MINISTERIO DE ECONOMÍA
GOBIERNO DE
EL SALVADOR
UNÁMONOS PARA CRECER

Informe de Evaluación y Tratamiento de Riesgos

Versión:	1
Fecha :	08-Nov-2014
Creado por:	Ernesto Lizano Mario Pastori Francisco Valiente

Tabla de Contenido

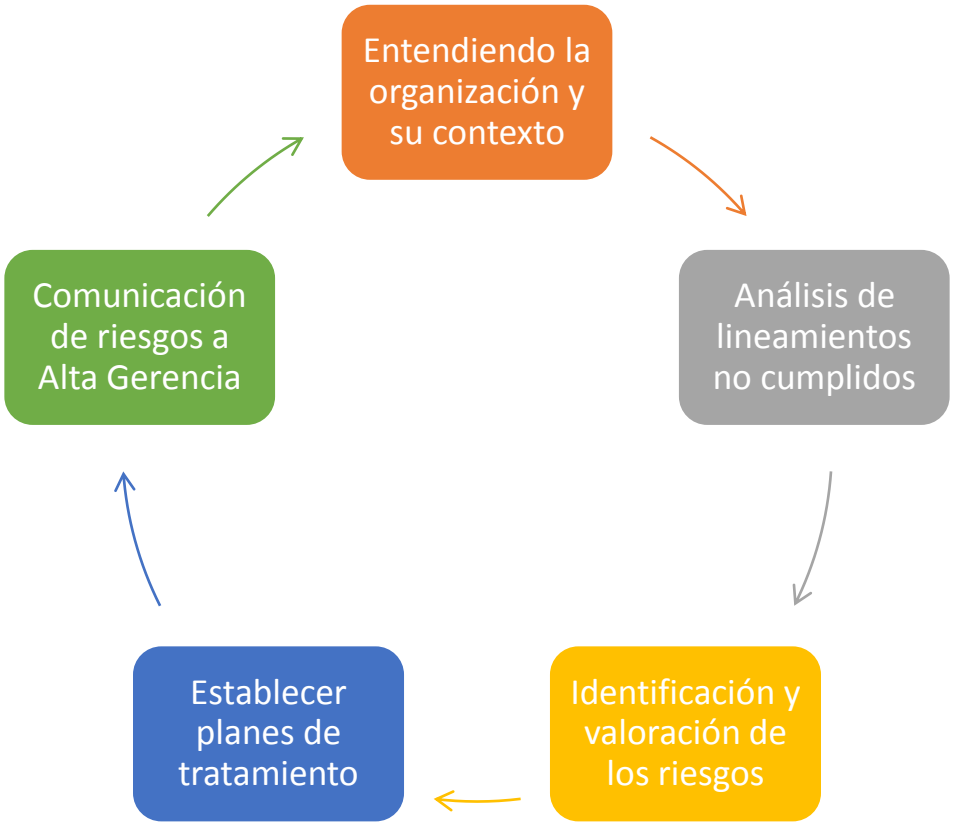
Alcance

Identificación y análisis de Riesgos TI, a los activos de información que sustentan los procesos críticos del Ministerio de Economía.

Objetivos

- Identificar y evaluar los riesgos de TI asociados a los activos de información críticos del MINEC.
- Comunicar a la Alta Gerencia los riesgos identificados.
- Definir planes de tratamiento para los riesgos identificados.

Metodología



Participantes

Los participantes de esta gestión son los empleados del MINEC que participaron en la evaluación y establecimiento de los planes de tratamiento de riesgos, así como también el equipo de consultores que sirvieron de asesores para la gestión de Riesgos.

Proceso Crítico	Gestor	Consultor
Pago al Subsidio del GLP	Mario Hernández	Mario Pastori
Gestión de Tarjeta Solidaria	Jorge Guevara	Mario Pastori
Gestión del Fondo de Desarrollo Productivo	Ernesto Lizano	Francisco Valiente
Regulación de Precios de Combustibles	Mauricio Morales	Francisco Valiente
Acceso a Aplicativos	Ernesto Lizano	Francisco Valiente

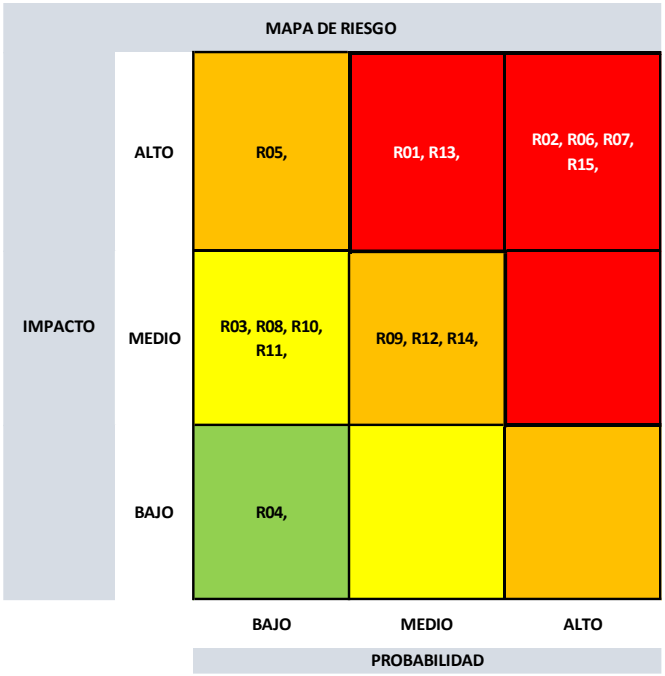
Situación Actual

Por medio del análisis de lineamientos no cumplidos basado en las mejores prácticas (Anexo 1- Cuestionario de Identificación de Riesgos por Proceso Crítico y Anexo 2- Tabulación de Cuestionarios de Identificación de Riesgos por Proceso Crítico), se identificaron y evaluaron riesgos de TI asociados a los activos de información críticos del MINEC (Anexo 3- Matriz de Riesgos).

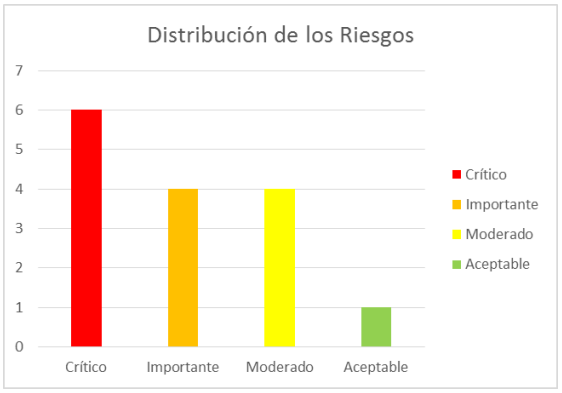
A continuación se presentan el mapa de riesgos y los resultados generales de los riesgos identificados como Críticos e Importantes.

Mapa de Riesgos

De acuerdo al resultado del análisis el Mapa de Riesgos Actual es:



Estando los riesgos distribuidos de la siguiente manera:



Distribución de los Riesgos		
Severidad del Riesgo	**Conteo**	**Porcentaje**
Crítico	6	40%
Importante	4	27%
Moderado	4	27%
Aceptable	1	7%
Grand Total	**15**	**100%**

Resultados Generales sobre los Riesgos Críticos e Importantes

Riesgos Críticos

De acuerdo con la valoración de riesgos, se encontraron riesgos con nivel de severidad Críticos; los cuales se relacionan a continuación:

Riesgo	Vulnerabilidad Identificada	Activo de información
R02	El acceso a los usuarios no es deshabilitado después de varios intentos de ingreso consecutivos fallidos.	• Pago al Subsidio del GLP • Gestión de Tarjeta Solidaria • Gestión del Fondo de Desarrollo Productivo • Regulación de Precios de Combustibles
R06	Información sensible y claves e ID de usuarios se transfieren a través de protocolos inseguros o por canales sin medidas de protección.	• Pago al Subsidio del GLP • Gestión de Tarjeta Solidaria • Acceso a Aplicativos
R07	Información sensible se almacena de forma legible.	• Regulación de Precios de Combustibles
R15	Ausencia de planes de contingencia y/o continuidad.	• Pago al Subsidio del GLP • Gestión de Tarjeta Solidaria • Gestión del Fondo de Desarrollo Productivo • Regulación de Precios de Combustibles • Acceso a Aplicativos
R01	Ausencia de parámetros de contraseñas seguras en los sistemas (Longitud mínima y/o combinaciones de números, letras y caracteres especiales/ cambios periódicos/ historial).	• Gestión del Fondo de Desarrollo Productivo • Regulación de Precios de Combustibles • Acceso a Aplicativos
R13	Ausencia de bitácora o registro de ingreso en el Centro de Datos.	• Pago al Subsidio del GLP • Gestión de Tarjeta Solidaria • Gestión del Fondo de Desarrollo Productivo • Regulación de Precios de Combustibles • Acceso a Aplicativos

Riesgos Importantes

De acuerdo con la valoración de riesgos, se encontraron riesgos con nivel de severidad Importante; los cuales se relacionan a continuación:

Riesgo	Vulnerabilidad Identificada	Activo de información
R05	Ausencia de perfiles de acceso específico que limiten las actividades entre los ambientes de desarrollo, pruebas y producción.	• Regulación de Precios de Combustibles
R09	Ausencia de registro y/o alertas de accesos a datos confidenciales y privilegiados / intentos de acceso fallido al sistema.	• Pago al Subsidio del GLP • Gestión de Tarjeta Solidaria • Gestión del Fondo de Desarrollo Productivo • Regulación de Precios de Combustibles
R12	Credenciales de autenticación quemadas en código fuente de las aplicaciones.	• Gestión del Fondo de Desarrollo Productivo • Regulación de Precios de Combustibles • Acceso a Aplicativos
R14	Ausencia de un proceso de revisión periódico de los registros de acceso y alertas de intento de violación al Centro de Datos.	• Pago al Subsidio del GLP • Gestión de Tarjeta Solidaria • Gestión del Fondo de Desarrollo Productivo • Regulación de Precios de Combustibles • Acceso a Aplicativos

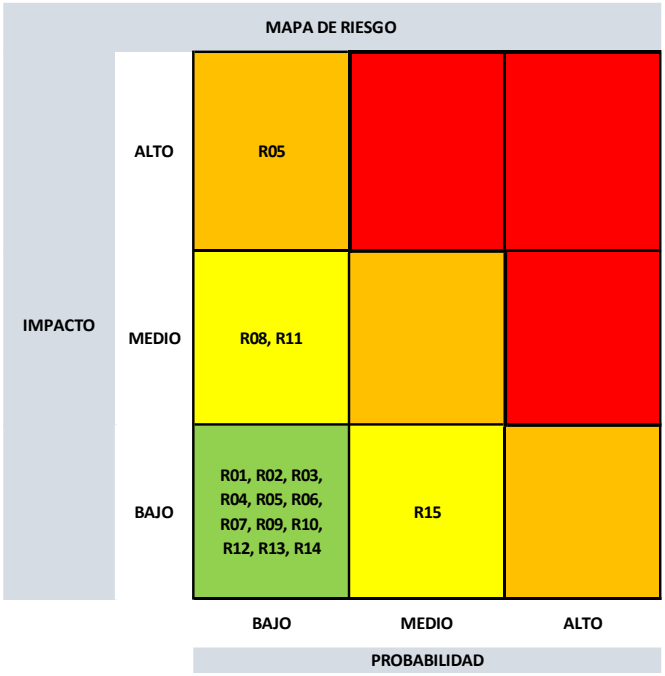
Planes de Tratamiento Propuestos

Por medio del análisis de los resultados de los riesgos de TI identificados y valorados previamente, se determinaron planes de tratamiento encaminados a tratar dichos riesgos (Anexo 3- Matriz de Riesgos).

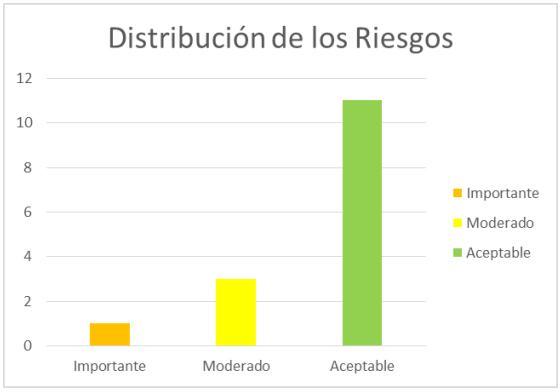
A continuación se presenta el mapa de riesgos esperados una vez sean implementados los planes de tratamiento y los planes de tratamiento sobre los riesgos identificados como Críticos e Importantes.

Mapa de Riesgos

De acuerdo al resultado del análisis el Mapa de Riesgos Actual es:



Estando los riesgos distribuidos de la siguiente manera:



Distribución de los Riesgos		
Severidad Residual	**Conteo**	**Porcentaje**
Importante	1	7%
Moderado	3	20%
Aceptable	11	73%
Grand Total	**15**	**100%**

Planes de Tratamiento

Riesgos Críticos

A continuación se presentas los planes de tratamiento propuestos para mitigar los riesgos considerados Críticos:

Riesgo	Vulnerabilidad Identificada	Plan de Tratamiento	Fecha Propuesta de Cierre
R02	El acceso a los usuarios no es deshabilitado después de varios intentos de ingreso consecutivos fallidos.	Se implementará el bloqueo de las cuentas de usuarios en caso de varios intentos de acceso fallidos al recurso o componente tecnológico.	15-ene-15
R06	Información sensible y claves e ID de usuarios se transfieren a través de protocolos inseguros o por canales sin medidas de protección.	Se implementarán mecanismos para mantener ilegibles las contraseñas e información sensible al momento de transmitirlas, por medio de certificados digitales SSL. Además, se incluirán mecanismos de validación que re direccionen automáticamente las páginas hacia protocolo HTTPS.	04-dic-14
R07	Información sensible se almacena de forma legible.	Se identificará, definirá e implementará medidas de seguridad según la clasificación y valoración de los activos de información. Dentro de estas medidas se considerará: • Procesos de clasificación de información. • Estándar de cifrado. • Cifrado de información (tablas, columnas, según aplique).	04-may-15
R15	Ausencia de planes de contingencia y/o continuidad.	Establecer e implementar planes y procesos de Gestión de continuidad del servicio de IT, que permitan recuperar de manera oportuna los servicios críticos de TI, ante la ocurrencia de una interrupción mayor o desastre; que se minimicen, al máximo, las consecuencias de un desastre o causa de fuerza mayor.	04-may-15
R01	Ausencia de parámetros de contraseñas seguras en los sistemas (Longitud mínima y/o combinaciones	Se implementarán mecanismos que permitan la creación de contraseñas	15-ene-15

