficial de Seguridad de la Información en el comité institucional y de desempeño. También se evidencio que los roles, las responsabilidades y las funciones dentro del SGSI, aún no se tienen definidos, no hay un área de riesgos en la cual los temas de riesgo cibernético estén contemplados.

Aunque se evidencia cierta conciencia en Seguridad de la Información hay temas que se deben mejorar, como es el caso de los activos de información**.** No se evidencia el seguimiento a los registros de auditoria, pues el Sistema de Gestión de Seguridad de la Información, la última vez que se evaluó fue en el año 2017. No se tiene una lista de contactos de entidades reguladoras, autoridades y organismos con conocimiento y experticia en Seguridad de la Información, a los cuales se pueda acudir en caso de un incidente de Seguridad de la Información.

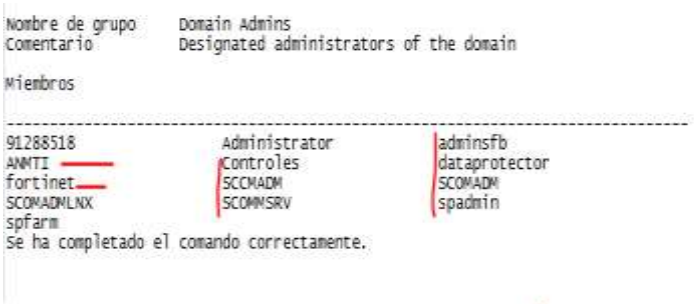
5.1.3 Gestión de Activos:

En cuanto a la gestión de activos no se pudo determinar la razonabilidad y suficiencia de un inventario de activos, se tiene establecido desde el portal de datos abiertos, pero este no corresponde a un inventario de activos de información que sirva de insumo principal de un Sistema de Gestión de Seguridad de la Información. Con el inventario de activos se procede a la evaluación de riesgos de acuerdo al impacto y probabilidad de materialización del riesgo y no existen procedimientos, herramientas de software y hardware para la eliminación de información en medios magnéticos y que los datos confidenciales se eliminen de forma segura (borrado criptográfico, desmagnetización o destrucción física).

5.1.4 Controles de Acceso:

En el manual de seguridad de la información se hace referencia a la autenticación de doble factor, y este no se tiene implementado en los sistemas de información críticos de la ANM. No hay un proceso de revisión de cuentas privilegiadas, hay cuentas por defecto, las cuales son utilizadas en el Directorio Activo, como la utilización del usuario Administrador del Directorio Activo, en tareas de operación y gestión del Directorio de Servicios.

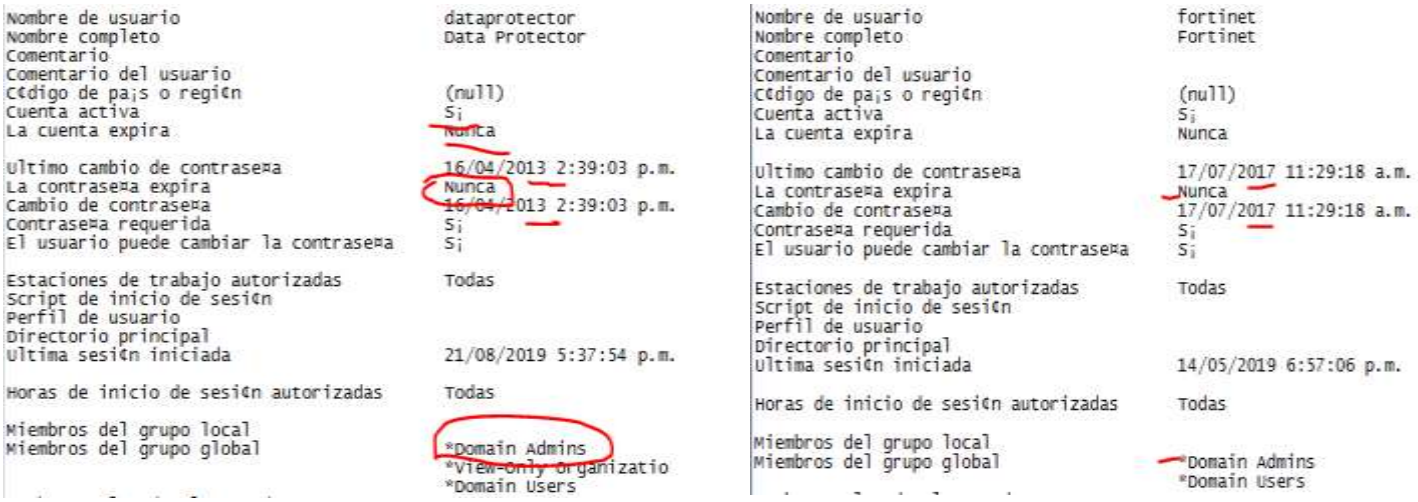
Se evidencia la presencia de usuarios genéricos en la red y que hacen parte del grupo global "*Domain Admins*", Administradores del Dominio ANM.LOCAL, algunos de ellos son (dataprotector, adminsfb, Controles, etc).



```
Nombre de grupo     Domain Admins
Comentario          Designated administrators of the domain

Miembros

-------------------------------------------------------------------------------
91288518             Administrator        adminsfb
ANMTI                Controles            dataprotector
fortinet             SCCMADM              SCOMADM
SCOMADMLNX           SCOMMSRV             spadmin
spfarm
Se ha completado el comando correctamente.
```

Imagen Nro. 1: Usuarios genéricos en el grupo "Domain Admins", del dominio ANM.LOCAL

Se evidenciaron cuentas genéricas del grupo "Domain Admins", Administradores del Dominio ANM.LOCAL, en las cuales la contraseña nunca expira y son cuentas de red creadas en los años 2013 y 2017 respectivamente.

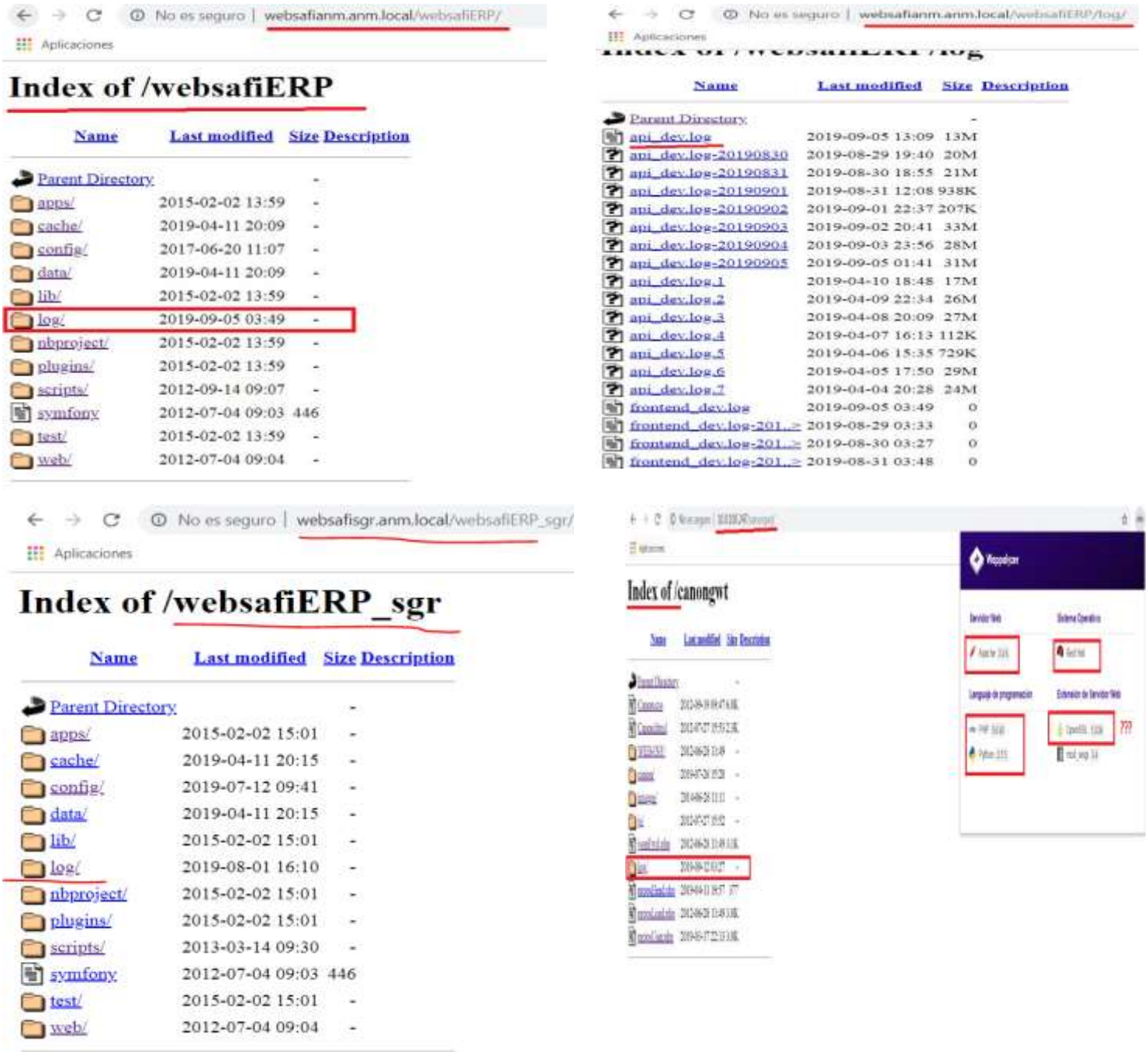


```
Nombre de usuario                 dataprotector
Nombre completo                   Data Protector
Comentario
Comentario del usuario
C¢digo de pa¡s o regi¢n           (null)
Cuenta activa                     S¡
La cuenta expira                  Nunca

Ultimo cambio de contrase¤a       16/04/2013 2:39:03 p.m.
La contrase¤a expira              Nunca
Cambio de contrase¤a              16/04/2013 2:39:03 p.m.
Contrase¤a requerida              S¡
El usuario puede cambiar la contrase¤a  S¡

Estaciones de trabajo autorizadas Todas
Script de inicio de sesi¢n
Perfil de usuario
Directorio principal
Ultima sesi¢n iniciada            21/08/2019 5:37:54 p.m.

Horas de inicio de sesi¢n autorizadas  Todas

Miembros del grupo local
Miembros del grupo global         *Domain Admins
                                  *View-Only Organizatio
                                  *Domain Users
```

```
Nombre de usuario                 fortinet
Nombre completo                   Fortinet
Comentario
Comentario del usuario
C¢digo de pa¡s o regi¢n           (null)
Cuenta activa                     S¡
La cuenta expira                  Nunca

Ultimo cambio de contrase¤a       17/07/2017 11:29:18 a.m.
La contrase¤a expira              Nunca
Cambio de contrase¤a              17/07/2017 11:29:18 a.m.
Contrase¤a requerida              S¡
El usuario puede cambiar la contrase¤a  S¡

Estaciones de trabajo autorizadas Todas
Script de inicio de sesi¢n
Perfil de usuario
Directorio principal
Ultima sesi¢n iniciada            14/05/2019 6:57:06 p.m.

Horas de inicio de sesi¢n autorizadas  Todas

Miembros del grupo local
Miembros del grupo global         *Domain Admins
                                  *Domain Users
```

Imágenes Nro. 2: Usuarios dataprotector y fortinet en el grupo "Domain Admins", que la contraseña nunca expira

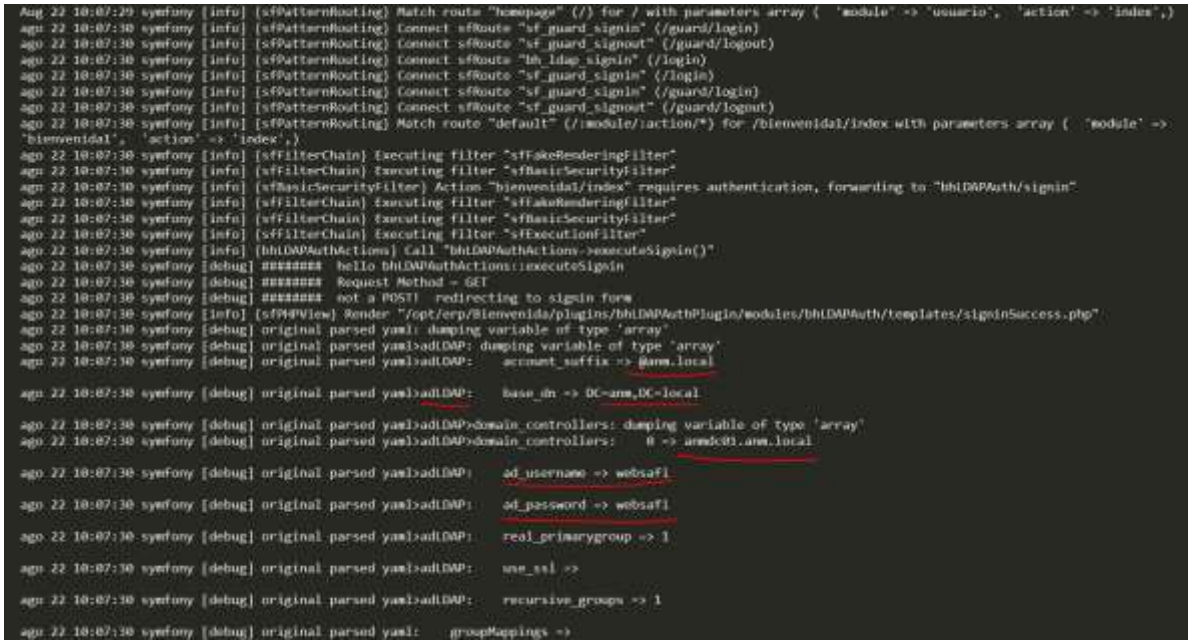
En los sistemas de información WEBSAFI, CANON y WEBSAFISGR, se evidencian archivos a los cuales se logra acceder debido a que el servidor permite listar los directorios.



Imágenes Nro. 3: Listado de directorios "Índex Of" en los servidores de la aplicaciones Websafi, Websafi SGR y Canon

En **archivos de log** se evidencian credenciales de acceso a las aplicaciones (Websafi, Websafi SGR y Canon), en los **archivos de configuración** punto yml y punto propierties, se observan cadenas de conexión a los gestores de bases de datos, también se encontraron manuales en los cuales, está el paso a paso de la

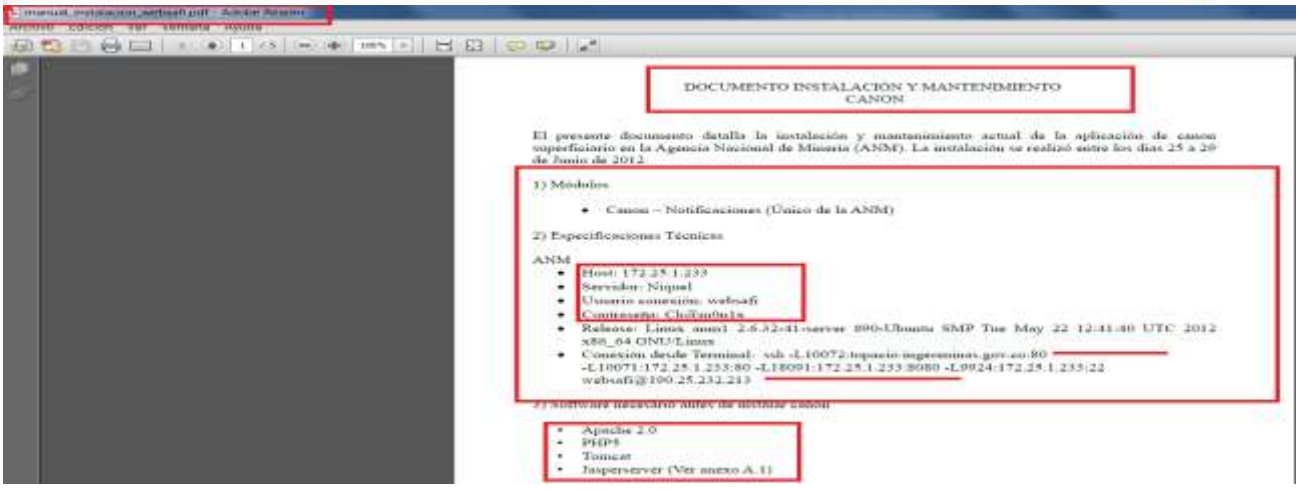
configuración de las aplicaciones, inclusive con el usuario y contraseña de conexión a base de datos, conexión por SSH, la dirección ip del servidor y demás datos adicionales, que vulneran la confidencialidad de la información.



```
Datos conexion ERP
ERP
ERP_classpath=./jdbc/oracle/ojdbc6.jar
ERP_password=werp
ERP_url=jdbc:oracle:thin:@zirconio2.ingeominas.gov.co:1522:anmerp
ERP_user=werp
Datos conexion Directorio Activo
DIRECTORIO_ACTIVO
directorio_classpath=ldap
directorio_password=W3bs@fi
directorio_url=ldap://172.25.1.218:389/dc=ingeominas,dc=local
directorio_user=CN=sofhouse,CN=Users,DC=ingeominas,DC=local
```

```
all:
  doctrine:
    class: sfDoctrineDatabase
    param:
      classname: DoctrinePDO
      dsn: 'oracle:dbname=//anmrac.anm.local:1521/WEBSAFIPROD;charset=AL32UTF8'
      username: werp
      password: WERP
```

```
Datos conexion ERP
ERP
ERP_classpath=./jdbc/oracle/ojdbc6.jar
ERP_password=werp
ERP_url=jdbc:oracle:thin:@zirconio2.ingeominas.gov.co:1522:anmerp
ERP_user=werp
Datos conexion Directorio Activo
DIRECTORIO_ACTIVO
directorio_classpath=ldap
directorio_password=W3bs@fi
directorio_url=ldap://172.25.1.218:389/dc=ingeominas,dc=local
directorio_user=CN=sofhouse,CN=Users,DC=ingeominas,DC=local
```



DOCUMENTO INSTALACION Y MANTENIMIENTO
CANON

El presente documento detalla la instalación y mantenimiento actual de la aplicación de canon superficiario en la Agencia Nacional de Minería (ANM). La instalación se realizó entre los días 25 a 29 de Junio de 2012.

1) Módulos

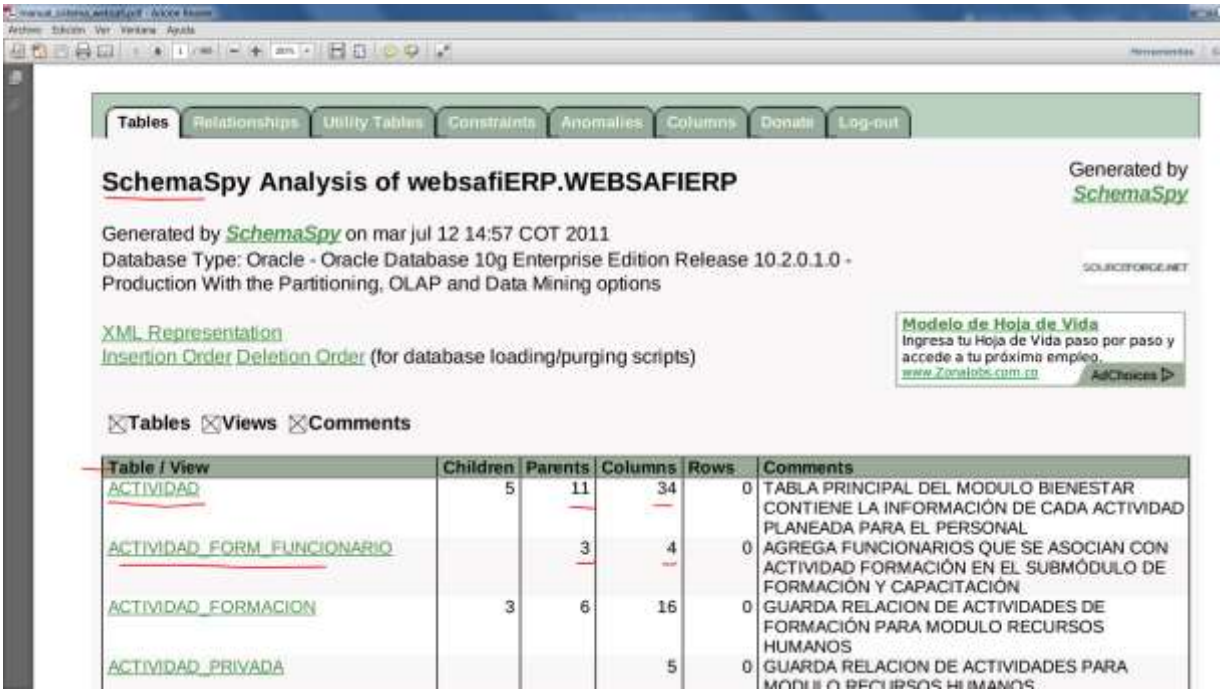
- Canon – Notificaciones (Único de la ANM)

2) Especificaciones Técnicas

ANM

- Host: 172.25.1.233
- Servidor: Niquel
- Usuario conexión: websafi
- Contraseña: Chiribuela
- Release: Linux anm1 2.6.32-41-server #90-Ubuntu SMP Tue May 22 12:41:40 UTC 2012 x86_64 GNU/Linux
- Conexión desde Terminal: ssh -L10072:topazio.ingeominas.gov.co:80 -L10071:172.25.1.233:80 -L18091:172.25.1.233:8080 -L0924:172.25.1.235:22 websafi@190.25.232.213

- Apache 2.0
- PHP4
- Tomcat
- Inspeserver (Ver anexo A.1)



Tables | Relationships | Utility Tables | Constraints | Anomalies | Columns | Donate | Log-out