Riesgo	Vulnerabilidad Identificada	Plan de Tratamiento	Fecha Propuesta de Cierre
	de números, letras y caracteres especiales/ cambios periódicos/ historial).	seguras y que cumplan con las siguientes características: • Longitud mínima de la contraseña. • Uso de caracteres alfanuméricos que incluyan mayúsculas, minúsculas, números y caracteres especiales. • La contraseña no podrá ser igual a ninguna de las utilizadas recientemente.	
R13	Ausencia de bitácora o registro de ingreso en el Centro de Datos.	Se definirá e implementará un procedimiento de control de acceso físico que incluya al menos: solicitud, niveles de autorización de acceso, personas que otorgan la autorización, acceso en caso de emergencia, eliminación de accesos. Además, se contará con una bitácora física de todos los accesos al Centro de Datos, que deberá ser firmada cada vez que ingrese cualquier persona fuera del grupo autorizado de la Gerencia de Informática.	04-dic-15

Riesgos Importantes

A continuación se presentas los planes de tratamiento propuestos para mitigar los riesgos considerados Importantes:

Riesgo	Vulnerabilidad Identificada	Plan de Tratamiento	Fecha Propuesta de Cierre
R05	Ausencia de perfiles de acceso específico que limiten las actividades entre los ambientes de desarrollo, pruebas y producción.	Aceptar temporalmente el Riesgo.	N/A
R09	Ausencia de registro y/o alertas de accesos a datos confidenciales y privilegiados / intentos de acceso fallido al sistema.	Se implementarán mecanismos para registrar y alertar sobre: • Accesos a datos confidenciales y privilegiados. • Intentos de acceso fallido al sistema.	04-may-15
R12	Credenciales de autenticación quemadas en código fuente de las aplicaciones.	Se implementarán mecanismos para cifrar el string de conexión contenido en el archivo de configuración de las aplicaciones.	15-ene-15
R14	Ausencia de un proceso de revisión periódico de los registros de acceso y alertas de intento de violación al Centro de Datos.	Se realizará revisión periódica de los registros o log de ingreso, derechos de acceso a las instalaciones y revocar los accesos cuando sea necesario.	04-dic-14

Anexos

Anexo 1- Cuestionario de Identificación de Riesgos por Proceso Crítico

Cuestionario de Identificación de Riesgos: Proceso Crítico del Negocio "Pago al Subsidio del GLP"

Completado por:	**Mario Hernández**
Fecha:	**11/3/2014**

1. *Análisis de Riesgos y Clasificación de Información*

#	Preguntas	Respuesta
1.1	¿Existe definido un responsable (colaborador, área, gerencia, dirección, entre otros) de la información de los sistemas?	SI
1.2	¿Existe definido un administrador (ej. colaborador, área, gerencia, dirección, entre otros) de los sistemas?	SI
1.3	¿La información de los sistemas fue identificada y clasificada por su responsable (dueño), teniendo en cuenta su criticidad?	SI

2. *Identificación y Autenticación*

#	Preguntas	Respuesta
2.1	¿Todos los usuarios son identificados en los sistemas mediante una única cuenta de acceso y al menos un método de autenticación?	SI
2.2	¿Los sistemas restringen que la contraseña esté conformada por mínimo 8 caracteres con combinaciones de números, letras y caracteres especiales?	SI
2.3	¿El acceso de los usuarios es bloqueado después de máximo 5 intentos de ingreso consecutivos fallidos?	NO
2.4	¿Los sistemas solicitan el cambio periódico de contraseña, máximo cada 90 días?	SI
2.5	¿Las cuentas de usuario que sobrepasen el período de 90 días de inactividad son bloqueadas de manera preventiva por los sistemas?	SI
2.6	¿Los sistemas informan al menos con 15 días de anticipación el vencimiento de la contraseña?	NO
2.7	¿Los sistemas almacenan historial de contraseñas (al menos 10)?	SI
2.8	¿Los sistemas solicitan el cambio obligatorio de la contraseña en el primer uso de la cuenta o cuando ha sido restablecida?	SI
2.9	¿La sesión de usuario dentro de los sistemas es cerrada de forma automática, después de 15 minutos de inactividad?	SI
2.10	Los sistemas cuentan con un módulo de administración de seguridad que permite al menos: - La creación, modificación, desactivación y eliminación de usuarios. - La administración de parámetros de seguridad. - La generación de reportes (usuarios, perfiles, etc.).	SI

3. Autorización y Controles de Acceso

#	Preguntas	Respuesta
3.1	¿Los sistemas permiten establecer roles o niveles de acceso de acuerdo a las actividades, responsabilidades y necesidades de cada usuario?	SI
3.2	¿El personal que realiza funciones asociadas a un ambiente específico del sistema (desarrollo, pruebas o producción), cuenta con un perfil de acceso que limita sus actividades exclusivamente a este ambiente?	SI
3.3	¿Las cuentas de usuario con perfil de administración únicamente son utilizadas para labores administrativas?	N/A
3.4	¿Los sistemas cuentan con la capacidad de controlar el acceso de los usuarios a sus diferentes módulos y funciones?	SI

4. Protección de los Datos

#	Preguntas	Respuesta
4.1	¿La información de ingreso a los sistemas (*usuario y contraseña*) se mantiene ilegible al momento de *transmitirla*? *(ej. SSL, IPSEC, VPN, cifrado de datos, etc.)*	NO
4.2	¿El *intercambio de archivos* con información *confidencial* o *sensible*, se realiza utilizando protocolos seguros (FTPS, SFTP) o mediante el cifrado de los datos?	SI
4.3	Si los sistemas tienen arquitectura Web y están expuestos a Internet, ¿se implementan protocolos seguros (ej. HTTPS con su respectivo certificado) para proteger la información transmitida?	NO
4.4	¿Las *contraseñas* de todas las cuentas de los sistemas se *almacenan ilegibles* (cifrado con algoritmos fuertes, truncamiento, hash, etc.)? *(ej. 3DES, AES, SHA, etc.)*	SI
4.5	¿La información *confidencial o sensible* de los sistemas (incluyendo la que se almacena en las copias de respaldo) se *almacena ilegible*?*(ej. 3DES, AES, SHA, etc.)*	SI
4.6	Si los sistemas procesan, transmiten o almacenan información de tarjetas de pago (crédito, débito) ¿se ha definido o contemplado definir un proceso de gestión de las llaves criptográficas usadas para el cifrado de la información de los sistemas?	N/A
4.7	¿La información *confidencial o sensible* del ambiente productivo se utiliza para actividades de desarrollo o pruebas, sin pasar por un proceso de despersonalización o enmascaramiento?	SI

5. Alertas/Eventos

#	Preguntas	Respuesta
5.1	¿Los sistemas y los componentes tecnológicos que lo soportan (servidores, bases de datos, etc.) están en capacidad de registrar, alertar y almacenar los eventos que afecten la seguridad de la información?	SI
5.2	¿Cuáles de los siguientes eventos se ha considerado registrar en los sistemas o en los componentes tecnológicos que lo soportan?	

5.2.1	Accesos a información clasificada como *confidencial y privilegiada* de la compañía.	SI
5.2.2	Acciones realizadas con privilegios especiales (administradores, superusuarios, etc.)	SI
5.2.3	Intentos de acceso a los sistemas (exitosos y fallidos).	NO
5.2.4	Creación, modificación, eliminación, desactivación, bloqueo y desbloqueo de usuarios.	SI
5.2.5	Cambios en la configuración de seguridad en sistemas, bases de datos, equipos de comunicación, etc.	SI
5.3	¿Qué información se incluye en los registros de eventos de seguridad?	
5.3.1	Fecha y hora del evento.	SI
5.3.2	Identificación del usuario que lo realiza.	SI
5.3.3	Tipo de evento.	SI
5.3.4	Descripción del evento. (Detalle del evento, acción ejecutada, éxito o fracaso de la operación, etc.).	SI
5.3.5	Componente del sistema o recurso afectado.	SI
5.3.6	Identificación del equipo desde el cual se realizó la operación (ej. dirección IP, dirección MAC, nombre del equipo, etc.).	SI
5.4	¿Se ha considerado implementar mecanismos de seguridad para evitar que los registros de eventos (logs) sean modificados (ej. a través de control de acceso, segregación de redes, etc.)?	SI
5.5	¿La fecha y la hora de los sistemas y los componentes que lo soportan se encuentran sincronizados con un servicio de sincronización de relojes?	SI

6. Gestión de Vulnerabilidades

#	Preguntas	Respuesta
6.1	¿Se ha contemplado la ejecución de pruebas de vulnerabilidades y/o intrusión a los sistemas y los componentes que lo soportan (servidores, bases de datos, equipos de comunicaciones, etc.)?	SI
6.1.1	¿Se ha contemplado establecer planes de acción encaminados a resolver las vulnerabilidades encontradas?	SI
6.2	¿Las plataformas que soportan los sistemas se encuentran aseguradas de tal forma que sólo ejecute los servicios requeridos por los sistemas?	SI

7. Desarrollo Seguro de Sistemas

#	Preguntas	Respuesta
7.1	¿Se consideran prácticas de desarrollo seguro de aplicaciones y establecimiento de pruebas técnicas, funcionales y de seguridad del sistema?	SI
7.2	¿Los sistemas cuentan con ambientes de desarrollo, pruebas y producción?	NO
7.3	¿Los sistemas realizan validación de datos de entrada (ej. tipos de datos esperados, longitudes de datos esperados, tipos de caracteres esperados, etc.)?	SI

7.4	¿La información de autenticación (usuarios y contraseñas) y/o direcciones IP se encuentran en *texto claro,* "quemadas" en el código fuente del sistema o en un archivo de configuración sin cifrar?	NO
7.5	En el caso que algún sistema ha sido suministrado o desarrollado por un tercero, ¿se tiene contemplado realizar actualizaciones periódicas del software con el fin de garantizar la funcionalidad y seguridad del mismo?	N/A

8. Seguridad en Redes

#	Preguntas	Respuesta
8.1	¿Los sistemas interactúan con otros *sistemas* o *componentes tecnológicos* diferentes a los que lo soportan (ej. servicios, bases de datos, servidores, etc.)?	SI
8.2	¿El sistema interactúa con *sistemas* o *componentes tecnológicos* ubicados en redes externas a las de la Organización (ej. proveedores, entes reguladores, aliados, etc.)?	SI
8.3	¿Se cuenta con algún mecanismo de seguridad a nivel de red para la protección de la información que se intercambia con estos *sistemas* o *componentes tecnológicos* externos (SSL, IPSEC, etc.)?	SI
8.4	¿Las conexiones desde y hacia la red donde se encuentran los sistemas o los componentes tecnológicos son controladas por dispositivos de seguridad tipo *firewall*?	SI
8.5	¿Los *componentes de almacenamiento de datos* (ej. Bases de datos) del sistema se encuentran ubicados en un segmento seguro de la red y no en zonas catalogadas como no seguras (ej. DMZ)?	SI
8.6	¿Existen sistemas de prevención y/o detección de intrusos ubicados en la red donde se encuentra el sistema y los componentes tecnológicos que lo soportan?	SI

9. Seguridad Física

#	Preguntas	Respuesta
9.1	¿El centro de procesamiento de información (centro de datos) cuenta con controles de acceso físico (ej. exclusas, tarjetas de proximidad, biométricos, chapa convencional con llave, etc.)?	SI
9.2	¿El centro de procesamiento de información (centro de datos) cuenta con controles ambientales (ej. aire acondicionado, detectores de incendio e inundación, extintores, etc.)?	SI
9.3	¿El centro de procesamiento de información (centro de datos) cuenta con circuitos alternos y equipo de respaldo para suministro de energía?	SI
9.4	¿Existe una bitácora o registro de acceso al centro de procesamiento de información (centro de datos) mantenida al menos por (3) tres meses?	NO
9.5	¿Se cuenta con un proceso de revisión periódico de los registros de acceso y alertas de intento de violación al centro de procesamiento de información (centro de cómputo)?	NO

10. Continuidad del Negocio

#	Preguntas	Respuesta
10.1	Los sistemas y los componentes tecnológicos que lo soportan se encuentran dentro del alcance del *plan de continuidad de negocio de la organización*?	NO
10.2	En caso de no existir un plan de continuidad en la organización, ¿existen planes documentados de contingencia y/o recuperación de los sistemas y los componentes que lo soportan?	SI
10.3	¿Se ha considerado la implementación de procedimientos periódicos de copia de respaldo de la información de los sistemas?	SI
10.3.1	¿Los medios de almacenamiento para copias de respaldo (back ups) han sido dimensionados de acuerdo con las necesidades de los sistemas y cubren el tiempo de retención de información definido?	SI
10.4	¿Las copias de respaldo de la información de los sistemas cuentan con mecanismos de almacenamiento y custodia externa?	SI

11. No Repudio

#	Preguntas	Respuesta
11.1	¿El sistema realiza transacciones electrónicas (ej. redención de pago subsidio, etc.)?	SI
11.2	El sistema cuenta con mecanismos para registrar la información necesaria para certificar las transacciones electrónicas realizadas en sus diferentes etapas: - Requerimiento del servicio (Origen del requerimiento, Dirección IP del origen). - Resultado de la transacción (Aprobación o rechazo). - Evidencia de la transferencia y almacenamiento de información. - Evidencia de la verificación.	SI
11.3	¿La información de las transacciones rechazadas es almacenada con el fin de verificar posteriormente si la transacción concluyó consistentemente en todos los sistemas que involucró?	SI

12. Contratación, Licenciamiento y Documentación

#	Preguntas	Respuesta
12.1	¿El sistema o algunos de los componentes que lo soportan (frameworks, código fuente, aplicaciones de soporte, etc.) requieren licenciamiento para su uso (comercial, open source, etc.)?	SI
12.1.1	¿Todas las licencias cuentan con los respectivos soportes (documento físico o electrónico de condiciones de licenciamiento, factura de compra, contrato de adquisición, etc.)?	SI
12.1.2	¿Los medios originales de instalación, manuales y documentos de licencia de uso del sistema o los componentes que lo soportan, son inventariados y conservados por el área responsable en un lugar seguro y designado específicamente para este fin?	SI

12.3	¿Se cuenta con manuales de instalación, configuración, administración, operación y usuario final formalmente documentados?	SI

Cuestionario de Identificación de Riesgos: Proceso Crítico del Negocio "Gestión de Tarjeta Solidaria"

Completado por:	**Jorge Guevara**
Fecha:	**11/3/2014**

1. *Análisis de Riesgos y Clasificación de Información*

#	Preguntas	Respuesta
1.1	¿Existe definido un responsable (colaborador, área, gerencia, dirección, entre otros) de la información de los sistemas?	SI
1.2	¿Existe definido un administrador (ej. colaborador, área, gerencia, dirección, entre otros) de los sistemas?	SI
1.3	¿La información de los sistemas fue identificada y clasificada por su responsable (dueño), teniendo en cuenta su criticidad?	SI