SchemaSpy Analysis of websafiERP.WEBSAFIERP

Generated by SchemaSpy

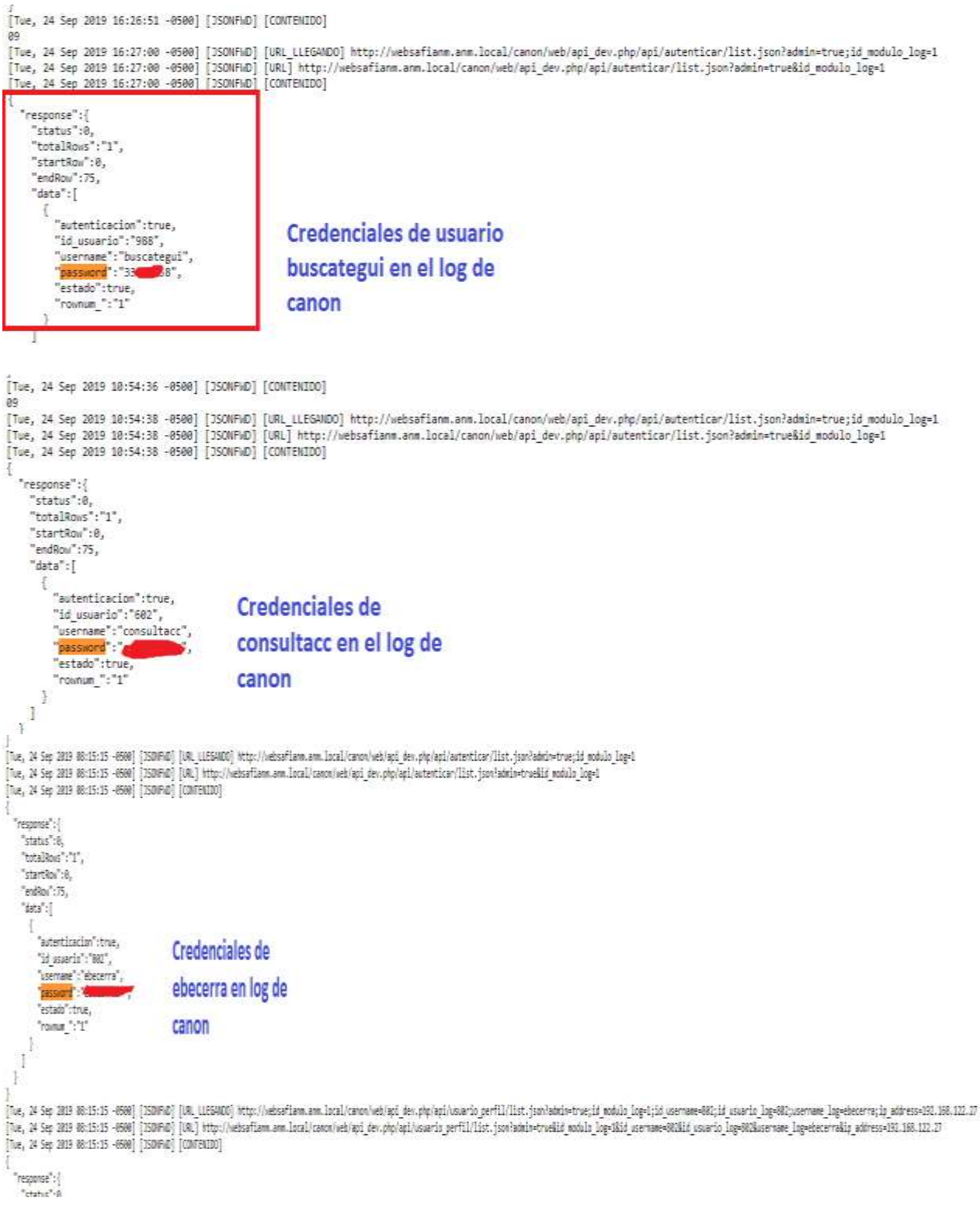
Generated by SchemaSpy on mar jul 12 14:57 COT 2011
Database Type: Oracle - Oracle Database 10g Enterprise Edition Release 10.2.0.1.0 - Production With the Partitioning, OLAP and Data Mining options

XML Representation
Insertion Order Deletion Order (for database loading/purging scripts)

☒Tables ☒Views ☒Comments

Table / View	Children	Parents	Columns	Rows	Comments
ACTIVIDAD	5	11	34	0	TABLA PRINCIPAL DEL MODULO BIENESTAR CONTIENE LA INFORMACIÓN DE CADA ACTIVIDAD PLANEADA PARA EL PERSONAL
ACTIVIDAD_FORM_FUNCIONARIO		3	4	0	AGREGA FUNCIONARIOS QUE SE ASOCIAN CON ACTIVIDAD FORMACIÓN EN EL SUBMÓDULO DE FORMACIÓN Y CAPACITACIÓN
ACTIVIDAD_FORMACION	3	6	16	0	GUARDA RELACION DE ACTIVIDADES DE FORMACIÓN PARA MODULO RECURSOS HUMANOS
ACTIVIDAD_PRIVADA			5	0	GUARDA RELACION DE ACTIVIDADES PARA MODULO RECURSOS HUMANOS

```
adLDAP:
# These settings are parameters for the adLDAP library.  See
# its code (plugins/bhLDAPAuthPlugin/lib/adLDAP.php) and documentation
# (http://adldap.sourceforge.net) for help.

  # the AD domain's name
  account_suffix      :  "@anm.local"

  # base for all users and groups
  base_dn             :  "DC=anm,DC=local"


  # An array of domain controllers. Specify multiple controllers if you
  # would like the class to balance the LDAP queries amongst multiple servers
  domain_controllers:
    - "anmdc01.anm.local"

  ad_username         : websafi
  ad_password         : websafi

  # AD does not return the primary group.
  # http://support.microsoft.com/?kbid=321360

  # This tweak will resolve the real primary group, but may be resource
  # intensive.  Setting to false will fudge "Domain Users" and is much
  # faster. Keep in mind though that if someone's primary group is NOT
  # domain users, this is obviously going to bollocks the results
  real_primarygroup   : true


  # Use SSL, but your server needs to be setup.
  #  see http://adldap.sourceforge.net/ldap_ssl.php
  use_ssl             : false  -> ????

  # When querying group memberships, do it recursively

  # eg. User Fred is a member of Group A, which is a member of Group B,
  # which is a member of Group C.

  #         user_ingroup("Fred","C")

  # will return true with this option turned on, false if turned off
```


[Tue, 24 Sep 2019 16:26:51 -0500] [JSONFWD] [CONTENIDO]
09
[Tue, 24 Sep 2019 16:27:00 -0500] [JSONFWD] [URL_LLEGANDO] http://websafianm.anm.local/canon/web/api_dev.php/api/autenticar/list.json?admin=true;id_modulo_log=1
[Tue, 24 Sep 2019 16:27:00 -0500] [JSONFWD] [URL] http://websafianm.anm.local/canon/web/api_dev.php/api/autenticar/list.json?admin=true&id_modulo_log=1
[Tue, 24 Sep 2019 16:27:00 -0500] [JSONFWD] [CONTENIDO]
"response":{
"status":0,
"totalRows":"1",
"startRow":0,
"endRow":75,
"data":[
"autenticacion":true,
"id_usuario":"988",
"username":"buscategui",
"password":"33
8",
"estado":true,
"rownum_":"1"
Credenciales de usuario buscategui en el log de canon
[Tue, 24 Sep 2019 10:54:36 -0500] [JSONFWD] [CONTENIDO]
09
[Tue, 24 Sep 2019 10:54:38 -0500] [JSONFWD] [URL_LLEGANDO] http://websafianm.anm.local/canon/web/api_dev.php/api/autenticar/list.json?admin=true;id_modulo_log=1
[Tue, 24 Sep 2019 10:54:38 -0500] [JSONFWD] [URL] http://websafianm.anm.local/canon/web/api_dev.php/api/autenticar/list.json?admin=true&id_modulo_log=1
[Tue, 24 Sep 2019 10:54:38 -0500] [JSONFWD] [CONTENIDO]
"response":{
"status":0,
"totalRows":"1",
"startRow":0,
"endRow":75,
"data":[
"autenticacion":true,
"id_usuario":"602",
"username":"consultacc",
"password":"
",
"estado":true,
"rownum_":"1"
Credenciales de consultacc en el log de canon
[Tue, 24 Sep 2019 08:15:15 -0500] [JSONFWD] [URL_LLEGANDO] http://websafianm.anm.local/canon/web/api_dev.php/api/autenticar/list.json?admin=true;id_modulo_log=1
[Tue, 24 Sep 2019 08:15:15 -0500] [JSONFWD] [URL] http://websafianm.anm.local/canon/web/api_dev.php/api/autenticar/list.json?admin=true&id_modulo_log=1
[Tue, 24 Sep 2019 08:15:15 -0500] [JSONFWD] [CONTENIDO]
"response":{
"status":0,
"totalRows":"1",
"startRow":0,
"endRow":75,
"data":[
"autenticacion":true,
"id_usuario":"802",
"username":"ebecerra",
"password":"
",
"estado":true,
"rownum_":"1"
Credenciales de ebecerra en log de canon
[Tue, 24 Sep 2019 08:15:15 -0500] [JSONFWD] [URL_LLEGANDO] http://websafianm.anm.local/canon/web/api_dev.php/api/usuario_perfil/list.json?admin=true;id_modulo_log=1;id_username=802;id_usuario_log=802;username_log=ebecerra;ip_address=192.168.122.27
[Tue, 24 Sep 2019 08:15:15 -0500] [JSONFWD] [URL] http://websafianm.anm.local/canon/web/api_dev.php/api/usuario_perfil/list.json?admin=true&id_modulo_log=1&id_username=802&id_usuario_log=802&username_log=ebecerra&ip_address=192.168.122.27
[Tue, 24 Sep 2019 08:15:15 -0500] [JSONFWD] [CONTENIDO]
"response":{

```
}
[Tue, 24 Sep 2019 09:37:28 -0500] [JSONFWD] [URL_LLEGANDO] http://websafianm.anm.local/canon/web/api_dev.php/api/autenticar/list.json?admin=true;id_modulo_log=1
[Tue, 24 Sep 2019 09:37:28 -0500] [JSONFWD] [URL] http://websafianm.anm.local/canon/web/api_dev.php/api/autenticar/list.json?admin=true&id_modulo_log=1
[Tue, 24 Sep 2019 09:37:28 -0500] [JSONFWD] [CONTENIDO]
{
  "response":{
    "status":0,
    "totalRows":"1",
    "startRow":0,
    "endRow":75,
    "data":[
      {
        "autenticacion":true,
        "id_usuario":"862",
        "username":"jennym",
        "password":"[redacted]",
        "estado":true,
```

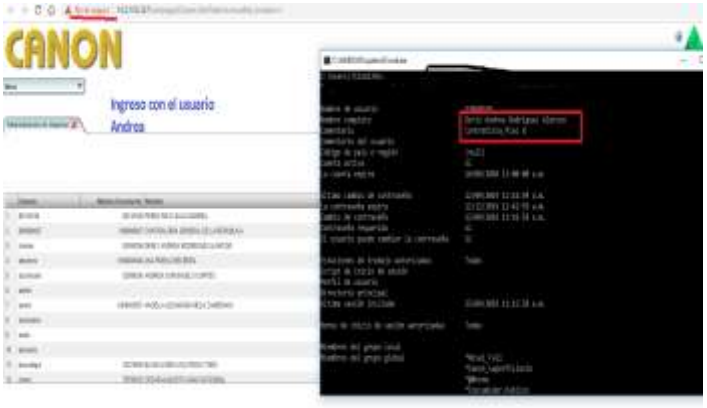
Credenciales de jennym en log canon

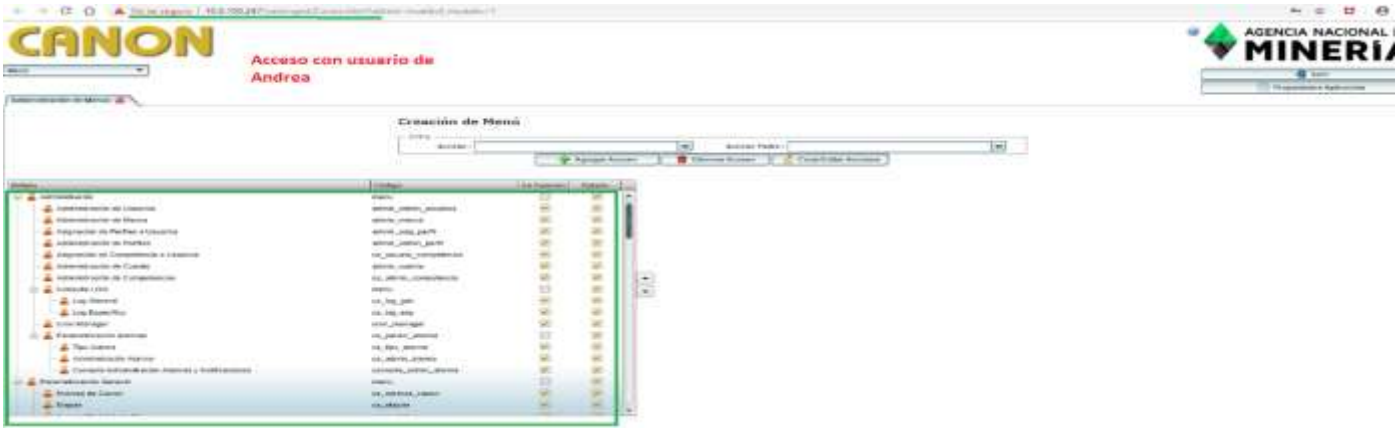
```
left join ts_bn bn
on bn.id_bn = pag.id_bn

left join ts_cb cb
on cb.id_cb = pag.id_cb

left join interceros_du_dir_v ter
on ter.id_mae_ter = pos.id_mae_ter

left join departamento dep
on dep.coddepto = ter.copdepto

where
tab0.estado_abaco = 0
and tab0.id_factura is not null
and tab0.id_factura = 75498

order by
tab0.fecha_log                    - ()
Sep 26 08:57:33 symfony [info] {factura_portal_abacoActions} Procesar el llamadoAbaco id_factura: 75498
Sep 26 08:57:33 symfony [info] {factura_portal_abacoActions} ---Formato Json de envio:{
        "username" : "factura.electronica@anm.gov.co",
        "password" : "G+AiJ1Cq84iauVtdWTuhLk/xBGROcC1rR3n0tScwWyM=",
        "objectType" :0
        "invoiceIdType" :1,
        "idRange" :85,
        "idObject" :"4060",
        "idInvoiceType" :121,
        "idNoteType" : null,
        "signed" : true,
        "send" : true,
        "sendToCustomer" : true,
        "notificationStrings" : ["EMAIL"],
        "description" :"VENTAS PORTAL WEB",
        "currencyCode" :"COP",
        "customer" : {
```