2. *Identificación y Autenticación*

#	Preguntas	Respuesta
2.1	¿Todos los usuarios son identificados en los sistemas mediante una única cuenta de acceso y al menos un método de autenticación?	SI
2.2	¿Los sistemas restringen que la contraseña esté conformada por mínimo 8 caracteres con combinaciones de números, letras y caracteres especiales?	SI
2.3	¿El acceso de los usuarios es bloqueado después de máximo 5 intentos de ingreso consecutivos fallidos?	NO
2.4	¿Los sistemas solicitan el cambio periódico de contraseña, máximo cada 90 días?	SI
2.5	¿Las cuentas de usuario que sobrepasen el período de 90 días de inactividad son bloqueadas de manera preventiva por los sistemas?	SI
2.6	¿Los sistemas informan al menos con 15 días de anticipación el vencimiento de la contraseña?	NO
2.7	¿Los sistemas almacenan historial de contraseñas (al menos 10)?	SI
2.8	¿Los sistemas solicitan el cambio obligatorio de la contraseña en el primer uso de la cuenta o cuando ha sido restablecida?	SI
2.9	¿La sesión de usuario dentro de los sistemas es cerrada de forma automática, después de 15 minutos de inactividad?	SI

2.10	Los sistemas cuentan con un módulo de administración de seguridad que permite al menos: - La creación, modificación, desactivación y eliminación de usuarios. - La administración de parámetros de seguridad. - La generación de reportes (usuarios, perfiles, etc.).	SI

3. Autorización y Controles de Acceso

#	Preguntas	Respuesta
3.1	¿Los sistemas permiten establecer roles o niveles de acceso de acuerdo a las actividades, responsabilidades y necesidades de cada usuario?	SI
3.2	¿El personal que realiza funciones asociadas a un ambiente específico del sistema (desarrollo, pruebas o producción), cuenta con un perfil de acceso que limita sus actividades exclusivamente a este ambiente?	SI
3.3	¿Las cuentas de usuario con perfil de administración únicamente son utilizadas para labores administrativas?	N/A
3.4	¿Los sistemas cuentan con la capacidad de controlar el acceso de los usuarios a sus diferentes módulos y funciones?	SI

4. Protección de los Datos

#	Preguntas	Respuesta
4.1	¿La información de ingreso a los sistemas (*usuario y contraseña*) se mantiene ilegible al momento de *transmitirla*? *(ej. SSL, IPSEC, VPN, cifrado de datos, etc.)*	NO
4.2	¿El *intercambio de archivos* con información *confidencial* o *sensible*, se realiza utilizando protocolos seguros (FTPS, SFTP) o mediante el cifrado de los datos?	N/A
4.3	Si los sistemas tienen arquitectura Web y están expuestos a Internet, ¿se implementan protocolos seguros (ej. HTTPS con su respectivo certificado) para proteger la información transmitida?	NO
4.4	¿Las *contraseñas* de todas las cuentas de los sistemas se *almacenan ilegibles* (cifrado con algoritmos fuertes, truncamiento, hash, etc.)? *(ej. 3DES, AES, SHA, etc.)*	SI
4.5	¿La información *confidencial o sensible* de los sistemas (incluyendo la que se almacena en las copias de respaldo) se *almacena ilegible*?*(ej. 3DES, AES, SHA, etc.)*	SI
4.6	Si los sistemas procesan, transmiten o almacenan información de tarjetas de pago (crédito, débito) ¿se ha definido o contemplado definir un proceso de gestión de las llaves criptográficas usadas para el cifrado de la información de los sistemas?	N/A
4.7	¿La información *confidencial o sensible* del ambiente productivo se utiliza para actividades de desarrollo o pruebas, sin pasar por un proceso de despersonalización o enmascaramiento?	SI

5. Alertas/Eventos

#	Preguntas	Respuesta
5.1	¿Los sistemas y los componentes tecnológicos que lo soportan (servidores, bases de datos, etc.) están en capacidad de registrar, alertar y almacenar los eventos que afecten la seguridad de la información?	SI
5.2	¿Cuáles de los siguientes eventos se ha considerado registrar en los sistemas o en los componentes tecnológicos que lo soportan?	
5.2.1	Accesos a información clasificada como *confidencial y privilegiada* de la compañía.	SI
5.2.2	Acciones realizadas con privilegios especiales (administradores, superusuarios, etc.)	SI
5.2.3	Intentos de acceso a los sistemas (exitosos y fallidos).	NO
5.2.4	Creación, modificación, eliminación, desactivación, bloqueo y desbloqueo de usuarios.	SI
5.2.5	Cambios en la configuración de seguridad en sistemas, bases de datos, equipos de comunicación, etc.	SI
5.3	¿Qué información se incluye en los registros de eventos de seguridad?	
5.3.1	Fecha y hora del evento.	SI
5.3.2	Identificación del usuario que lo realiza.	SI
5.3.3	Tipo de evento.	SI
5.3.4	Descripción del evento. (Detalle del evento, acción ejecutada, éxito o fracaso de la operación, etc.).	SI
5.3.5	Componente del sistema o recurso afectado.	SI
5.3.6	Identificación del equipo desde el cual se realizó la operación (ej. dirección IP, dirección MAC, nombre del equipo, etc.).	SI
5.4	¿Se ha considerado implementar mecanismos de seguridad para evitar que los registros de eventos (logs) sean modificados (ej. a través de control de acceso, segregación de redes, etc.)?	SI
5.5	¿La fecha y la hora de los sistemas y los componentes que lo soportan se encuentran sincronizados con un servicio de sincronización de relojes?	SI

6. Gestión de Vulnerabilidades

#	Preguntas	Respuesta
6.1	¿Se ha contemplado la ejecución de pruebas de vulnerabilidades y/o intrusión a los sistemas y los componentes que lo soportan (servidores, bases de datos, equipos de comunicaciones, etc.)?	SI
6.1.1	¿Se ha contemplado establecer planes de acción encaminados a resolver las vulnerabilidades encontradas?	SI
6.2	¿Las plataformas que soportan los sistemas se encuentran aseguradas de tal forma que sólo ejecute los servicios requeridos por los sistemas?	SI

7. Desarrollo Seguro de Sistemas

#	Preguntas	Respuesta

7.1	¿Se consideran prácticas de desarrollo seguro de aplicaciones y establecimiento de pruebas técnicas, funcionales y de seguridad del sistema?	SI
7.2	¿Los sistemas cuentan con ambientes de desarrollo, pruebas y producción?	NO
7.3	¿Los sistemas realizan validación de datos de entrada (ej. tipos de datos esperados, longitudes de datos esperados, tipos de caracteres esperados, etc.)?	SI
7.4	¿La información de autenticación (usuarios y contraseñas) y/o direcciones IP se encuentran en *texto claro,* "quemadas" en el código fuente del sistema o en un archivo de configuración sin cifrar?	NO
7.5	En el caso que algún sistema ha sido suministrado o desarrollado por un tercero, ¿se tiene contemplado realizar actualizaciones periódicas del software con el fin de garantizar la funcionalidad y seguridad del mismo?	N/A

8. Seguridad en Redes

#	Preguntas	Respuesta
8.1	¿Los sistemas interactúan con otros *sistemas* o *componentes tecnológicos* diferentes a los que lo soportan (ej. servicios, bases de datos, servidores, etc.)?	SI
8.2	¿El sistema interactúa con *sistemas* o *componentes tecnológicos* ubicados en redes externas a las de la Organización (ej. proveedores, entes reguladores, aliados, etc.)?	SI
8.3	¿Se cuenta con algún mecanismo de seguridad a nivel de red para la protección de la información que se intercambia con estos *sistemas* o *componentes tecnológicos* externos (SSL, IPSEC, etc.)?	SI
8.4	¿Las conexiones desde y hacia la red donde se encuentran los sistemas o los componentes tecnológicos son controladas por dispositivos de seguridad tipo *firewall*?	SI
8.5	¿Los *componentes de almacenamiento de datos* (ej. Bases de datos) del sistema se encuentran ubicados en un segmento seguro de la red y no en zonas catalogadas como no seguras (ej. DMZ)?	SI
8.6	¿Existen sistemas de prevención y/o detección de intrusos ubicados en la red donde se encuentra el sistema y los componentes tecnológicos que lo soportan?	SI

9. Seguridad Física

#	Preguntas	Respuesta
9.1	¿El centro de procesamiento de información (centro de datos) cuenta con controles de acceso físico (ej. exclusas, tarjetas de proximidad, biométricos, chapa convencional con llave, etc.)?	SI
9.2	¿El centro de procesamiento de información (centro de datos) cuenta con controles ambientales (ej. aire acondicionado, detectores de incendio e inundación, extintores, etc.)?	SI
9.3	¿El centro de procesamiento de información (centro de datos) cuenta con circuitos alternos y equipo de respaldo para suministro de energía?	SI

9.4	¿Existe una bitácora o registro de acceso al centro de procesamiento de información (centro de datos) mantenida al menos por (3) tres meses?	NO
9.5	¿Se cuenta con un proceso de revisión periódico de los registros de acceso y alertas de intento de violación al centro de procesamiento de información (centro de cómputo)?	NO

10. Continuidad del Negocio

#	Preguntas	Respuesta
10.1	Los sistemas y los componentes tecnológicos que lo soportan se encuentran dentro del alcance del *plan de continuidad de negocio de la organización*?	NO
10.2	En caso de no existir un plan de continuidad en la organización, ¿existen planes documentados de contingencia y/o recuperación de los sistemas y los componentes que lo soportan?	SI
10.3	¿Se ha considerado la implementación de procedimientos periódicos de copia de respaldo de la información de los sistemas?	SI
10.3.1	¿Los medios de almacenamiento para copias de respaldo (back ups) han sido dimensionados de acuerdo con las necesidades de los sistemas y cubren el tiempo de retención de información definido?	SI
10.4	¿Las copias de respaldo de la información de los sistemas cuentan con mecanismos de almacenamiento y custodia externa?	SI

11. No Repudio

#	Preguntas	Respuesta
11.1	¿El sistema realiza transacciones electrónicas (ej. redención de pago subsidio, etc.)?	SI
11.2	El sistema cuenta con mecanismos para registrar la información necesaria para certificar las transacciones electrónicas realizadas en sus diferentes etapas: - Requerimiento del servicio (Origen del requerimiento, Dirección IP del origen). - Resultado de la transacción (Aprobación o rechazo). - Evidencia de la transferencia y almacenamiento de información. - Evidencia de la verificación.	SI
11.3	¿La información de las transacciones rechazadas es almacenada con el fin de verificar posteriormente si la transacción concluyó consistentemente en todos los sistemas que involucró?	SI

12. Contratación, Licenciamiento y Documentación

#	Preguntas	Respuesta
12.1	¿El sistema o algunos de los componentes que lo soportan (frameworks, código fuente, aplicaciones de soporte, etc.) requieren licenciamiento para su uso (comercial, open source, etc.)?	SI

12.1.1	¿Todas las licencias cuentan con los respectivos soportes (documento físico o electrónico de condiciones de licenciamiento, factura de compra, contrato de adquisición, etc.)?	SI
12.1.2	¿Los medios originales de instalación, manuales y documentos de licencia de uso del sistema o los componentes que lo soportan, son inventariados y conservados por el área responsable en un lugar seguro y designado específicamente para este fin?	SI
12.3	¿Se cuenta con manuales de instalación, configuración, administración, operación y usuario final formalmente documentados?	SI

Cuestionario de Identificación de Riesgos: Proceso Crítico del Negocio "Gestión del Fondo de Desarrollo Productivo"

Completado por:	**Ernesto Lizano**
Fecha:	**11/4/2014**

1. *Análisis de Riesgos y Clasificación de Información*

#	Preguntas	Respuesta
1.1	¿Existe definido un responsable (colaborador, área, gerencia, dirección, entre otros) de la información de los sistemas?	SI
1.2	¿Existe definido un administrador (ej. colaborador, área, gerencia, dirección, entre otros) de los sistemas?	SI
1.3	¿La información de los sistemas fue identificada y clasificada por su responsable (dueño), teniendo en cuenta su criticidad?	SI

2. *Identificación y Autenticación*

#	Preguntas	Respuesta
2.1	¿Todos los usuarios son identificados en los sistemas mediante una única cuenta de acceso y al menos un método de autenticación?	SI
2.2	¿Los sistemas restringen que la contraseña esté conformada por mínimo 8 caracteres con combinaciones de números, letras y caracteres especiales?	SI
2.3	¿El acceso de los usuarios es bloqueado después de máximo 5 intentos de ingreso consecutivos fallidos?	NO
2.4	¿Los sistemas solicitan el cambio periódico de contraseña, máximo cada 90 días?	NO
2.5	¿Las cuentas de usuario que sobrepasen el período de 90 días de inactividad son bloqueadas de manera preventiva por los sistemas?	NO
2.6	¿Los sistemas informan al menos con 15 días de anticipación el vencimiento de la contraseña?	NO
2.7	¿Los sistemas almacenan historial de contraseñas (al menos 10)?	NO
2.8	¿Los sistemas solicitan el cambio obligatorio de la contraseña en el primer uso de la cuenta o cuando ha sido restablecida?	SI

2.9	¿La sesión de usuario dentro de los sistemas es cerrada de forma automática, después de 15 minutos de inactividad?	SI
2.10	Los sistemas cuentan con un módulo de administración de seguridad que permite al menos: - La creación, modificación, desactivación y eliminación de usuarios. - La administración de parámetros de seguridad. - La generación de reportes (usuarios, perfiles, etc.).	SI

3. Autorización y Controles de Acceso

#	Preguntas	Respuesta
3.1	¿Los sistemas permiten establecer roles o niveles de acceso de acuerdo a las actividades, responsabilidades y necesidades de cada usuario?	SI
3.2	¿El personal que realiza funciones asociadas a un ambiente específico del sistema (desarrollo, pruebas o producción), cuenta con un perfil de acceso que limita sus actividades exclusivamente a este ambiente?	SI
3.3	¿Las cuentas de usuario con perfil de administración únicamente son utilizadas para labores administrativas?	N/A
3.4	¿Los sistemas cuentan con la capacidad de controlar el acceso de los usuarios a sus diferentes módulos y funciones?	SI

4. Protección de los Datos

#	Preguntas	Respuesta
4.1	¿La información de ingreso a los sistemas (*usuario y contraseña*) se mantiene ilegible al momento de *transmitirla*? *(ej. SSL, IPSEC, VPN, cifrado de datos, etc.)*	SI
4.2	¿El *intercambio de archivos* con información *confidencial* o *sensible*, se realiza utilizando protocolos seguros (FTPS, SFTP) o mediante el cifrado de los datos?	N/A
4.3	Si los sistemas tienen arquitectura Web y están expuestos a Internet, ¿se implementan protocolos seguros (ej. HTTPS con su respectivo certificado) para proteger la información transmitida?	SI
4.4	¿Las *contraseñas* de todas las cuentas de los sistemas se *almacenan ilegibles* (cifrado con algoritmos fuertes, truncamiento, hash, etc.)? *(ej. 3DES, AES, SHA, etc.)*	SI
4.5	¿La información *confidencial o sensible* de los sistemas (incluyendo la que se almacena en las copias de respaldo) se *almacena ilegible*?*(ej. 3DES, AES, SHA, etc.)*	SI
4.6	Si los sistemas procesan, transmiten o almacenan información de tarjetas de pago (crédito, débito) ¿se ha definido o contemplado definir un proceso de gestión de las llaves criptográficas usadas para el cifrado de la información de los sistemas?	N/A
4.7	¿La información *confidencial o sensible* del ambiente productivo se utiliza para actividades de desarrollo o pruebas, sin pasar por un proceso de despersonalización o enmascaramiento?	SI