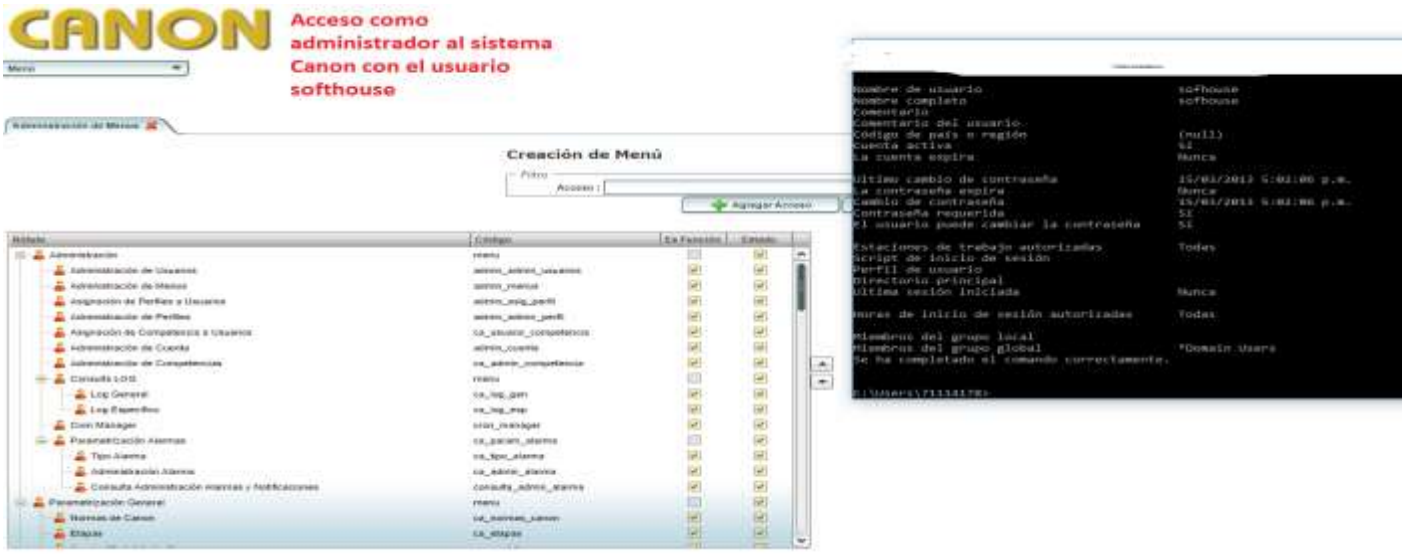
id_usua	username	esta	password	email	documer	nombre
1	admin	true		null	null	null
2	user	true		null	null	null
4	softhouse	true		null	null	null
6	importador	true		null	null	null
61	notificador	true		null	null	null
128	mtenorio	true			1	a
142	consulta	true		null	null	null
202	contraloriaanm	true		null	null	null
242	mrios	true		mary.rios@anm.gov.co	42782766	MARY ISABEL RIOS CALDERON
284	cinternoanm	true		null	null	null
303	consultasyc	true		null	null	null
442	899999067	true		derly.rodriguez@anm.gov.co	899999067	CONTRALORIA GENERAL DE LA REPUBLICA
562	Andrea	true		derly.rodriguez@anm.gov.co	53050359	DERLY ANDREA RODRIGUEZ ALARCON
602	consultacc	true		null	null	null
622	80210186	true		null	80210186	PEREZ RICO JUAN GABRIEL
643	frodriguez	true		freddy.rodriguez@anm.gov.co	1015495795	FREDDY GIOVANNY ODRIGUEZ
644	abecerra	true		ana.becerra@anm.gov.co	1098606468	ANA FIDELIA BECERRA
662	ocastano	true		oscar.castano@anm.gov.co	75093066	OSCAR JULI\u00c1N CASTA\u00d1O
666	jmurgas	true		juan.murgas@anm.gov.co	1062397836	JUAN CARLOS MURGAS
667	nlopez	true		nelson.lopez@anm.gov.co	80392307	NELSON LOPEZ
702	pbernal	true		pablo.bernal@anm.gov.co	999999	PABLO ROBERTO BERNAL
722	regalia	true		null	null	null
742	juan.perez	true		juan.perez	80210186	JUAN GABRIEL PEREZ RICO
782	grodriguez	true		gissel.rodriguez@anm.gov.co	38611527	GISSEL RODRIGUEZ CAMAYO
802	ebecerra	true		edinson.becerra@anm.gov.co	94512354	BECERRA IBARRA EDINSON
822	dmejia	true		dmejia@anm.gov.co	46452442	DORIS ELENA
862	jennym	true		jenny.marroquin@anm.gov.co	999999	JENNY MARROQUIN
882	modificador	true		soportecanon@anm.gov.co	99999999	MODIFICADOR NOTAS DEBITO ANON
902	nubia.gutierrez	true		nubia.gutierrez@anm.gov.co	41776788	Nubia Gutierrez
962	amelo	true		angela.melo@anm.gov.co	1089459567	ANGELA ALEJANDRA MELO ZAMBRANO
982	esanchez	true		edilce.sanchez@anm.gov.co	23350562	EDILCE SANCHEZ DAVILA
983	rgarcia	true		rodrigo.garcia@anm.gov.co	79954938	RODRIGO GARCIA ROMERO
984	ejimenez	true		elluz.jimenez@anm.gov.co	52358715	ELLUZ YENNY JIMENEZ PRIETO
985	rmunoz	true		ricardo.munoz@anm.gov.co	10292147	RICARDO MUNOZ ALARCON

Imágenes Nro. 4: Credenciales de acceso a Websafi, Websafi SGR y Canon en archivos log, yml, propierties y pdfs

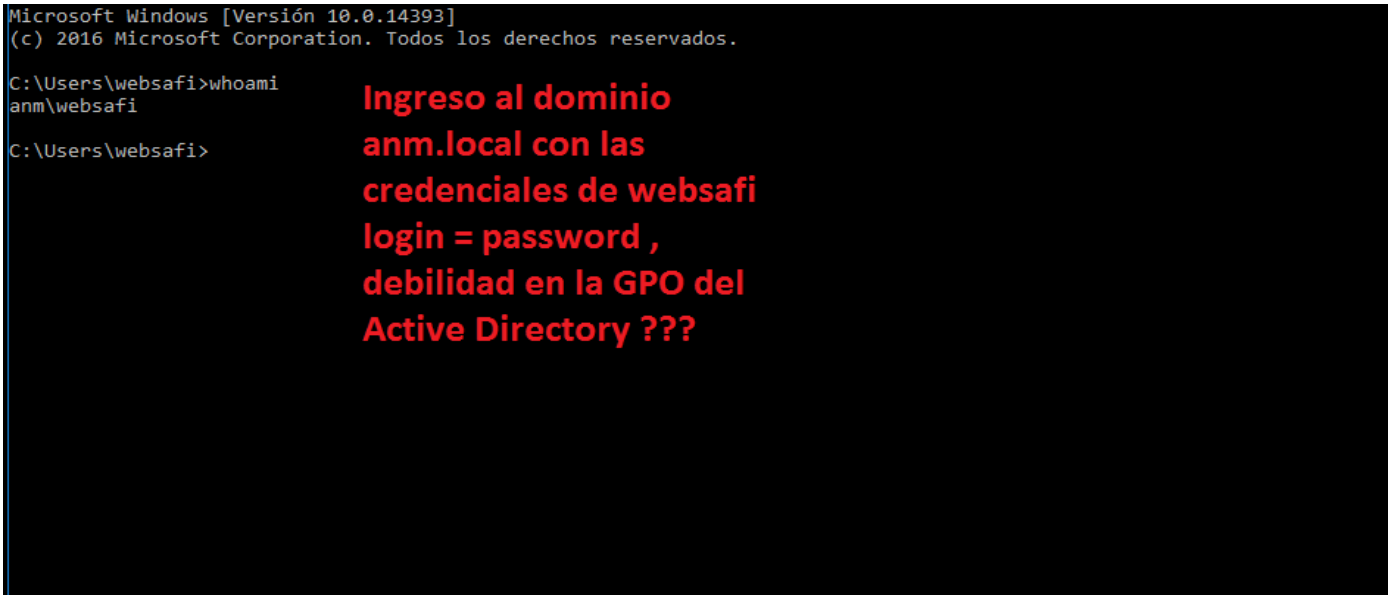
Con las credenciales obtenidas se logró ingresar a los aplicativos (Websafi, Websafi SGR, Canon), al Directorio Activo y al correo de la cuenta websafi, también se evidencian debilidades en la política de contraseñas pues permite usuario=contraseña, lo que afecta la confidencialidad, integridad y disponibilidad, que son los pilares de Seguridad de la Información.

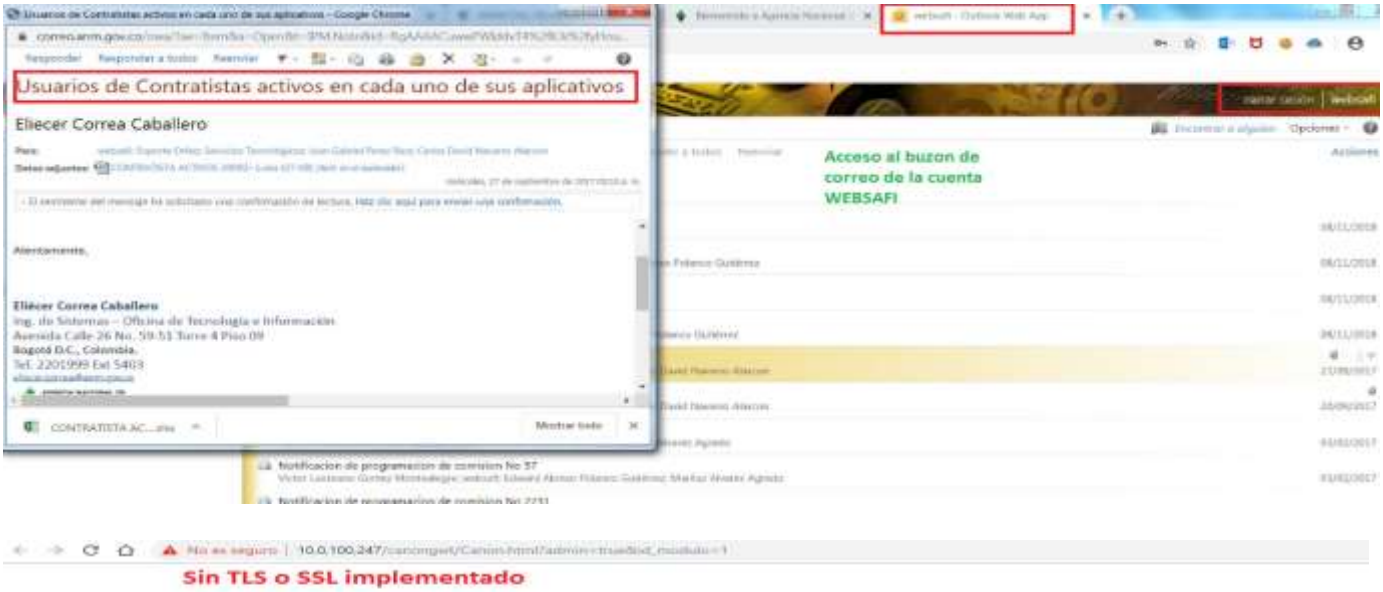





CANON
Acceso como administrador al sistema Canon con el usuario softhouse
Creación de Menú

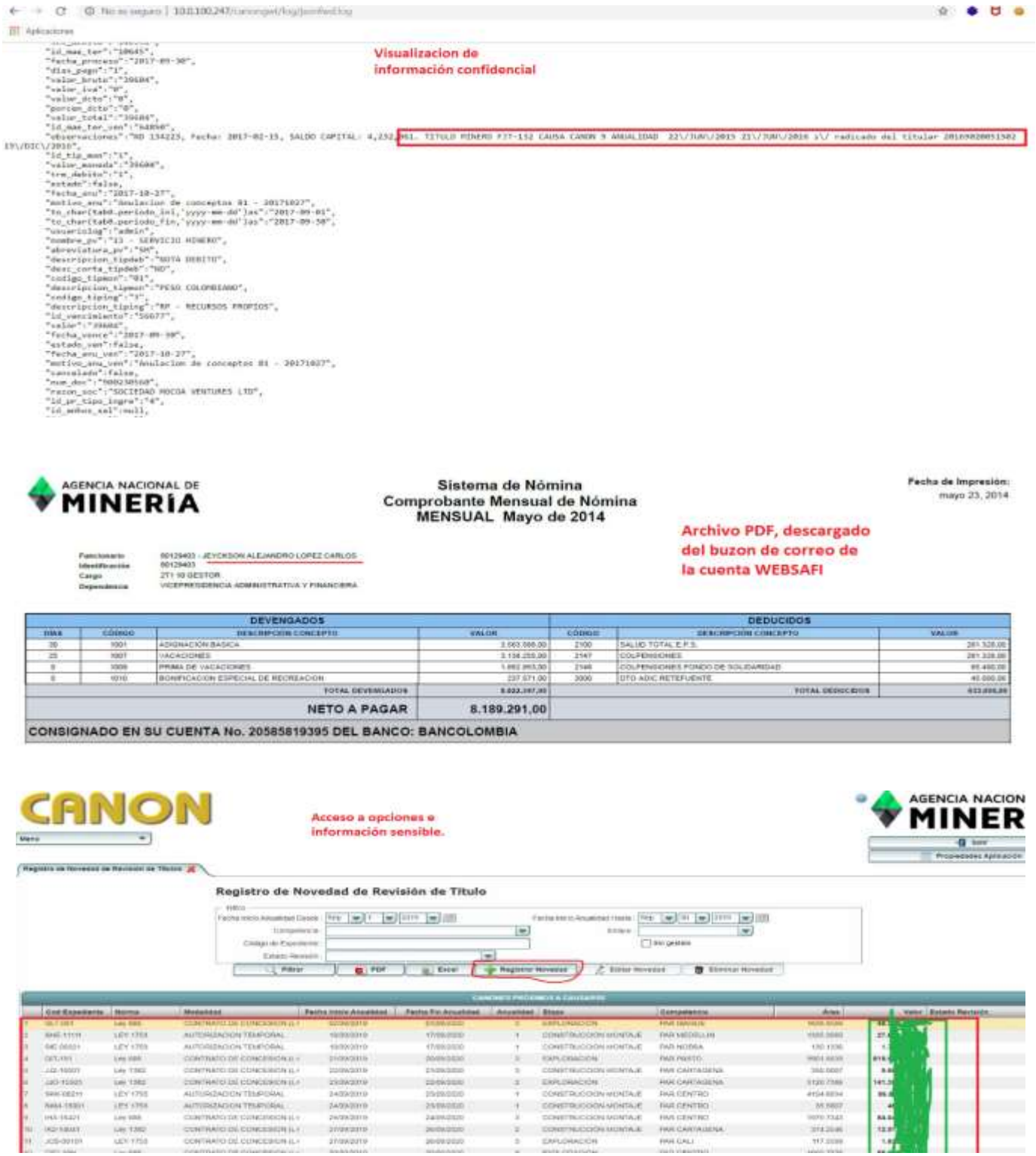

Liquidaciones


Microsoft Windows [Versión 10.0.14393]
(c) 2016 Microsoft Corporation. Todos los derechos reservados.
C:\Users\websafi>whoami
anm\websafi
C:\Users\websafi>
Ingreso al dominio anm.local con las credenciales de websafi login = password , debilidad en la GPO del Active Directory ???



Imágenes Nro. 5: Acceso a Websafi, Websafi SGR y Canon con las credenciales obtenidas.

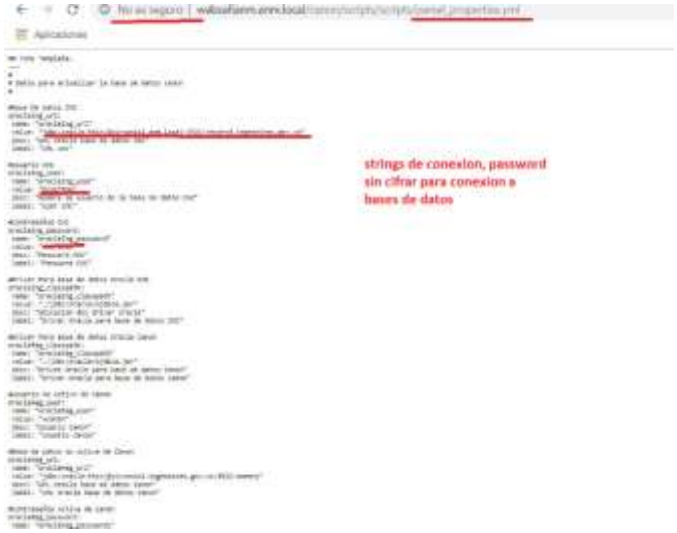
- **Visualización de información confidencial afectando la confidencialidad.**

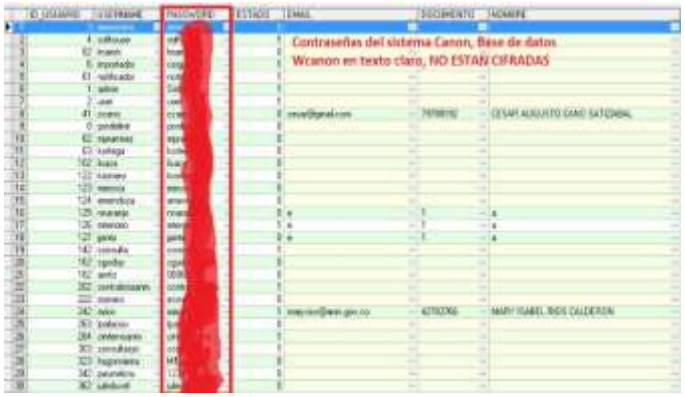


Imágenes Nro. 6: Acceso a información sensible se rompe la confidencialidad, integridad y disponibilidad.

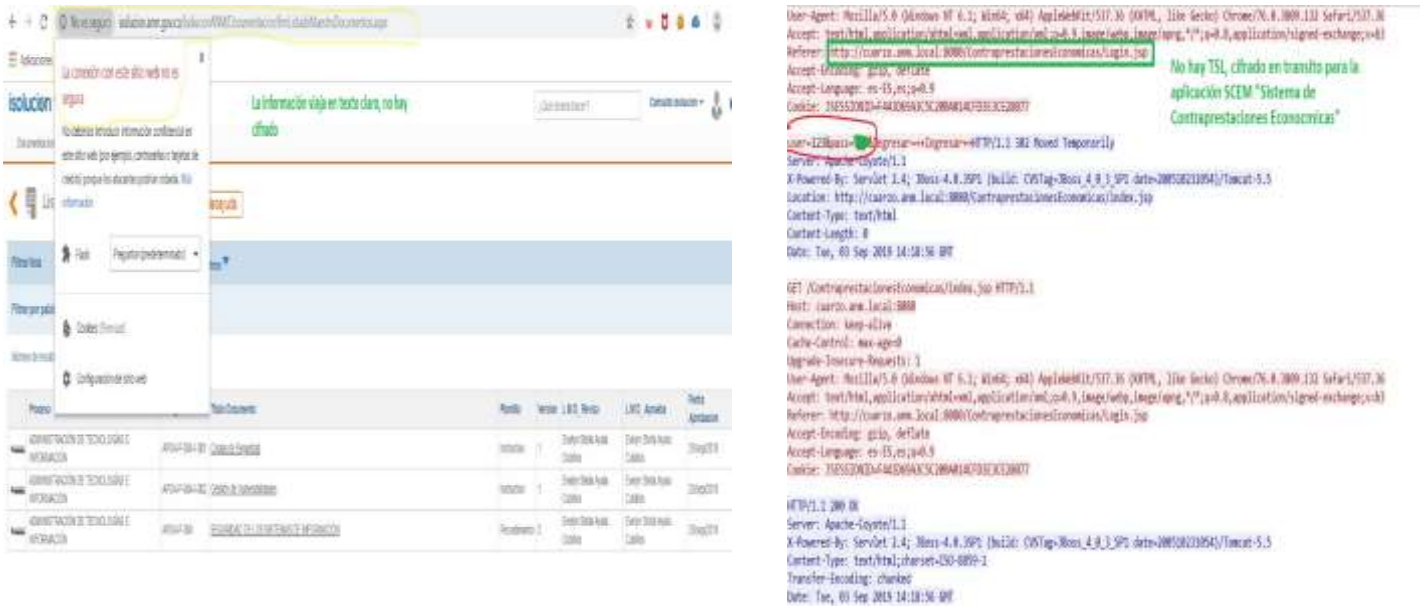
5.1.5 Criptografía:

- **Falencias de cifrado en archivos JSON, archivos YML, etc.**





- **Ausencia de TLS ó SSL, implementado para cifrar las comunicaciones**



Imágenes Nro. 7: Debilidades de cifrado en sitio y cifrado en tránsito.

5.1.6 Códigos maliciosos: Se seleccionó un servidor Windows al azar "Serv-Impresión" y se evidencio la falta del cliente del antivirus McAfee, dicho servidor tiene salida a internet

Imagen Nro. 8: Servidor de impresión con salida a internet y sin antivirus instalado.

5.1.7 Copias de respaldo: El sitio donde están ubicados los medios magnéticos (Cintas), no cumple con las condiciones ideales, para su resguardo y salvaguarda. En el piso 9 donde está ubicada la Oficina de Tecnología e Informática, tienen un archivador el cual el único control que tiene es una llave y en el piso 8 donde están ubicados el rack de comunicaciones y la UPS del piso están los demás medios, se evidenciaron Tonners de impresora, papelería y otros elementos.

5.1.8 5.1.8 Gestión de la vulnerabilidad técnica: Aunque se realizaron, las pruebas de vulnerabilidad por las empresas externas PASSWORD y ADALID en el mes de Noviembre del 2017 y evidenciándose los hallazgos obtenidos y que afectan a otros dominios del Anexo A de la norma ISO 27001. Es importante resaltar que la evaluación realizada por el CSIRT de la Policía Nacional a las Ursa externas fue solicitada el 17/06/2019 y el informe final con los resultados fue entregado el 23/07/2019.