5. *Alertas/Eventos*

#	Preguntas	Respuesta
5.1	¿Los sistemas y los componentes tecnológicos que lo soportan (servidores, bases de datos, etc.) están en capacidad de registrar, alertar y almacenar los eventos que afecten la seguridad de la información?	SI
5.2	¿Cuáles de los siguientes eventos se ha considerado registrar en los sistemas o en los componentes tecnológicos que lo soportan?	
5.2.1	Accesos a información clasificada como *confidencial y privilegiada* de la compañía.	SI
5.2.2	Acciones realizadas con privilegios especiales (administradores, superusuarios, etc.)	SI
5.2.3	Intentos de acceso a los sistemas (exitosos y fallidos).	NO
5.2.4	Creación, modificación, eliminación, desactivación, bloqueo y desbloqueo de usuarios.	SI
5.2.5	Cambios en la configuración de seguridad en sistemas, bases de datos, equipos de comunicación, etc.	SI
5.3	¿Qué información se incluye en los registros de eventos de seguridad?	
5.3.1	Fecha y hora del evento.	SI
5.3.2	Identificación del usuario que lo realiza.	SI
5.3.3	Tipo de evento.	SI
5.3.4	Descripción del evento. (Detalle del evento, acción ejecutada, éxito o fracaso de la operación, etc.).	SI
5.3.5	Componente del sistema o recurso afectado.	SI
5.3.6	Identificación del equipo desde el cual se realizó la operación (ej. dirección IP, dirección MAC, nombre del equipo, etc.).	NO
5.4	¿Se ha considerado implementar mecanismos de seguridad para evitar que los registros de eventos (logs) sean modificados (ej. a través de control de acceso, segregación de redes, etc.)?	SI
5.5	¿La fecha y la hora de los sistemas y los componentes que lo soportan se encuentran sincronizados con un servicio de sincronización de relojes?	SI

6. *Gestión de Vulnerabilidades*

#	Preguntas	Respuesta
6.1	¿Se ha contemplado la ejecución de pruebas de vulnerabilidades y/o intrusión a los sistemas y los componentes que lo soportan (servidores, bases de datos, equipos de comunicaciones, etc.)?	SI
6.1.1	¿Se ha contemplado establecer planes de acción encaminados a resolver las vulnerabilidades encontradas?	SI
6.2	¿Las plataformas que soportan los sistemas se encuentran aseguradas de tal forma que sólo ejecute los servicios requeridos por los sistemas?	SI

7. *Desarrollo Seguro de Sistemas*

#	Preguntas	Respuesta
7.1	¿Se consideran prácticas de desarrollo seguro de aplicaciones y establecimiento de pruebas técnicas, funcionales y de seguridad del sistema?	SI
7.2	¿Los sistemas cuentan con ambientes de desarrollo, pruebas y producción?	SI
7.3	¿Los sistemas realizan validación de datos de entrada (ej. tipos de datos esperados, longitudes de datos esperados, tipos de caracteres esperados, etc.)?	SI
7.4	¿La información de autenticación (usuarios y contraseñas) y/o direcciones IP se encuentran en *texto claro,* "quemadas" en el código fuente del sistema o en un archivo de configuración sin cifrar?	SI
7.5	En el caso que algún sistema ha sido suministrado o desarrollado por un tercero, ¿se tiene contemplado realizar actualizaciones periódicas del software con el fin de garantizar la funcionalidad y seguridad del mismo?	SI

8. Seguridad en Redes

#	Preguntas	Respuesta
8.1	¿Los sistemas interactúan con otros *sistemas* o *componentes tecnológicos* diferentes a los que lo soportan (ej. servicios, bases de datos, servidores, etc.)?	SI
8.2	¿El sistema interactúa con *sistemas* o *componentes tecnológicos* ubicados en redes externas a las de la Organización (ej. proveedores, entes reguladores, aliados, etc.)?	SI
8.3	¿Se cuenta con algún mecanismo de seguridad a nivel de red para la protección de la información que se intercambia con estos *sistemas* o *componentes tecnológicos* externos (SSL, IPSEC, etc.)?	SI
8.4	¿Las conexiones desde y hacia la red donde se encuentran los sistemas o los componentes tecnológicos son controladas por dispositivos de seguridad tipo *firewall*?	SI
8.5	¿Los *componentes de almacenamiento de datos* (ej. Bases de datos) del sistema se encuentran ubicados en un segmento seguro de la red y no en zonas catalogadas como no seguras (ej. DMZ)?	SI
8.6	¿Existen sistemas de prevención y/o detección de intrusos ubicados en la red donde se encuentra el sistema y los componentes tecnológicos que lo soportan?	SI

9. Seguridad Física

#	Preguntas	Respuesta
9.1	¿El centro de procesamiento de información (centro de datos) cuenta con controles de acceso físico (ej. exclusas, tarjetas de proximidad, biométricos, chapa convencional con llave, etc.)?	SI
9.2	¿El centro de procesamiento de información (centro de datos) cuenta con controles ambientales (ej. aire acondicionado, detectores de incendio e inundación, extintores, etc.)?	SI

9.3	¿El centro de procesamiento de información (centro de datos) cuenta con circuitos alternos y equipo de respaldo para suministro de energía?	SI
9.4	¿Existe una bitácora o registro de acceso al centro de procesamiento de información (centro de datos) mantenida al menos por (3) tres meses?	NO
9.5	¿Se cuenta con un proceso de revisión periódico de los registros de acceso y alertas de intento de violación al centro de procesamiento de información (centro de cómputo)?	NO

10. Continuidad del Negocio

#	Preguntas	Respuesta
10.1	Los sistemas y los componentes tecnológicos que lo soportan se encuentran dentro del alcance del *plan de continuidad de negocio de la organización*?	NO
10.2	En caso de no existir un plan de continuidad en la organización, ¿existen planes documentados de contingencia y/o recuperación de los sistemas y los componentes que lo soportan?	SI
10.3	¿Se ha considerado la implementación de procedimientos periódicos de copia de respaldo de la información de los sistemas?	SI
10.3.1	¿Los medios de almacenamiento para copias de respaldo (back ups) han sido dimensionados de acuerdo con las necesidades de los sistemas y cubren el tiempo de retención de información definido?	SI
10.4	¿Las copias de respaldo de la información de los sistemas cuentan con mecanismos de almacenamiento y custodia externa?	SI

11. No Repudio

#	Preguntas	Respuesta
11.1	¿El sistema realiza transacciones electrónicas (ej. redención de pago subsidio, etc.)?	NO
11.2	El sistema cuenta con mecanismos para registrar la información necesaria para certificar las transacciones electrónicas realizadas en sus diferentes etapas: - Requerimiento del servicio (Origen del requerimiento, Dirección IP del origen). - Resultado de la transacción (Aprobación o rechazo). - Evidencia de la transferencia y almacenamiento de información. - Evidencia de la verificación.	N/A
11.3	¿La información de las transacciones rechazadas es almacenada con el fin de verificar posteriormente si la transacción concluyó consistentemente en todos los sistemas que involucró?	N/A

12. Contratación, Licenciamiento y Documentación

#	Preguntas	Respuesta

12.1	¿El sistema o algunos de los componentes que lo soportan (frameworks, código fuente, aplicaciones de soporte, etc.) requieren licenciamiento para su uso (comercial, open source, etc.)?	SI
12.1.1	¿Todas las licencias cuentan con los respectivos soportes (documento físico o electrónico de condiciones de licenciamiento, factura de compra, contrato de adquisición, etc.)?	SI
12.1.2	¿Los medios originales de instalación, manuales y documentos de licencia de uso del sistema o los componentes que lo soportan, son inventariados y conservados por el área responsable en un lugar seguro y designado específicamente para este fin?	SI
12.3	¿Se cuenta con manuales de instalación, configuración, administración, operación y usuario final formalmente documentados?	SI

Cuestionario de Identificación de Riesgos: Proceso Crítico del Negocio "Regulación de Precios de Combustibles"

Completado por:	**Mauricio Morales**
Fecha:	**11/4/2014**

1. *Análisis de Riesgos y Clasificación de Información*

#	Preguntas	Respuesta
1.1	¿Existe definido un responsable (colaborador, área, gerencia, dirección, entre otros) de la información de los sistemas?	SI
1.2	¿Existe definido un administrador (ej. colaborador, área, gerencia, dirección, entre otros) de los sistemas?	SI
1.3	¿La información de los sistemas fue identificada y clasificada por su responsable (dueño), teniendo en cuenta su criticidad?	SI

2. *Identificación y Autenticación*

#	Preguntas	Respuesta
2.1	¿Todos los usuarios son identificados en los sistemas mediante una única cuenta de acceso y al menos un método de autenticación?	SI
2.2	¿Los sistemas restringen que la contraseña esté conformada por mínimo 8 caracteres con combinaciones de números, letras y caracteres especiales?	NO
2.3	¿El acceso de los usuarios es bloqueado después de máximo 5 intentos de ingreso consecutivos fallidos?	NO
2.4	¿Los sistemas solicitan el cambio periódico de contraseña, máximo cada 90 días?	NO
2.5	¿Las cuentas de usuario que sobrepasen el período de 90 días de inactividad son bloqueadas de manera preventiva por los sistemas?	NO
2.6	¿Los sistemas informan al menos con 15 días de anticipación el vencimiento de la contraseña?	NO

2.7	¿Los sistemas almacenan historial de contraseñas (al menos 10)?	NO
2.8	¿Los sistemas solicitan el cambio obligatorio de la contraseña en el primer uso de la cuenta o cuando ha sido restablecida?	SI
2.9	¿La sesión de usuario dentro de los sistemas es cerrada de forma automática, después de 15 minutos de inactividad?	SI
2.10	Los sistemas cuentan con un módulo de administración de seguridad que permite al menos: - La creación, modificación, desactivación y eliminación de usuarios. - La administración de parámetros de seguridad. - La generación de reportes (usuarios, perfiles, etc.).	SI

3. Autorización y Controles de Acceso

#	Preguntas	Respuesta
3.1	¿Los sistemas permiten establecer roles o niveles de acceso de acuerdo a las actividades, responsabilidades y necesidades de cada usuario?	SI
3.2	¿El personal que realiza funciones asociadas a un ambiente específico del sistema (desarrollo, pruebas o producción), cuenta con un perfil de acceso que limita sus actividades exclusivamente a este ambiente?	NO
3.3	¿Las cuentas de usuario con perfil de administración únicamente son utilizadas para labores administrativas?	N/A
3.4	¿Los sistemas cuentan con la capacidad de controlar el acceso de los usuarios a sus diferentes módulos y funciones?	SI

4. Protección de los Datos

#	Preguntas	Respuesta
4.1	¿La información de ingreso a los sistemas (*usuario y contraseña*) se mantiene ilegible al momento de *transmitirla*? *(ej. SSL, IPSEC, VPN, cifrado de datos, etc.)*	SI
4.2	¿El *intercambio de archivos* con información *confidencial* o *sensible*, se realiza utilizando protocolos seguros (FTPS, SFTP) o mediante el cifrado de los datos?	N/A
4.3	Si los sistemas tienen arquitectura Web y están expuestos a Internet, ¿se implementan protocolos seguros (ej. HTTPS con su respectivo certificado) para proteger la información transmitida?	SI
4.4	¿Las *contraseñas* de todas las cuentas de los sistemas se *almacenan ilegibles* (cifrado con algoritmos fuertes, truncamiento, hash, etc.)? *(ej. 3DES, AES, SHA, etc.)*	SI
4.5	¿La información *confidencial o sensible* de los sistemas (incluyendo la que se almacena en las copias de respaldo) se *almacena ilegible*?*(ej. 3DES, AES, SHA, etc.)*	NO
4.6	Si los sistemas procesan, transmiten o almacenan información de tarjetas de pago (crédito, débito) ¿se ha definido o contemplado definir un proceso de gestión de las llaves criptográficas usadas para el cifrado de la información de los sistemas?	N/A

4.7	¿La información *confidencial o sensible* del ambiente productivo se utiliza para actividades de desarrollo o pruebas, sin pasar por un proceso de despersonalización o enmascaramiento?	SI

5. Alertas/Eventos

#	Preguntas	Respuesta
5.1	¿Los sistemas y los componentes tecnológicos que lo soportan (servidores, bases de datos, etc.) están en capacidad de registrar, alertar y almacenar los eventos que afecten la seguridad de la información?	SI
5.2	¿Cuáles de los siguientes eventos se ha considerado registrar en los sistemas o en los componentes tecnológicos que lo soportan?	
5.2.1	Accesos a información clasificada como *confidencial y privilegiada* de la compañía.	SI
5.2.2	Acciones realizadas con privilegios especiales (administradores, superusuarios, etc.)	SI
5.2.3	Intentos de acceso a los sistemas (exitosos y fallidos).	NO
5.2.4	Creación, modificación, eliminación, desactivación, bloqueo y desbloqueo de usuarios.	SI
5.2.5	Cambios en la configuración de seguridad en sistemas, bases de datos, equipos de comunicación, etc.	SI
5.3	¿Qué información se incluye en los registros de eventos de seguridad?	
5.3.1	Fecha y hora del evento.	SI
5.3.2	Identificación del usuario que lo realiza.	SI
5.3.3	Tipo de evento.	SI
5.3.4	Descripción del evento. (Detalle del evento, acción ejecutada, éxito o fracaso de la operación, etc.).	SI
5.3.5	Componente del sistema o recurso afectado.	SI
5.3.6	Identificación del equipo desde el cual se realizó la operación (ej. dirección IP, dirección MAC, nombre del equipo, etc.).	SI
5.4	¿Se ha considerado implementar mecanismos de seguridad para evitar que los registros de eventos (logs) sean modificados (ej. a través de control de acceso, segregación de redes, etc.)?	SI
5.5	¿La fecha y la hora de los sistemas y los componentes que lo soportan se encuentran sincronizados con un servicio de sincronización de relojes?	SI

6. Gestión de Vulnerabilidades

#	Preguntas	Respuesta
6.1	¿Se ha contemplado la ejecución de pruebas de vulnerabilidades y/o intrusión a los sistemas y los componentes que lo soportan (servidores, bases de datos, equipos de comunicaciones, etc.)?	SI
6.1.1	¿Se ha contemplado establecer planes de acción encaminados a resolver las vulnerabilidades encontradas?	SI

6.2	¿Las plataformas que soportan los sistemas se encuentran aseguradas de tal forma que sólo ejecute los servicios requeridos por los sistemas?	SI