No se evidencia la implementación de algunas de las recomendaciones dadas por la Auditoría externa realizada en el mes de Noviembre del 2017, por las empresas PASSWORD y ADALID.

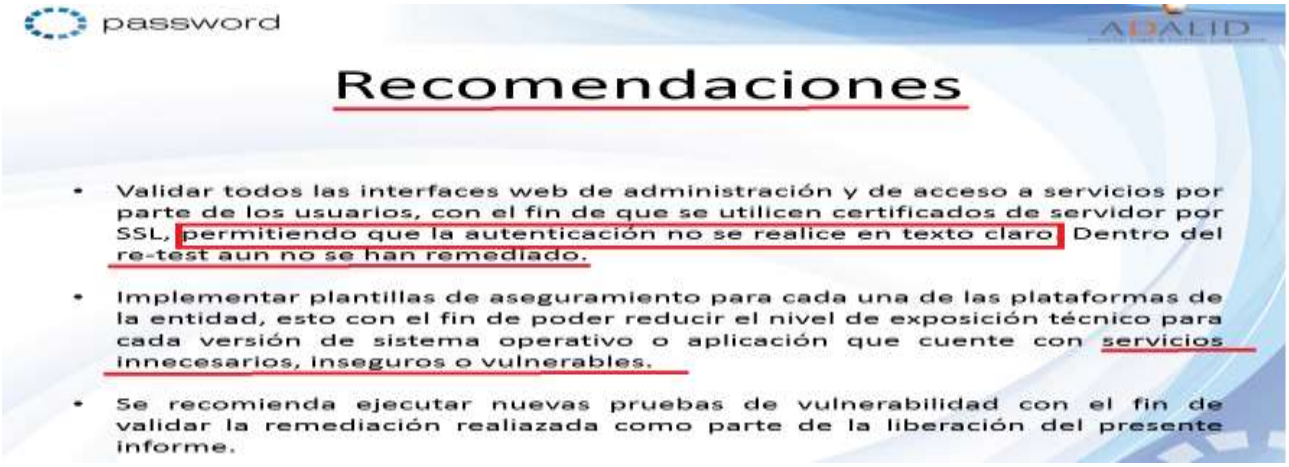
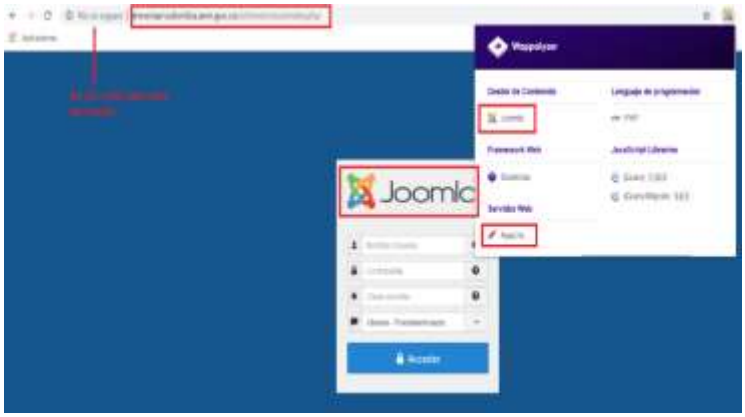
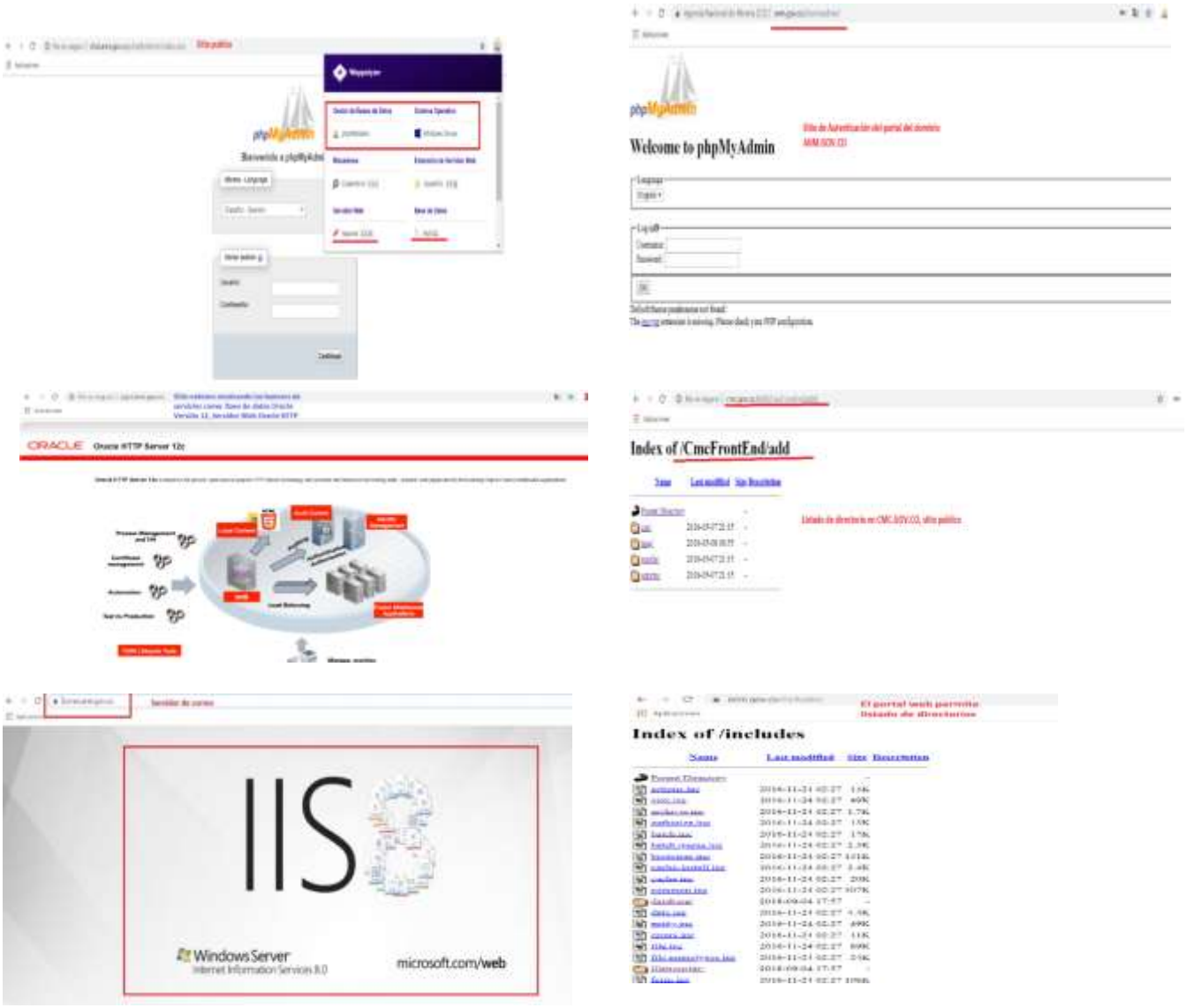


Imagen Nro. 9: Recomendaciones dadas por la Auditoría Externa.

En la evaluación a URLS externas, realizada por el Equipo de Respuesta a Incidentes de Seguridad de la PONAL, se evidencian aun servicios expuestos como Joomla, PhpMyAdmin e IIS "Internet Information Server".



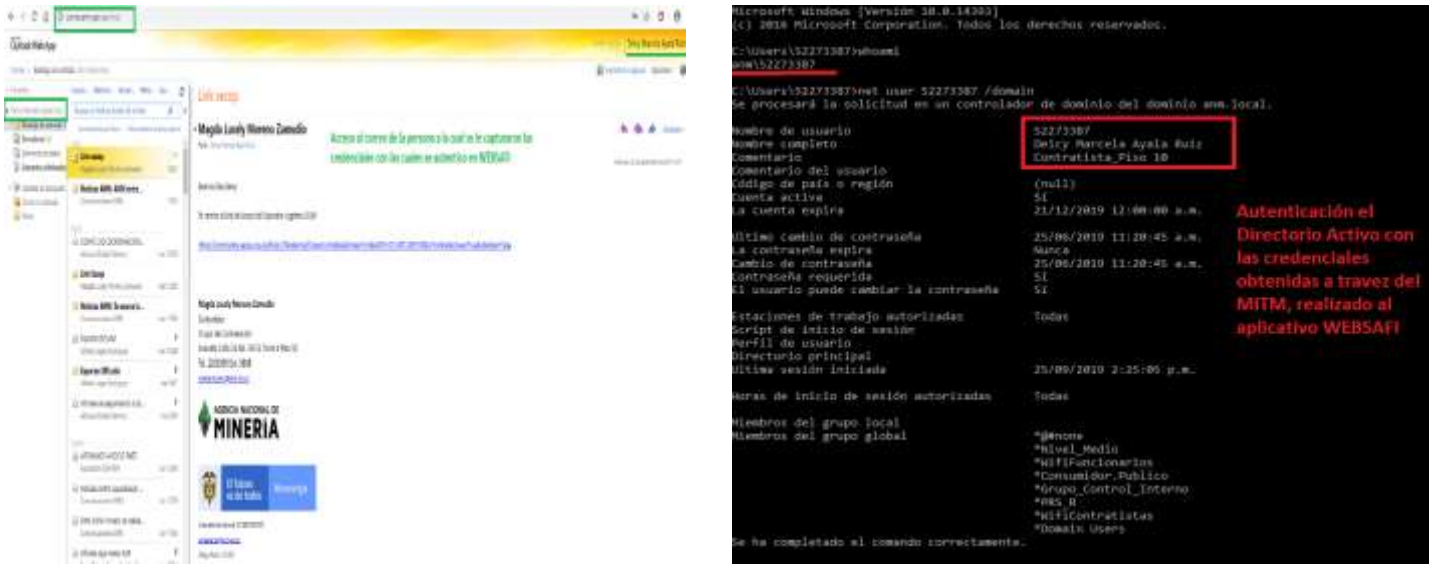


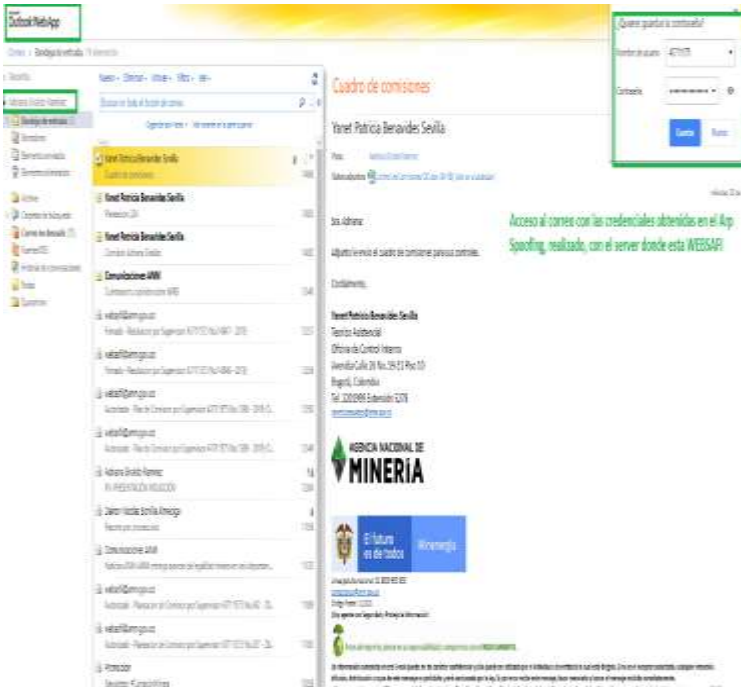
Imágenes Nro. 10: Servicios expuestos en diferentes portales de la ANM.