7. Desarrollo Seguro de Sistemas

#	Preguntas	Respuesta
7.1	¿Se consideran prácticas de desarrollo seguro de aplicaciones y establecimiento de pruebas técnicas, funcionales y de seguridad del sistema?	SI
7.2	¿Los sistemas cuentan con ambientes de desarrollo, pruebas y producción?	NO
7.3	¿Los sistemas realizan validación de datos de entrada (ej. tipos de datos esperados, longitudes de datos esperados, tipos de caracteres esperados, etc.)?	SI
7.4	¿La información de autenticación (usuarios y contraseñas) y/o direcciones IP se encuentran en *texto claro,* "quemadas" en el código fuente del sistema o en un archivo de configuración sin cifrar?	SI
7.5	En el caso que algún sistema ha sido suministrado o desarrollado por un tercero, ¿se tiene contemplado realizar actualizaciones periódicas del software con el fin de garantizar la funcionalidad y seguridad del mismo?	SI

8. Seguridad en Redes

#	Preguntas	Respuesta
8.1	¿Los sistemas interactúan con otros *sistemas* o *componentes tecnológicos* diferentes a los que lo soportan (ej. servicios, bases de datos, servidores, etc.)?	SI
8.2	¿El sistema interactúa con *sistemas* o *componentes tecnológicos* ubicados en redes externas a las de la Organización (ej. proveedores, entes reguladores, aliados, etc.)?	SI
8.3	¿Se cuenta con algún mecanismo de seguridad a nivel de red para la protección de la información que se intercambia con estos *sistemas* o *componentes tecnológicos* externos (SSL, IPSEC, etc.)?	SI
8.4	¿Las conexiones desde y hacia la red donde se encuentran los sistemas o los componentes tecnológicos son controladas por dispositivos de seguridad tipo *firewall*?	SI
8.5	¿Los *componentes de almacenamiento de datos* (ej. Bases de datos) del sistema se encuentran ubicados en un segmento seguro de la red y no en zonas catalogadas como no seguras (ej. DMZ)?	SI
8.6	¿Existen sistemas de prevención y/o detección de intrusos ubicados en la red donde se encuentra el sistema y los componentes tecnológicos que lo soportan?	SI

9. Seguridad Física

#	Preguntas	Respuesta

9.1	¿El centro de procesamiento de información (centro de datos) cuenta con controles de acceso físico (ej. exclusas, tarjetas de proximidad, biométricos, chapa convencional con llave, etc.)?	SI
9.2	¿El centro de procesamiento de información (centro de datos) cuenta con controles ambientales (ej. aire acondicionado, detectores de incendio e inundación, extintores, etc.)?	SI
9.3	¿El centro de procesamiento de información (centro de datos) cuenta con circuitos alternos y equipo de respaldo para suministro de energía?	SI
9.4	¿Existe una bitácora o registro de acceso al centro de procesamiento de información (centro de datos) mantenida al menos por (3) tres meses?	NO
9.5	¿Se cuenta con un proceso de revisión periódico de los registros de acceso y alertas de intento de violación al centro de procesamiento de información (centro de cómputo)?	NO

10. Continuidad del Negocio

#	Preguntas	Respuesta
10.1	Los sistemas y los componentes tecnológicos que lo soportan se encuentran dentro del alcance del *plan de continuidad de negocio de la organización*?	NO
10.2	En caso de no existir un plan de continuidad en la organización, ¿existen planes documentados de contingencia y/o recuperación de los sistemas y los componentes que lo soportan?	SI
10.3	¿Se ha considerado la implementación de procedimientos periódicos de copia de respaldo de la información de los sistemas?	SI
10.3.1	¿Los medios de almacenamiento para copias de respaldo (back ups) han sido dimensionados de acuerdo con las necesidades de los sistemas y cubren el tiempo de retención de información definido?	SI
10.4	¿Las copias de respaldo de la información de los sistemas cuentan con mecanismos de almacenamiento y custodia externa?	SI

11. No Repudio

#	Preguntas	Respuesta
11.1	¿El sistema realiza transacciones electrónicas (ej. redención de pago subsidio, etc.)?	NO
11.2	El sistema cuenta con mecanismos para registrar la información necesaria para certificar las transacciones electrónicas realizadas en sus diferentes etapas: - Requerimiento del servicio (Origen del requerimiento, Dirección IP del origen). - Resultado de la transacción (Aprobación o rechazo). - Evidencia de la transferencia y almacenamiento de información. - Evidencia de la verificación.	N/A

11.3	¿La información de las transacciones rechazadas es almacenada con el fin de verificar posteriormente si la transacción concluyó consistentemente en todos los sistemas que involucró?	N/A

12. Contratación, Licenciamiento y Documentación

#	Preguntas	Respuesta
12.1	¿El sistema o algunos de los componentes que lo soportan (frameworks, código fuente, aplicaciones de soporte, etc.) requieren licenciamiento para su uso (comercial, open source, etc.)?	SI
12.1.1	¿Todas las licencias cuentan con los respectivos soportes (documento físico o electrónico de condiciones de licenciamiento, factura de compra, contrato de adquisición, etc.)?	SI
12.1.2	¿Los medios originales de instalación, manuales y documentos de licencia de uso del sistema o los componentes que lo soportan, son inventariados y conservados por el área responsable en un lugar seguro y designado específicamente para este fin?	SI
12.3	¿Se cuenta con manuales de instalación, configuración, administración, operación y usuario final formalmente documentados?	SI

Cuestionario de Identificación de Riesgos: Proceso Crítico del Negocio "Acceso a Aplicativos"

Completado por:	**Ernesto Lizano**
Fecha:	**11/4/2014**

1. Análisis de Riesgos y Clasificación de Información

#	Preguntas	Respuesta
1.1	¿Existe definido un responsable (colaborador, área, gerencia, dirección, entre otros) de la información de los sistemas?	SI
1.2	¿Existe definido un administrador (ej. colaborador, área, gerencia, dirección, entre otros) de los sistemas?	SI
1.3	¿La información de los sistemas fue identificada y clasificada por su responsable (dueño), teniendo en cuenta su criticidad?	SI

2. Identificación y Autenticación

#	Preguntas	Respuesta
2.1	¿Todos los usuarios son identificados en los sistemas mediante una única cuenta de acceso y al menos un método de autenticación?	SI
2.2	¿Los sistemas restringen que la contraseña esté conformada por mínimo 8 caracteres con combinaciones de números, letras y caracteres especiales?	NO

2.3	¿El acceso de los usuarios es bloqueado después de máximo 5 intentos de ingreso consecutivos fallidos?	SI
2.4	¿Los sistemas solicitan el cambio periódico de contraseña, máximo cada 90 días?	NO
2.5	¿Las cuentas de usuario que sobrepasen el período de 90 días de inactividad son bloqueadas de manera preventiva por los sistemas?	NO
2.6	¿Los sistemas informan al menos con 15 días de anticipación el vencimiento de la contraseña?	NO
2.7	¿Los sistemas almacenan historial de contraseñas (al menos 10)?	NO
2.8	¿Los sistemas solicitan el cambio obligatorio de la contraseña en el primer uso de la cuenta o cuando ha sido restablecida?	SI
2.9	¿La sesión de usuario dentro de los sistemas es cerrada de forma automática, después de 15 minutos de inactividad?	SI
2.10	Los sistemas cuentan con un módulo de administración de seguridad que permite al menos: - La creación, modificación, desactivación y eliminación de usuarios. - La administración de parámetros de seguridad. - La generación de reportes (usuarios, perfiles, etc.).	SI

3. Autorización y Controles de Acceso

#	Preguntas	Respuesta
3.1	¿Los sistemas permiten establecer roles o niveles de acceso de acuerdo a las actividades, responsabilidades y necesidades de cada usuario?	SI
3.2	¿El personal que realiza funciones asociadas a un ambiente específico del sistema (desarrollo, pruebas o producción), cuenta con un perfil de acceso que limita sus actividades exclusivamente a este ambiente?	SI
3.3	¿Las cuentas de usuario con perfil de administración únicamente son utilizadas para labores administrativas?	N/A
3.4	¿Los sistemas cuentan con la capacidad de controlar el acceso de los usuarios a sus diferentes módulos y funciones?	SI

4. Protección de los Datos

#	Preguntas	Respuesta
4.1	¿La información de ingreso a los sistemas (*usuario y contraseña*) se mantiene ilegible al momento de *transmitirla*? *(ej. SSL, IPSEC, VPN, cifrado de datos, etc.)*	NO
4.2	¿El *intercambio de archivos* con información *confidencial* o *sensible*, se realiza utilizando protocolos seguros (FTPS, SFTP) o mediante el cifrado de los datos?	N/A
4.3	Si los sistemas tienen arquitectura Web y están expuestos a Internet, ¿se implementan protocolos seguros (ej. HTTPS con su respectivo certificado) para proteger la información transmitida?	NO

4.4	¿Las *contraseñas* de todas las cuentas de los sistemas se *almacenan ilegibles* (cifrado con algoritmos fuertes, truncamiento, hash, etc.)? *(ej. 3DES, AES, SHA, etc.)*	SI
4.5	¿La información *confidencial o sensible* de los sistemas (incluyendo la que se almacena en las copias de respaldo) se *almacena ilegible*?*(ej. 3DES, AES, SHA, etc.)*	N/A
4.6	Si los sistemas procesan, transmiten o almacenan información de tarjetas de pago (crédito, débito) ¿se ha definido o contemplado definir un proceso de gestión de las llaves criptográficas usadas para el cifrado de la información de los sistemas?	N/A
4.7	¿La información *confidencial o sensible* del ambiente productivo se utiliza para actividades de desarrollo o pruebas, sin pasar por un proceso de despersonalización o enmascaramiento?	NO

5. Alertas/Eventos

#	Preguntas	Respuesta
5.1	¿Los sistemas y los componentes tecnológicos que lo soportan (servidores, bases de datos, etc.) están en capacidad de registrar, alertar y almacenar los eventos que afecten la seguridad de la información?	SI
5.2	¿Cuáles de los siguientes eventos se ha considerado registrar en los sistemas o en los componentes tecnológicos que lo soportan?	
5.2.1	Accesos a información clasificada como *confidencial y privilegiada* de la compañía.	N/A
5.2.2	Acciones realizadas con privilegios especiales (administradores, superusuarios, etc.)	SI
5.2.3	Intentos de acceso a los sistemas (exitosos y fallidos).	SI
5.2.4	Creación, modificación, eliminación, desactivación, bloqueo y desbloqueo de usuarios.	SI
5.2.5	Cambios en la configuración de seguridad en sistemas, bases de datos, equipos de comunicación, etc.	SI
5.3	¿Qué información se incluye en los registros de eventos de seguridad?	
5.3.1	Fecha y hora del evento.	SI
5.3.2	Identificación del usuario que lo realiza.	SI
5.3.3	Tipo de evento.	SI
5.3.4	Descripción del evento. (Detalle del evento, acción ejecutada, éxito o fracaso de la operación, etc.).	SI
5.3.5	Componente del sistema o recurso afectado.	SI
5.3.6	Identificación del equipo desde el cual se realizó la operación (ej. dirección IP, dirección MAC, nombre del equipo, etc.).	SI
5.4	¿Se ha considerado implementar mecanismos de seguridad para evitar que los registros de eventos (logs) sean modificados (ej. a través de control de acceso, segregación de redes, etc.)?	SI
5.5	¿La fecha y la hora de los sistemas y los componentes que lo soportan se encuentran sincronizados con un servicio de sincronización de relojes?	SI

6. Gestión de Vulnerabilidades

#	Preguntas	Respuesta
6.1	¿Se ha contemplado la ejecución de pruebas de vulnerabilidades y/o intrusión a los sistemas y los componentes que lo soportan (servidores, bases de datos, equipos de comunicaciones, etc.)?	SI
6.1.1	¿Se ha contemplado establecer planes de acción encaminados a resolver las vulnerabilidades encontradas?	SI
6.2	¿Las plataformas que soportan los sistemas se encuentran aseguradas de tal forma que sólo ejecute los servicios requeridos por los sistemas?	SI

7. Desarrollo Seguro de Sistemas

#	Preguntas	Respuesta
7.1	¿Se consideran prácticas de desarrollo seguro de aplicaciones y establecimiento de pruebas técnicas, funcionales y de seguridad del sistema?	SI
7.2	¿Los sistemas cuentan con ambientes de desarrollo, pruebas y producción?	SI
7.3	¿Los sistemas realizan validación de datos de entrada (ej. tipos de datos esperados, longitudes de datos esperados, tipos de caracteres esperados, etc.)?	SI
7.4	¿La información de autenticación (usuarios y contraseñas) y/o direcciones IP se encuentran en *texto claro,* "quemadas" en el código fuente del sistema o en un archivo de configuración sin cifrar?	SI
7.5	En el caso que algún sistema ha sido suministrado o desarrollado por un tercero, ¿se tiene contemplado realizar actualizaciones periódicas del software con el fin de garantizar la funcionalidad y seguridad del mismo?	N/A

8. Seguridad en Redes

#	Preguntas	Respuesta
8.1	¿Los sistemas interactúan con otros *sistemas* o *componentes tecnológicos* diferentes a los que lo soportan (ej. servicios, bases de datos, servidores, etc.)?	SI
8.2	¿El sistema interactúa con *sistemas* o *componentes tecnológicos* ubicados en redes externas a las de la Organización (ej. proveedores, entes reguladores, aliados, etc.)?	NO
8.3	¿Se cuenta con algún mecanismo de seguridad a nivel de red para la protección de la información que se intercambia con estos *sistemas* o *componentes tecnológicos* externos (SSL, IPSEC, etc.)?	N/A
8.4	¿Las conexiones desde y hacia la red donde se encuentran los sistemas o los componentes tecnológicos son controladas por dispositivos de seguridad tipo *firewall*?	SI
8.5	¿Los *componentes de almacenamiento de datos* (ej. Bases de datos) del sistema se encuentran ubicados en un segmento seguro de la red y no en zonas catalogadas como no seguras (ej. DMZ)?	SI
8.6	¿Existen sistemas de prevención y/o detección de intrusos ubicados en la red donde se encuentra el sistema y los componentes tecnológicos que lo soportan?	SI

9. Seguridad Física

#	Preguntas	Respuesta
9.1	¿El centro de procesamiento de información (centro de datos) cuenta con controles de acceso físico (ej. exclusas, tarjetas de proximidad, biométricos, chapa convencional con llave, etc.)?	SI
9.2	¿El centro de procesamiento de información (centro de datos) cuenta con controles ambientales (ej. aire acondicionado, detectores de incendio e inundación, extintores, etc.)?	SI
9.3	¿El centro de procesamiento de información (centro de datos) cuenta con circuitos alternos y equipo de respaldo para suministro de energía?	SI
9.4	¿Existe una bitácora o registro de acceso al centro de procesamiento de información (centro de datos) mantenida al menos por (3) tres meses?	NO
9.5	¿Se cuenta con un proceso de revisión periódico de los registros de acceso y alertas de intento de violación al centro de procesamiento de información (centro de cómputo)?	NO