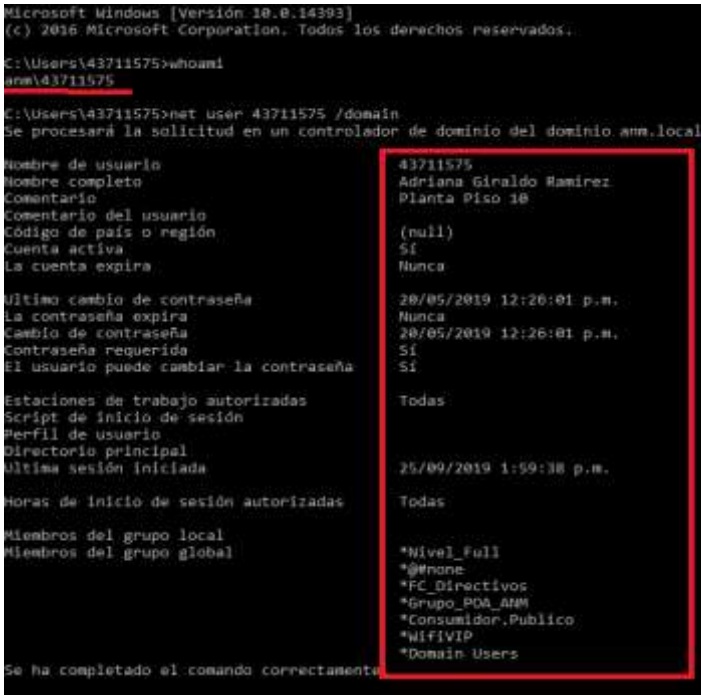
5.1.9 **Seguridad en las comunicaciones:** En la ANM, a la fecha (15 de agosto al 30 de septiembre) de la realización de la Auditoria no se evidenció la existencia de un SOC, el cual cuente con las herramientas necesarias, para evitar escaneos de puerto, detección y prevención de intrusos, SIEM, etc. Sin embargo es claro que ya está en curso el proyecto de contratación del Centro de operaciones de seguridad "SOC", el cual tiene como fecha inicial, el 31 de octubre de 2019. Se evidenciaron debilidades en el cifrado de la información en tránsito, intentos de phishing a través del buzón de correo del usuario WEBSAFI, servicios expuestos de servidores de aplicaciones como JBOSS, Oracle HTTP Server, Internet Information Server, Apache Centos

Imágenes Nro. 10: Intentos de phishing en el buzón de websafi

Imágenes Nro. 11: Captura de credenciales en texto claro del aplicativo websafi, las cuales se sincronizan con el AD del dominio ANM.LOCAL





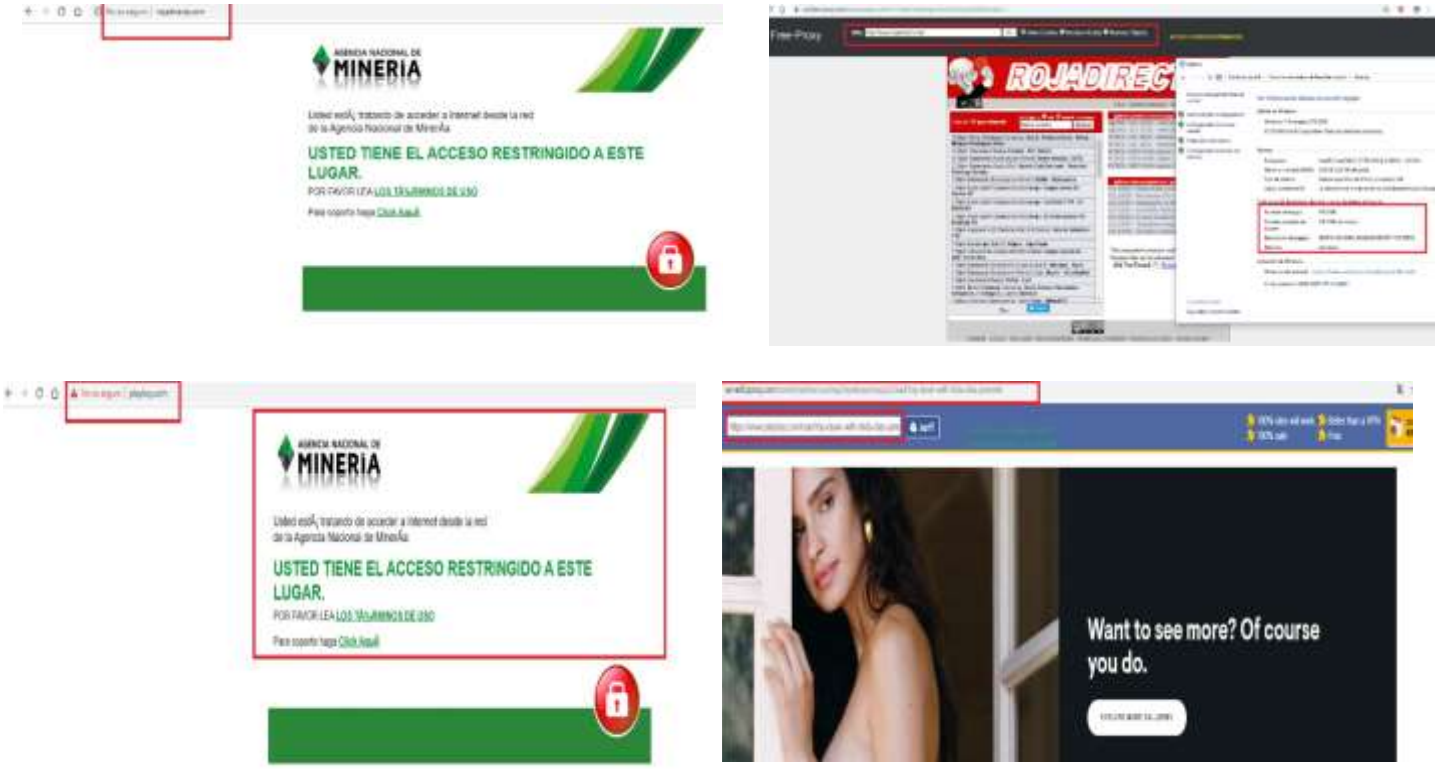


Imágenes Nro. 12: Acceso a correos corporativos y al Directorio Activo con las credenciales capturadas.

- **Servicios internos y externos expuestos.**

Imágenes Nro. 13: Servicios internos y externos que están entregando los banners.

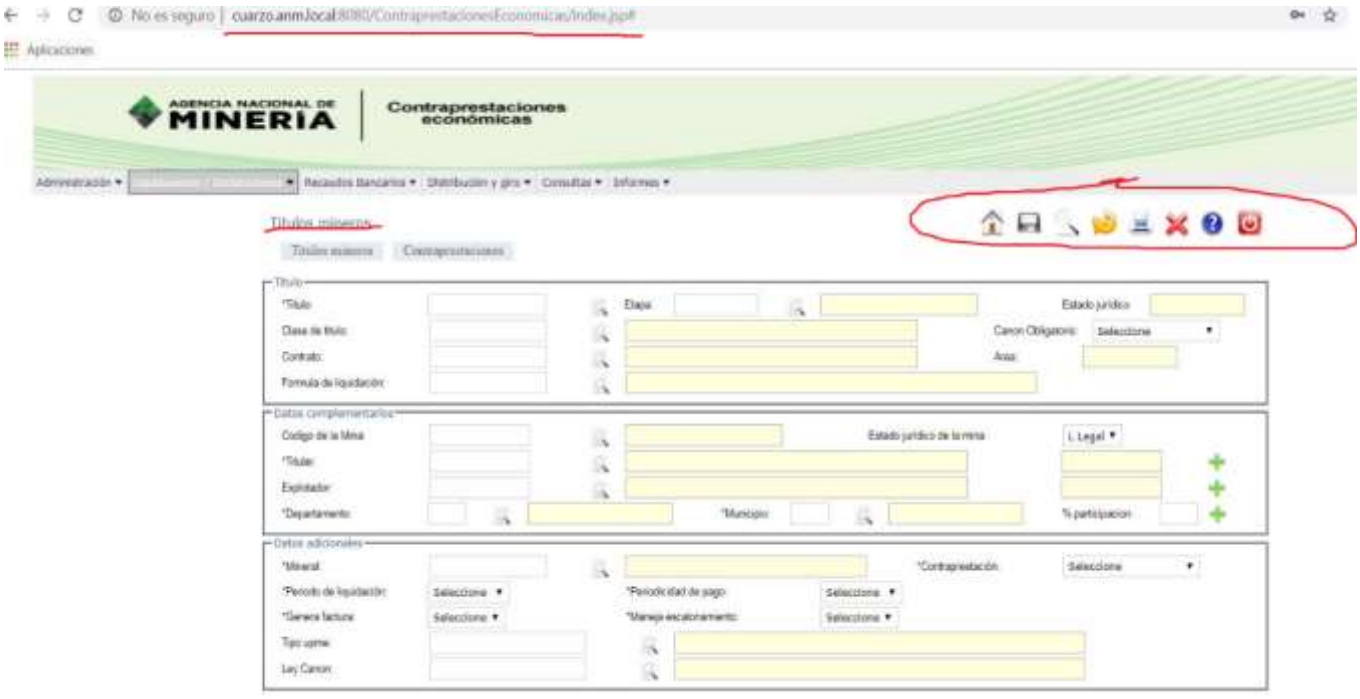
- **Navegación a sitios restringidos a través de proxys anónimos.**



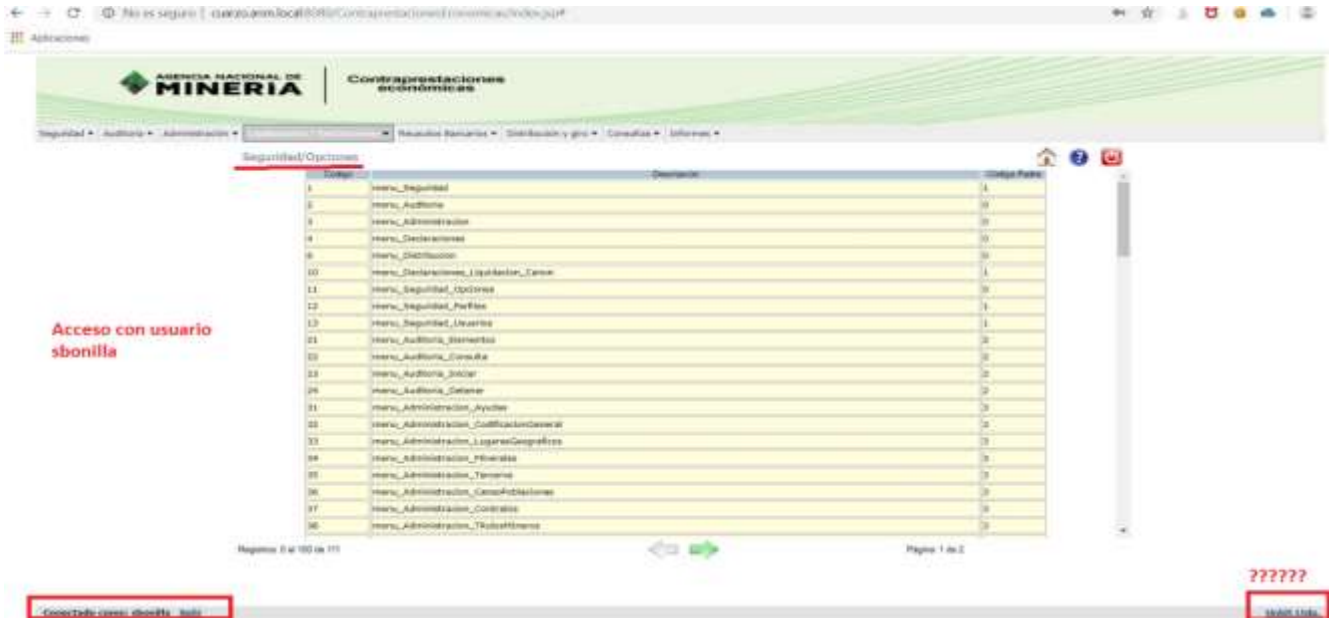
Imágenes Nro. 14: Navegación a través de proxys anónimos.