10. Continuidad del Negocio

#	Preguntas	Respuesta
10.1	Los sistemas y los componentes tecnológicos que lo soportan se encuentran dentro del alcance del *plan de continuidad de negocio de la organización*?	NO
10.2	En caso de no existir un plan de continuidad en la organización, ¿existen planes documentados de contingencia y/o recuperación de los sistemas y los componentes que lo soportan?	SI
10.3	¿Se ha considerado la implementación de procedimientos periódicos de copia de respaldo de la información de los sistemas?	SI
10.3.1	¿Los medios de almacenamiento para copias de respaldo (back ups) han sido dimensionados de acuerdo con las necesidades de los sistemas y cubren el tiempo de retención de información definido?	SI
10.4	¿Las copias de respaldo de la información de los sistemas cuentan con mecanismos de almacenamiento y custodia externa?	SI

11. No Repudio

#	Preguntas	Respuesta
11.1	¿El sistema realiza transacciones electrónicas (ej. redención de pago subsidio, etc.)?	NO

11.2	El sistema cuenta con mecanismos para registrar la información necesaria para certificar las transacciones electrónicas realizadas en sus diferentes etapas: - Requerimiento del servicio (Origen del requerimiento, Dirección IP del origen). - Resultado de la transacción (Aprobación o rechazo). - Evidencia de la transferencia y almacenamiento de información. - Evidencia de la verificación.	N/A
11.3	¿La información de las transacciones rechazadas es almacenada con el fin de verificar posteriormente si la transacción concluyó consistentemente en todos los sistemas que involucró?	N/A

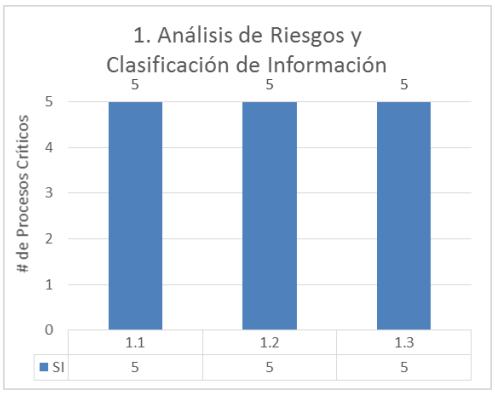
12. Contratación, Licenciamiento y Documentación

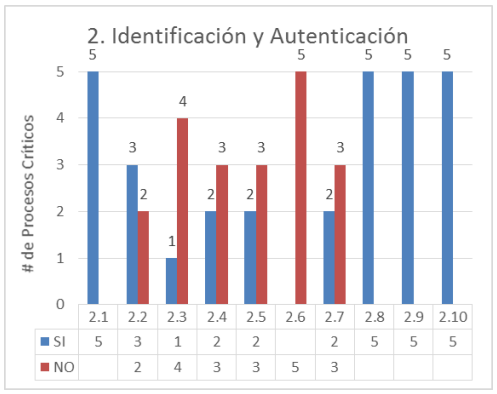
#	Preguntas	Respuesta
12.1	¿El sistema o algunos de los componentes que lo soportan (frameworks, código fuente, aplicaciones de soporte, etc.) requieren licenciamiento para su uso (comercial, open source, etc.)?	SI
12.1.1	¿Todas las licencias cuentan con los respectivos soportes (documento físico o electrónico de condiciones de licenciamiento, factura de compra, contrato de adquisición, etc.)?	SI
12.1.2	¿Los medios originales de instalación, manuales y documentos de licencia de uso del sistema o los componentes que lo soportan, son inventariados y conservados por el área responsable en un lugar seguro y designado específicamente para este fin?	SI
12.3	¿Se cuenta con manuales de instalación, configuración, administración, operación y usuario final formalmente documentados?	SI

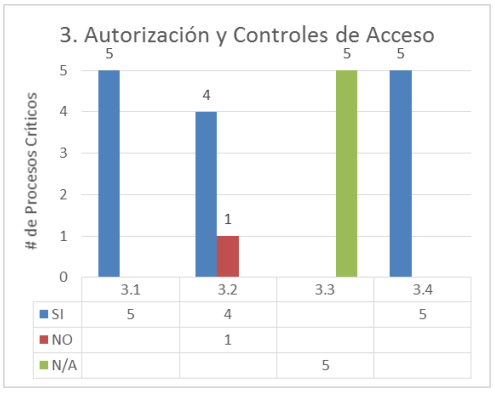
Anexo 2- Tabulación de Cuestionarios de Identificación de Riesgos por Proceso Crítico

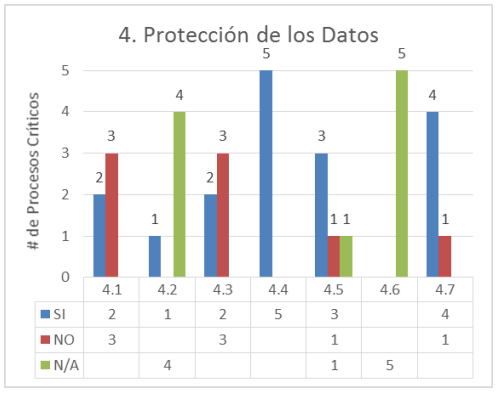
Dominio		Respuesta Obtenida		
	Pregunta	SI	NO	N/A
1. Análisis de Riesgos y Clasificación de Información	1.1	5		
	1.2	5		
	1.3	5		
2. Identificación y Autenticación	2.1	5		
	2.2	3	2	
	2.3	1	4	
	2.4	2	3	
	2.5	2	3	
	2.6		5	
	2.7	2	3	
	2.8	5		
	2.9	5		
	2.10	5		
3. Autorización y Controles de Acceso	3.1	5		
	3.2	4	1	
	3.3			5
	3.4	5		
4. Protección de los Datos	4.1	2	3	
	4.2	1		4
	4.3	2	3	
	4.4	5		
	4.5	3	1	1
	4.6			5
	4.7	4	1	
5. Alertas/Eventos	5.1	5		
	5.2.1	4		1
	5.2.2	5		
	5.2.3	1	4	
	5.2.4	5		
	5.2.5	5		
	5.3.1	5		
	5.3.2	5		
	5.3.3	5		
	5.3.4	5		
	5.3.5	5		
	5.3.6	4	1	
	5.4	5		

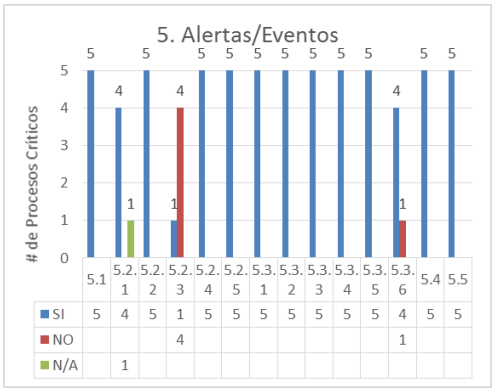
Dominio		Respuesta Obtenida		
	Pregunta	SI	NO	N/A
	5.5	5		
6. Gestión de Vulnerabilidades	6.1	5		
	6.1.1	5		
	6.2	5		
7. Desarrollo Seguro de Sistemas	7.1	5		
	7.2	2	3	
	7.3	5		
	7.4	3	2	
	7.5	2		3
8. Seguridad en Redes	8.1	5		
	8.2	4	1	
	8.3	4		1
	8.4	5		
	8.5	5		
	8.6	5		
9. Seguridad Física	9.1	5		
	9.2	5		
	9.3	5		
	9.4		5	
	9.5		5	
10. Continuidad del Negocio	10.1		5	
	10.2	5		
	10.3	5		
	10.3.1	5		
	10.4	5		
11. No Repudio	11.1	2	3	
	11.2	2		3
	11.3	2		3
12. Contratación, Licenciamiento y Documentación	12.1	5		
	12.1.1	5		
	12.1.2	5		
	12.3	5		

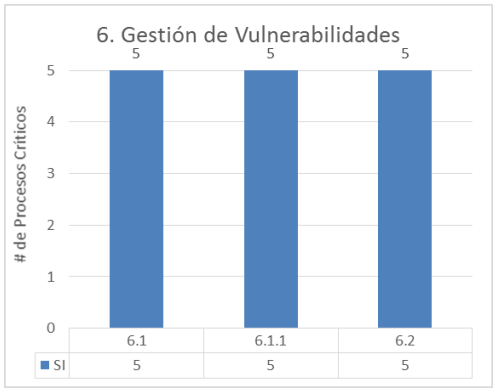

1. Análisis de Riesgos y Clasificación de Información
de Procesos Críticos
1.1 1.2 1.3
SI 5 5 5

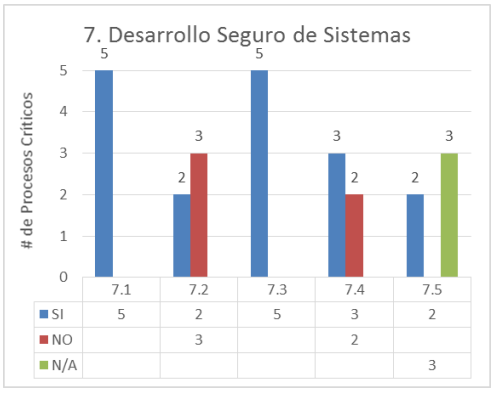

2. Identificación y Autenticación
de Procesos Críticos
2.1 2.2 2.3 2.4 2.5 2.6 2.7 2.8 2.9 2.10
SI 5 3 1 2 2 2 5 5 5
NO 2 4 3 3 5 3

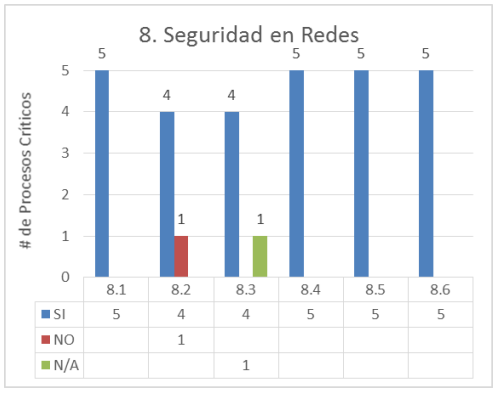

3. Autorización y Controles de Acceso
de Procesos Críticos
3.1 3.2 3.3 3.4
SI 5 4 5
NO 1
N/A 5

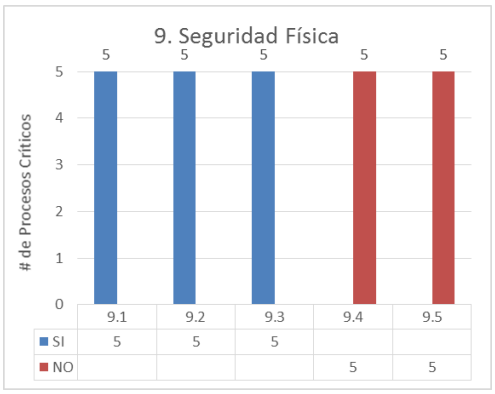

4. Protección de los Datos
de Procesos Críticos
4.1 4.2 4.3 4.4 4.5 4.6 4.7
SI 2 1 2 5 3 4
NO 3 3 1 1
N/A 4 1 5

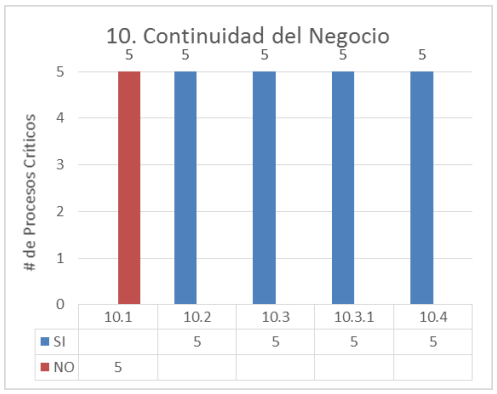

5. Alertas/Eventos
de Procesos Críticos
5.1 5.2.1 5.2.2 5.2.3 5.2.4 5.2.5 5.3.1 5.3.2 5.3.3 5.3.4 5.3.5 5.3.6 5.4 5.5
SI 5 4 5 1 5 5 5 5 5 5 5 4 5 5
NO 4 1
N/A 1