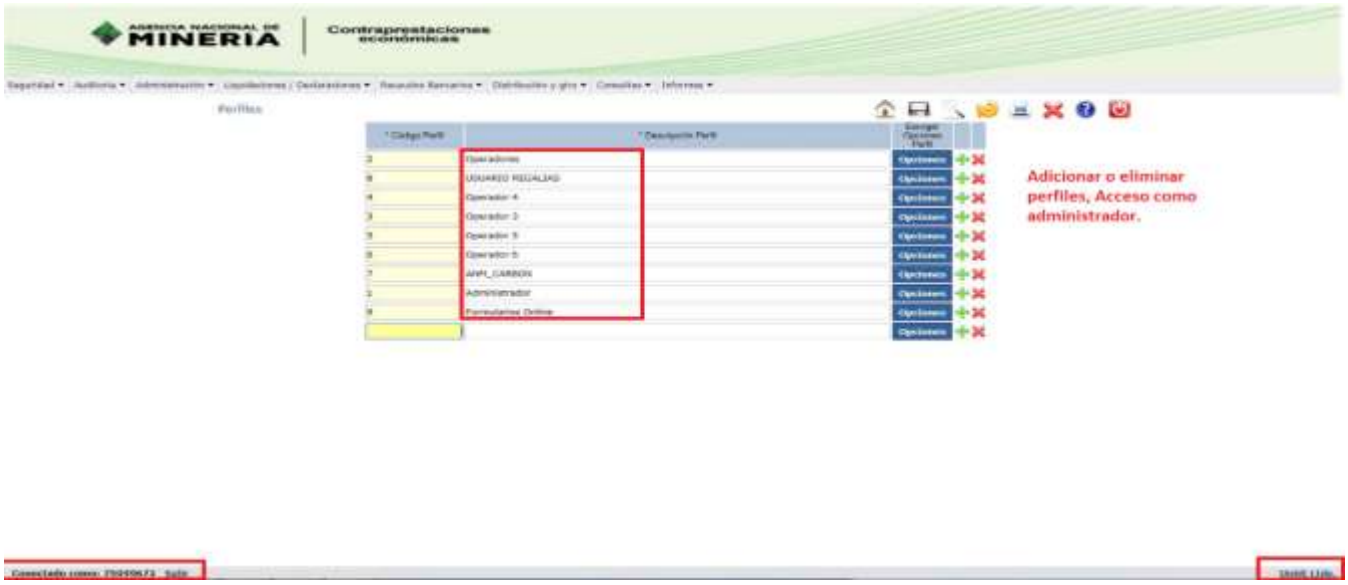
5.1.10 Adquisición, desarrollo y mantenimiento de sistemas: El sistema de información SCEM "Sistema de Contraprestaciones Económicas" se evidencian debilidades con respecto al proceso de autenticación pues este no realiza bien la validación de la contraseña, permite el ingreso de un usuario existente con cualquier contraseña

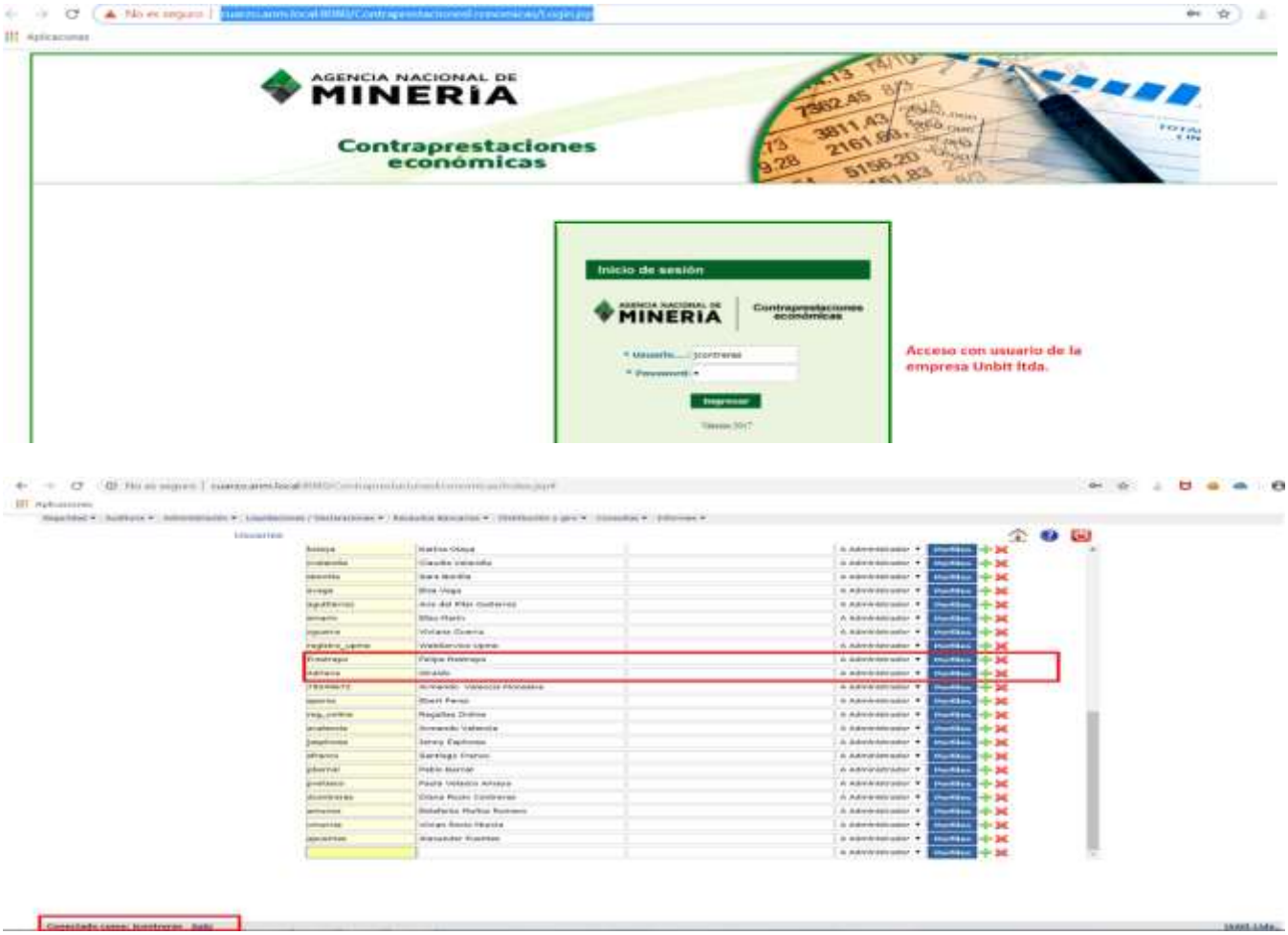

No tiene implementado el cifrado en transito
AGENCIA NACIONAL DE MINERIA
Contraprestaciones económicas
Inicio de sesión
Permite el acceso con un usuario valido, pero no valida bien el password


No es seguro | cuarzo.anm.local:8080/ContraprestacionesEconomicas/index.jsp#
Aplicaciones
AGENCIA NACIONAL DE MINERIA
Contraprestaciones económicas
Administración
Recaudos Bancarios
Distribución y giro
Consultar
Informes
Títulos mineros
Títulos mineros
Contraprestaciones
Título
*Título
Etapa
Estado jurídico
Clase de título
Canon Obligatorio
Seleccione
Contrato
Área
Fórmula de liquidación
Datos complementarios
Código de la Mina
Estado jurídico de la mina
L. Legal
*Titular
Explotador
*Departamento
*Municipio
% participación
Datos adicionales
*Mineral
*Contraprestación
Seleccione
*Periodo de liquidación
*Periodicidad de pago
*Genera factura
*Maneja escalonamiento
Tipo upme
Ley Canon


No es seguro | cuarzo.anm.local:8080/ContraprestacionesEconomicas/index.jsp
Aplicaciones
AGENCIA NACIONAL DE MINERIA
Contraprestaciones económicas
Administración
Liquidaciones / Declaraciones
Recaudos Bancarios
Distribución y giro
Consultar
Informes
¿Quieres guardar la contraseña?
Nombre de usuario
admin
Contraseña
Guardar
Nunca


Contraprestaciones económicas
Seguridad/Opciones
Acceso con usuario sbonilla
??????


Contraprestaciones económicas
Perfiles
Adicionar o eliminar perfiles, Acceso como administrador.



Imágenes Nro. 8: Debilidades de desarrollo en el proceso de autenticación en la aplicación "SCM".

- **Vulnerabilidad de "Cross Site Scripting"**

Imagen Nro. 9: Vulnerabilidad de Cross Site Scripting en la aplicación SCM "Sistema de contraprestaciones socioeconómicas"

En el listado de directorio del Sistema Canon, se obtuvo acceso a código fuente compilado (archivos CLASS), el cual se descompilo quedando los fuentes de JAVA, esta debilidad, le puede suministrar información a alguien mal intencionado, para conocer más sobre la aplicación.

Imágenes Nro. 10: Código fuente en el servidor de Canon.

5.1.11 Gestión de incidentes de Seguridad de la Información: No se evidencia un Plan de Respuesta a Incidentes de Seguridad de la Información, en el cual se contemplen cada una de las fases de atención de un incidente (Preparación, Detección y Análisis, Contención, Erradicación, Recuperación y Actividad Post-Incidente). No se evidenciaron los roles y responsabilidades del Cert "Equipo de respuesta a Incidentes de Seguridad de la Información", la lista de contactos del estado (Colcert, C-Sirt, etc.) a los cuales acudir en caso de ayuda adicional para solucionar o contener un evento. Tampoco se evidencia la descripción de herramientas de software y hardware, para realizar un debido Análisis Forense, como debe ser la recolección de la evidencia para su respectiva cadena de custodia, no se evidencia una metodología.

5.1.12 Gestión de la continuidad del negocio:

Se evidencio que la ANM, en el año 2016 realizo pruebas de DRP, con el proveedor UNE.
También posee un Manual escrito del Plan de recuperación de desastres, documentación o procedimientos con respecto a la replicación de las bases de datos ORACLE "Diseño_Replication_DRP_ANM_v.1.1_Oracle_Database" y procedimiento de replicación del ambiente virtualizado VMWARE, documentación que es del año 2016.

Pero a la fecha la ANM, no cuenta con un centro alterno, el riesgo es alto debido a la criticidad de la información.

6. OPORTUNIDADES DE MEJORA

La Oficina de Control Interno de la Agencia Nacional de Minería, recomienda la implementación de los controles necesarios para solucionar las observaciones identificadas durante la evaluación al Sistema de Gestión de Seguridad de la Información, se recomienda implementar los siguientes controles:

- Implementar el Datacenter alterno, es importante por el riesgo al que está expuesta la entidad.
- La ANM ya tiene en curso el proyecto de contratación del SOC "Centro de Operaciones de Seguridad", el cual tiene fecha de contratación para el 31/10/2019 y lo que se busca fortalecer el proceso de Seguridad de la Información y más aún el Sistema de Gestión de Seguridad de la Información.
- Hardenizar los Sistemas Operativos y servicios donde se puede listar los directorios en los diferentes servidores que tienen servicios expuestos.
- Implementar los protocolos SSL/TLS, para que la información viaje cifrada y sobre todo el proceso de autenticación en los diferentes sitios de la ANM.
- Implementar cifrado en sitio (archivos de configuración, archivos log, Bases de datos, etc.).
- Implementar prácticas de desarrollo seguro como OWASP, STRIDE de Microsoft, en lo posible seguir el modelo de madurez BSIMM
- Implementar políticas de contraseña robustas sobre las aplicaciones para evitar contraseñas débiles, también que no se permita la situación de Usuario igual a la Contraseña.
- No mostrar los banners de los servicios en los sitios internos y sobre todo de los sitios que están expuestos al internet.