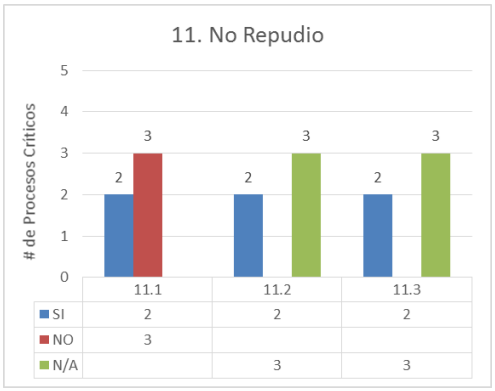

6. Gestión de Vulnerabilidades
de Procesos Críticos
6.1 6.1.1 6.2
SI 5 5 5

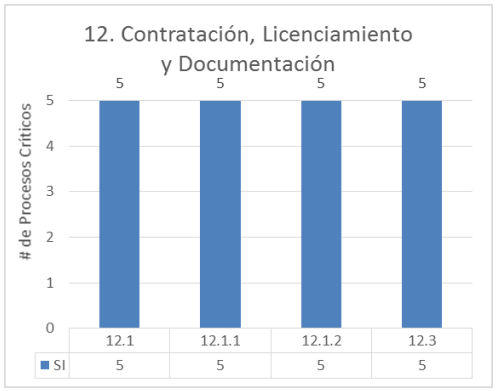

7. Desarrollo Seguro de Sistemas
de Procesos Críticos
7.1 7.2 7.3 7.4 7.5
SI 5 2 5 3 2
NO 3 2
N/A 3


8. Seguridad en Redes
de Procesos Críticos
8.1 8.2 8.3 8.4 8.5 8.6
SI 5 4 4 5 5 5
NO 1
N/A 1


9. Seguridad Física
de Procesos Críticos
5 5 5 5 5
9.1 9.2 9.3 9.4 9.5
SI 5 5 5
NO 5 5


10. Continuidad del Negocio
de Procesos Críticos
5 5 5 5 5
10.1 10.2 10.3 10.3.1 10.4
SI 5 5 5 5
NO 5

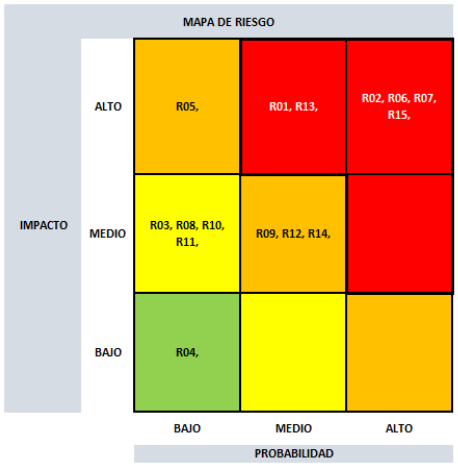

11. No Repudio
de Procesos Críticos
2 3 2 3 2 3
11.1 11.2 11.3
SI 2 2 2
NO 3
N/A 3 3


12. Contratación, Licenciamiento y Documentación
de Procesos Críticos
5 5 5 5
12.1 12.1.1 12.1.2 12.3
SI 5 5 5 5

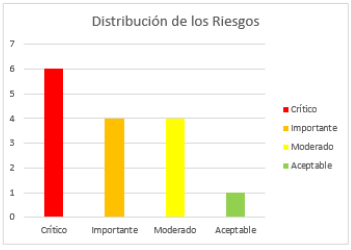
Anexo 3- Matriz de Riesgos

RIESGOS										
Código del Riesgo	Activo (Seleccionar)	Tipo de Activo	Descripción del riesgo	Consecuencias	Vulnerabilidad	Área Responsable del Riesgo	Fecha de Detección	Probabilidad Inherente	Impacto Inherente	Severidad del Riesgo
R01	• Gestión del Fondo de Desarrollo Productivo • Regulación de Precios de Combustibles • Acceso a Aplicativos	Aplicaciones	Acceso no autorizado al sistema debido a que no se cuenta con parámetros de contraseñas seguras en el sistema: • Longitud mínima y/o combinaciones de números, letras y caracteres especiales. • No se solicita cambio de clave periódicamente. • No se almacena historial de últimas	Confidencialidad; Integridad; Disponibilidad	Administración inadecuada de contraseñas	División de Desarrollo de Sistemas	04-nov-14	M	H	Crítico
R02	• Pago al Subsidio del GLP • Gestión de Tarjeta Solidaria • Gestión del Fondo de Desarrollo Productivo • Regulación de Precios de	Aplicaciones	Acceso no autorizado al sistema mediante ataques de fuerza bruta sobre las claves del sistema debido a que el acceso a los usuarios no es deshabilitado después de varios intentos de ingreso consecutivos fallidos.	Confidencialidad; Integridad; Disponibilidad	Administración inadecuada de contraseñas	División de Desarrollo de Sistemas	04-nov-14	H	H	Crítico
R03	• Gestión del Fondo de Desarrollo Productivo • Regulación de Precios de Combustibles • Acceso a Aplicativos	Aplicaciones	Acceso no autorizado al sistema con cuentas inactivas, debido a que las cuentas de usuario que sobrepasen el período de inactividad definido no son bloqueadas de manera preventiva.	Confidencialidad; Integridad; Disponibilidad	Falla de implementación de política de pantalla despejada/bloqueo sesión/cuentas inactivas	División de Desarrollo de Sistemas	04-nov-14	L	M	Moderado
R04	• Pago al Subsidio del GLP • Gestión de Tarjeta Solidaria • Gestión del Fondo de Desarrollo Productivo • Regulación de Precios de Combustibles	Aplicaciones	Implementación no válida o desalineada de la administración y características de expiración contraseñas debido a que el sistema no notifica con anticipación el vencimiento de las claves.	Cumplimiento	Administración inadecuada de contraseñas	División de Desarrollo de Sistemas	04-nov-14	L	L	Aceptable
R05	• Regulación de Precios de Combustibles	Aplicaciones	Acceso y uso inadecuado de ambientes específicos del sistema debido a que no se cuenta con perfiles de acceso específico que limiten las actividades entre los ambientes de desarrollo, pruebas y producción.	Confidencialidad; Integridad	Inadecuada segregación de funciones	División de Desarrollo de Sistemas	04-nov-14	L	H	Importante
R06	• Pago al Subsidio del GLP • Gestión de Tarjeta Solidaria • Acceso a Aplicativos	Aplicaciones	Ataques de seguridad (Sniffing, man in the middle, suplantación de servidor, alteración de paquetes) por interceptación sobre información sensible y claves e ID de usuarios que se intercambia entre los sistemas de arquitectura WEB o durante la transimisón a las bases de datos debido a que los mismos se transfieren a través de protocolos inseguros o por canales sin medidas de protección.	Confidencialidad	Fuga/divulgación/exposición de información sensible o privilegiada	División de Desarrollo de Sistemas	04-nov-14	H	H	Crítico
R07	• Regulación de Precios de Combustibles	Información	Exposición de datos sensibles o confidenciales cuando se almacenan debido a que estas se guardan de forma legible o con algoritmos de cifrado débil.	Confidencialidad; Cumplimiento	Administración de cifrado inadecuada/inexistente	División de Desarrollo de Sistemas	04-nov-14	H	H	Crítico
	• Pago al Subsidio del GLP • Gestión de Tarjeta		Fuga y posible copia no controlada de la información sensible debido al uso de datos		Uso inadecuado de datos de	División de				

Registro de Riesgos | Matriz de Riesgos | Tratamiento | Matriz de Riesgos Tratamiento



Código del Riesgo	Impa	Probabilidad Inherente
R01	H	M
R02	H	H
R03	M	L
R04	L	L
R05	H	L
R06	H	H
R07	H	H
R08	M	L
R09	M	M
R10	M	L
R11	M	L
R12	M	M
R13	H	M
R14	M	M
R15	H	H



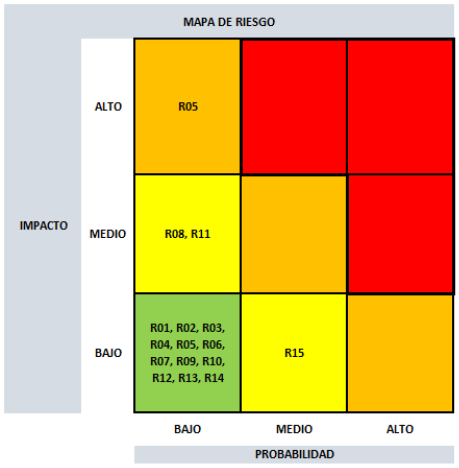
Distribución de los Riesgos		
Severidad del Riesgo	Conteo	Porcentaje
Crítico	6	40%
Importante	4	27%
Moderado	4	27%
Aceptable	1	7%
Grand Total	15	100%

Registro de Riesgos | Matriz de Riesgos | Tratamiento | Matriz de Riesgos Tratamiento

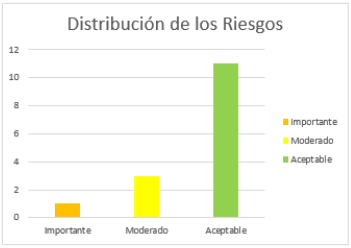
PLANES DE TRATAMIENTO

Código del Riesgo	Descripción del Riesgo	Severidad	Opción de Tratamiento	Descripción del Plan	Área Responsable del Tratamiento	Fecha Propuesta de Cierre	Probabilidad Residual	Impacto Residual	Severidad Residual	Riesgos Relacionados	Estado del Plan	Fecha de Cierre
R01	Acceso no autorizado al sistema debido a que no se cuenta con parámetros de contraseñas seguras en el sistema: • Longitud mínima y/o combinaciones de números, letras y caracteres especiales. • No se solicita cambio de clave periódicamente. • No se almacena historial de últimas	Crítico	Mitigar	Se implementarán mecanismos que permitan la creación de contraseñas seguras y que cumplan con las siguientes características: • Longitud mínima de la contraseña. • Uso de caracteres alfanuméricos que incluyan mayúsculas, minúsculas, números y caracteres especiales. • La contraseña no podrá ser igual a ninguna de las utilizadas recientemente.	División de Desarrollo de Sistemas	15-ene-15	L	L	Aceptable	R2,R3,R4	Activo	
R02	Acceso no autorizado al sistema mediante ataques de fuerza bruta sobre las claves del sistema debido a que el acceso a los usuarios no es deshabilitado después de varios intentos de ingreso consecutivos fallidos.	Crítico	Mitigar	Se implementará el bloqueo de las cuentas de usuarios en caso de varios intentos de acceso fallidos al recurso o componente tecnológico.	División de Desarrollo de Sistemas	15-ene-15	L	L	Aceptable	R1,R3,R4	Activo	
R03	Acceso no autorizado al sistema con cuentas inactivas, debido a que las cuentas de usuario que sobrepasen el período de inactividad definido no son bloqueadas de manera	Moderado	Mitigar	Se implementarán mecanismos que bloquen de forma automática las cuentas de usuario que no han sido accedidas en un período de 90 días.	División de Desarrollo de Sistemas	15-ene-15	L	L	Aceptable	R1,R2,R4	Activo	
R04	Implementación no válida o desalineada de la administración y características de expiración contraseñas debido a que el sistema no notifica con anticipación el vencimiento de las	Aceptable	Mitigar	Se implementarán mecanismos que notifiquen con 15 días de anticipación el vencimiento de las claves de usuario.	División de Desarrollo de Sistemas	15-ene-15	L	L	Aceptable	R1,R2,R3	Activo	
R05	Acceso y uso inadecuado de ambientes específicos del sistema debido a que no se cuenta con perfiles de acceso específico que limiten las actividades entre los ambientes de desarrollo, pruebas y producción.	Importante	Aceptar		División de Desarrollo de Sistemas	04-nov-14	L	H	Importante	R9,R12	Cerrado	04-nov-14
R06	Ataques de seguridad (sniffing, man in the middle, suplantación de servidor, alteración de paquetes) por interceptación sobre información sensible y claves e ID de usuarios que se intercambia entre los sistemas de arquitectura WEB o durante la transimisón a las bases de datos debido a que los mismos se transfieren a través de protocolos inseguros o por canales	Crítico	Mitigar	Se implementarán mecanismos para mantener ilegibles las contraseñas e información sensible al momento de transmitirlas, por medio de certificados digitales SSL. Además, se incluirán mecanismos de validación que re direccionen automáticamente las páginas hacia protocolo HTTPS.	División de Desarrollo de Sistemas	04-dic-14	L	L	Aceptable		Activo	
R07	Exposición de datos sensibles o confidenciales cuando se almacenan debido a que estas se guardan de forma legible o con algoritmos de cifrado débil.	Crítico	Mitigar	Se identificará, definirá e implementará medidas de seguridad según la clasificación y valoración de los activos de información. Dentro de estas medidas se considerará: • Procesos de clasificación de información. • Estándar de cifrado. • Cifrado de información (tablas, columnas, según aplique).	División de Desarrollo de Sistemas	04-may-15	L	L	Aceptable		Activo	
R08	Fuga y posible copia no controlada de la información sensible debido al uso de datos de producción en ambientes de pruebas sin que se haya ejecutado un procedimiento de despersonalización o enmascaramiento.	Moderado	Aceptar		División de Desarrollo de Sistemas	04-nov-14	L	M	Moderado	R6,R12	Cerrado	04-nov-14

Registro de Riesgos | Matriz de Riesgos | **Tratamiento** | Matriz de Riesgos Tratamiento



Código del Riesgo	Impa	Probabilidad Residual
R01	L	L
R02	L	L
R03	L	L
R04	L	L
R05	H	L
R06	L	L
R07	L	L
R08	M	L
R09	L	L
R10	L	L
R11	M	L
R12	L	L
R13	L	L
R14	L	L
R15	L	M



Distribución de los Riesgos		
Severidad Residual	Conteo	Porcentaje
Importante	1	7%
Moderado	3	20%
Aceptable	11	73%
Grand Total	**15**	**100%**

Registro de Riesgos | Matriz de Riesgos | Tratamiento | **Matriz de Riesgos Tratamiento**

Anexo 4 - Análisis de Riesgos

MINISTERIO DE ECONOMÍA
GOBIERNO DE
EL SALVADOR
UNÁMONOS PARA CRECER

Análisis de Impacto de Negocio (BIA)

Versión:	1
Fecha :	13-Nov-2014
Creado por:	Ernesto Lizano Mario Pastori Francisco Valiente

Tabla de Contenido

Introducción

Este Análisis de Impacto (BIA) es desarrollado como parte del proceso de plan de contingencia para los sistemas que sustentan los procesos críticos del MINEC. Fue desarrollado el 13 de Nov de 2014.

Objetivos

El objetivo del BIA es identificar y priorizar los procesos primarios del MINEC relacionándolos con los sistemas que los soportan, utilizando esta información para clasificar el impacto en los procesos si el sistema estuviera no disponible.

EL BIA está compuesto por los siguientes tres pasos:

1. **Determinación de los procesos de misión/de negocio y recuperación critica**. Procesos críticos del negocio soportados por el sistema son identificados y el impacto de una disrupción en el sistema a estos procesos es determinado junto con impactos de caídas programadas y un tiempo de caída estimado. El tiempo de caída refleja el tiempo máximo que la organización puede tolerar aun manteniendo el servicio.

2. **Identificación de requerimientos de recursos**. Esfuerzos de recuperación reales requieren una profunda evaluación de los recursos requeridos para los procesos de negocio e interdependencias relacionadas los más rápido posibles.

3. **Identificación de las prioridades de recuperación para los recursos del sistema**. Basándose en los resultados de las actividades anteriores, los recursos del sistema son claramente relacionados con los procesos críticos del negocio. Los niveles de prioridad son establecidos de acuerdo a la secuencia de recuperación de las actividades y recursos.

Descripción del sistema

Los sistemas incluidos en este documento son los siguientes:

1. Pago de subsidio del GLP

Descripción:	Sistema que soporta el proceso de pago del subsidio al Gas licuado que se entrega a más de 1 millón de personas mensualmente.
Entorno Operativo:	• Windows Server • SQL Server
Ubicación Física:	Centro de Datos, Edificio 1
Usuarios Involucrados:	• Administrador de Base de Datos • Analista Programador

2. Sistema de Gestión de Tarjeta Solidaria

Descripción:	La Tarjeta Solidaria es un sistema que se ha habilitado para atender activaciones, cambios de PIN y bloqueos, mediante el registro electrónico o llamada al 2590-9090, donde el operador pedirá los datos personales y dará un número secreto, que se debe guardar, ya que servirá al momento de la compra del gas.
Entorno Operativo:	Planta telefónica, Software propietario (AVAYA).
Ubicación Física:	Centro de Datos, Edificio 1
Usuarios Involucrados:	• Jefe de División de Desarrollo de Sistemas • Administrador de Bases de Datos

3. Gestión del Fondo de Desarrollo Productivo

Descripción:	Es un fondo financiero para otorgar cofinanciamiento no reembolsable a la Micro, Pequeña y Mediana Empresa (MIPYME), a fin de fortalecer la competitividad y generar impacto económico, el cofinanciamiento es de 60% del valor de la iniciativa para empresas dentro del área metropolitana de San Salvador (AMSS), 75% para las empresas ubicadas fuera del AMSS y 90% para proyectos de emprendimiento dinámico. Dirigido a: Micro, Pequeña y Mediana Empresa (MIPYMES).
Entorno Operativo:	• Linux • Oracle 11g
Ubicación Física:	Centro de Datos, Edificio 1
Usuarios Involucrados:	• Jefe de División de Desarrollo de Sistemas • Analista Programador

4. Sistema de Regulación de Precios de Combustibles (Hidrocarburos)

Descripción:	Permite el registro, inspección y control de los precios de los combustibles, esto se realiza mediante registro electrónico o llamada a un número de contacto. Estos precios son publicados para que la población los utilice como referencia.
Entorno Operativo:	• Windows Server • SQL Server 2008
Ubicación Física:	Centro de Datos, Edificio 1
Usuarios Involucrados:	• Jefe de División de Desarrollo de Sistemas • Analista Programador

5. Acceso a Aplicativos (Plataforma WEB MINEC)

Descripción:	Hace referencia a la página web institucional, que sirve de enlace para que instituciones y público en general acceda a los sistemas y servicios de interés.
Entorno Operativo:	• Linux • MySQL
Ubicación Física:	Centro de Datos, Edificio 1
Usuarios Involucrados:	• Analista Programador

Recolección de datos BIA

La recolección de datos se llevó a cabo en base a entrevistas con personal del Ministerio de Economía, Dirección de Tecnologías de la Información y Telecomunicaciones; esto como mando estratégico. Como mando táctico se llevaron a cabo entrevistas con el Jefe de Infraestructura y Desarrollo. Para la parte operativa se hicieron entrevistas con técnicos y desarrolladores.

Procesos y sistemas de criticidad

Partiendo de las aportaciones de los contactos internos del MINEC, se lograron identificar los procesos críticos o primarios del negocio, los cuales se detallan a continuación:

Proceso de Negocio	Descripción
Pago al subsidio del GLP	Proceso que soporta el pago del subsidio al Gas licuado que se entrega a más de 1 millón de personas mensualmente.
Sistema de Gestión de Tarjeta Solidaria	La Tarjeta Solidaria es un proceso que se ha habilitado para atender activaciones, cambios de PIN y bloqueos, mediante el registro electrónico o llamada al 2590-9090, donde el operador pedirá los datos personales y dará un número secreto, que se debe guardar, ya que servirá al momento de la compra del gas.

Proceso de Negocio	Descripción
Gestión del Fondo de Desarrollo Productivo	Es un fondo financiero para otorgar cofinanciamiento no reembolsable a la Micro, Pequeña y Mediana Empresa (MIPYME), a fin de fortalecer la competitividad y generar impacto económico, el cofinanciamiento es de 60% del valor de la iniciativa para empresas dentro del área metropolitana de San Salvador (AMSS), 75% para las empresas ubicadas fuera del AMSS y 90% para proyectos de emprendimiento dinámico. Dirigido a: Micro, Pequeña y Mediana Empresa (MIPYMES)
Sistema de Regulación de Precios de Combustibles (Hidrocarburos)	Permite el registro, inspección y control de los precios de los combustibles, esto se realiza mediante registro electrónico o llamada a un número de contacto. Estos precios son publicados para que la población los utilice como referencia.
Acceso a Aplicativos	Hace referencia a la página web institucional, que sirve de enlace para que instituciones y público en general acceda a los sistemas y servicios de interés.

Impactos de las Caídas y el Tiempo Estimado de Inactividad

Impactos de las Caídas

Las siguientes categorías de impacto representan áreas importantes para la consideración en el caso de una interrupción o impacto.

Categoría de Impacto: Social
Definición: Se entenderá como la respuesta objetiva de parte de la población o gran parte de esta, al cambio inducido en la disponibilidad de un proyecto o programa social sostenido en el tiempo y en algunos casos extendido a ciertos grupos no involucrados en etapas anteriores.

Los valores de impacto para evaluar esta categoría son:

- **Alto:** Si la cantidad de beneficiarios afectados por la interrupción es mayor a 40%.
- **Medio:** Si la cantidad de beneficiarios afectados por la interrupción no sobrepasa el 40% y es mayor al 20%.
- **Bajo:** Si la cantidad de beneficiarios afectados por la interrupción es menor al 20%.

Categoría de Impacto: Político
Definición: Se refiere a las implicaciones que genera la indisponibilidad del producto o servicio en el Gobierno de turno afectado directamente por las leyes y políticas públicas que son apoyadas por la Institución encargada de velar por el servicio.

Los valores de impacto para evaluar esta categoría son:

- **Alto:** Si la cantidad de beneficiarios afectados es mayor al 40%, el impacto político se considera alto debido a que la percepción de la imagen de la institución se ve afectada de forma crítica.
- **Medio:** Si la cantidad de beneficiarios afectados es mayor al 20% y menor al 40%, el impacto se considera medio debido a que la percepción de la imagen de la institución se ve afectada de forma moderada.
- **Bajo:** Si la cantidad de beneficiarios afectados es menor al 20%, el impacto se considera bajo debido a que la percepción de la imagen de la institución se ve levemente afectada.

La siguiente tabla resume el impacto para cada proceso de misión/de negocio si alguno de los sistemas descritos no estuviera disponible, basada en el siguiente criterio:

Proceso de Negocio	Categoría de impacto	
	Impacto Social	Impacto Político
Pago al subsidio del GLP	Alto	Alto
Sistema de Gestión de Tarjeta Solidaria	Alto	Alto
Gestión del Fondo de Desarrollo Productivo	Medio	Bajo
Sistema de Regulación de Precios de Combustibles (Hidrocarburos)	Medio	Bajo
Acceso a Aplicativos	Medio	Bajo

Tiempo Estimado de Inactividad

Trabajando directamente con los dueños de los procesos del negocio, personal del departamento, gerentes y otros interesados, se estimaron los factores de tiempo de inactividad para su consideración como consecuencia de un evento disruptivo.

- **Tiempo de inactividad máximo tolerable (MTD).** El MTD representa el tiempo total que los líderes/gerentes están dispuestos a aceptar en un corte de los procesos del negocio o interrupción, e incluye todas las consideraciones de impacto. La determinación del MTD es importante porque podría dejar planificadores de continuidad con dirección imprecisa en (1) selección de un método de recuperación adecuado, y (2) el grado de detalle que se requerirá en el desarrollo de los procedimientos de recuperación, incluyendo su alcance y contenido.

- **Tiempo de Recuperación Objetivo (RTO).** RTO define la cantidad máxima de tiempo que un recurso del sistema puede permanecer no disponible antes de que haya un impacto inaceptable en otros recursos del sistema, procesos del negocio soportados, y el MTD. Determinar el RTO de los recursos del sistema de información es importante para la selección de tecnologías apropiadas para el cumplimiento del MTD.

- **Punto de Recuperación Objetivo (RPO).** El RPO representa el punto en el tiempo, antes de que la perturbación o interrupción del sistema suceda, y al cual se deben recuperar los datos del proceso crítico del negocio, luego de una interrupción.

La siguiente tabla identifica el MTD, RTO, y RPO para los procesos críticos del negocio que dependen de los sistemas.

Proceso de Negocio	MTD	RTO	RPO
Pago al subsidio del GLP	4 horas	1 hora	1 hora
Sistema de Gestión de Tarjeta Solidaria	4 horas	24 horas	24 horas
Gestión del Fondo de Desarrollo Productivo	72 horas	24 horas	24 horas
Sistema de Regulación de Precios de Combustibles (Hidrocarburos)	168 horas	24 horas	24 horas
Acceso a Aplicativos	48 horas	24 horas	24 horas

Requerimientos de recursos

La siguiente tabla identifica los recursos que componen los sistemas:

Recurso/Componente del Sistema	Plataforma/SO/Versión (de ser aplicable)	Descripción
Servidor Web 1	• Dell PowerEdge M620 • Windows Server 2012	Servidor Web Pago al subsidio del GLP
Servidor Base de Datos 1	• Dell PowerEdge R410 • Windows Server 2008 • Microsoft SQL Server 2008 Standard	Base de Datos de Pago al subsidio del GLP
Servidor Web 2	• Dell PowerEdge M620 • Windows Server 2012	Servidor Sistema de Gestión de Tarjeta Solidaria
Servidor Web 3	• Dell PowerEdge R810 • Red Hat Enterprise • Oracle 11g	Servidor Web de Gestión del Fondo de Desarrollo Productivo
Servidor Base de Datos 3	• Base de datos Oracle 11g	Base de Datos de Gestión del Fondo de Desarrollo Productivo
Servidor Web 4	• Dell PowerEdge 2950 • Microsoft Windows Server 2008 R2 • IIS 7.0	Servidor Web de Sistema de Regulación de Precios de Combustibles (Hidrocarburos)

Servidor Base de datos 4	• Microsoft SQL Server 2008	Base de Datos de Sistema de Regulación de Precios de Combustibles (Hidrocarburos)
Servidor Web 6	• Dell PowerEdge M520 • Red Hat Enterprise	Servidor Web de Acceso a Aplicativos
Servidor Base de datos 6	• MySQL	Base de Datos de Acceso a Aplicativos

Prioridades de recuperación de los recursos del sistema

La siguiente tabla muestra el orden de recuperación para los recursos de los sistemas. La tabla también identifica el tiempo previsto para la recuperación de los recursos a raíz del "peor caso" de interrupción.

Prioridad	Recurso/Componente del Sistema	Descripción	RTO
1	Servidor Base de datos 1	Base de Datos de Pago al subsidio del GLP	½ hora
2	Servidor web 1	Servidor Web Pago al subsidio del GLP	½ hora
3	Servidor web 2	Servidor Sistema de Gestión de Tarjeta Solidaria	1 hora
4	Servidor Base de Datos 3	Base de Datos de Gestión del Fondo de Desarrollo Productivo	12 horas
5	Servidor Web 3	Servidor Web de Gestión del Fondo de Desarrollo Productivo	12 horas
6	Servidor Base de Datos 4	Base de Datos de Sistema de Regulación de Precios de Combustibles (Hidrocarburos)	12 horas
7	Servidor Web 4	Servidor Web de Sistema de Regulación de Precios de Combustibles (Hidrocarburos)	12 horas
8	Servidor Base de Datos 6	Base de Datos de Acceso a Aplicativos	12 horas
9	Servidor web 6	Servidor Web de Acceso a Aplicativos	12 horas

MINISTERIO DE ECONOMÍA
GOBIERNO DE
EL SALVADOR
UNÁMONOS PARA CRECER

Plan de Recuperación de Desastres

Versión:	1
Fecha :	23-Nov-2014
Creado por:	Ernesto Lizano Mario Pastori Francisco Valiente

Tabla de Contenido

Introducción

El Plan de Recuperación de Desastres (DRP) contiene la descripción detallada de actividades que el Ministerio de Economía debe desarrollar con el objetivo de soportar una situación de desastre que interrumpa la operación de sus procesos críticos, además de proveer las actividades necesarias para volver a operar normalmente posterior a dicha situación de desastre.

Objetivos

Objetivo General

Desarrollar y documentar un Plan de Recuperación de Desastres bien estructurado y fácil de entender, que ayudará al Ministerio de Economía a recuperarse pronta y efectivamente ante una situación de desastre no prevista o emergencia que interrumpa los procesos críticos del Negocio y sus activos de información, manteniendo en todo momento la confidencialidad, integridad y disponibilidad de la información.

Objetivos Específicos

- Identificar los procesos críticos del Negocio y los activos de información asociados a dichos procesos.
- Identificar al personal clave para la gestión del DRP y garantizar que todos los empleados comprendan sus funciones en la aplicación del mismo.
- Desarrollar y documentar una evaluación de los niveles de emergencia, para determinar las condiciones y procesos a seguir en caso surja un desastre.
- Desarrollar procedimientos de respaldos de información adecuados y congruentes a los requerimientos del Negocio.
- Determinar los procedimientos necesarios inmediatos, a medio y a largo plazo, para la recuperación de los recursos necesarios para sustentar los servicios críticos del Ministerio de Economía.

Alcance

En la actualidad la Dirección de Tecnologías de Información ofrece todos los servicios tecnológicos del Ministerio de Economía, tanto a clientes internos (colaboradores) como clientes externos. Es importante señalar que el presente DRP está enfocado en los procesos críticos del Ministerio y los activos de información que los soportan.

Identificación de los Procesos Críticos del Negocio

Partiendo de las aportaciones de los contactos internos del MINEC, se lograron identificar los procesos críticos o primarios del negocio, los cuales se detallan a continuación:

Proceso de Negocio	Descripción
Pago al subsidio del GLP	Proceso que soporta el pago del subsidio al Gas licuado que se entrega a más de 1 millón de personas mensualmente.
Sistema de Gestión de Tarjeta Solidaria	La Tarjeta Solidaria es un proceso que se ha habilitado para atender activaciones, cambios de PIN y bloqueos, mediante el registro electrónico o llamada al 2590-9090, donde el operador pedirá los datos personales y dará un número secreto, que se debe guardar, ya que servirá al momento de la compra del gas.
Gestión del Fondo de Desarrollo Productivo	Es un fondo financiero para otorgar cofinanciamiento no reembolsable a la Micro, Pequeña y Mediana Empresa (MIPYME), a fin de fortalecer la competitividad y generar impacto económico, el cofinanciamiento es de 60% del valor de la iniciativa para empresas dentro del área metropolitana de San Salvador (AMSS), 75% para las empresas ubicadas fuera del AMSS y 90% para proyectos de emprendimiento dinámico. Dirigido a: Micro, Pequeña y Mediana Empresa (MIPYMES)
Sistema de Regulación de Precios de Combustibles (Hidrocarburos)	Permite el registro, inspección y control de los precios de los combustibles, esto se realiza mediante registro electrónico o llamada a un número de contacto. Estos precios son publicados para que la población los utilice como referencia.
Acceso a Aplicativos	Hace referencia a la página web institucional, que sirve de enlace para que instituciones y público en general acceda a los sistemas y servicios de interés.

Recursos Informáticos

La siguiente tabla identifica los recursos que componen los sistemas y que proceso crítico soportan:

Recurso/Componente del Sistema	Plataforma/SO/Versión (de ser aplicable)	Descripción
Servidor Web 1	• Dell PowerEdge M620 • Windows Server 2012	Servidor Web Pago al subsidio del GLP
Servidor Base de Datos 1	• Dell PowerEdge R410 • Windows Server 2008 • Microsoft SQL Server 2008 Standard	Base de Datos de Pago al subsidio del GLP
Servidor Web 2	• Dell PowerEdge M620 • Windows Server 2012	Servidor Sistema de Gestión de Tarjeta Solidaria
Servidor Web 3	• Dell PowerEdge R810 • Red Hat Enterprise • Oracle 11g	Servidor Web de Gestión del Fondo de Desarrollo Productivo
Servidor Base de Datos 3	• Base de datos Oracle 11g	Base de Datos de Gestión del Fondo de Desarrollo Productivo
Servidor Web 4	• Dell PowerEdge 2950 • Microsoft Windows Server 2008 R2 • IIS 7.0	Servidor Web de Sistema de Regulación de Precios de Combustibles (Hidrocarburos)
Servidor Base de datos 4	• Microsoft SQL Server 2008	Base de Datos de Sistema de Regulación de Precios de Combustibles (Hidrocarburos)
Servidor Web 6	• Dell PowerEdge M520 • Red Hat Enterprise	Servidor Web de Acceso a Aplicativos
Servidor Base de datos 6	• MySQL	Base de Datos de Acceso a Aplicativos

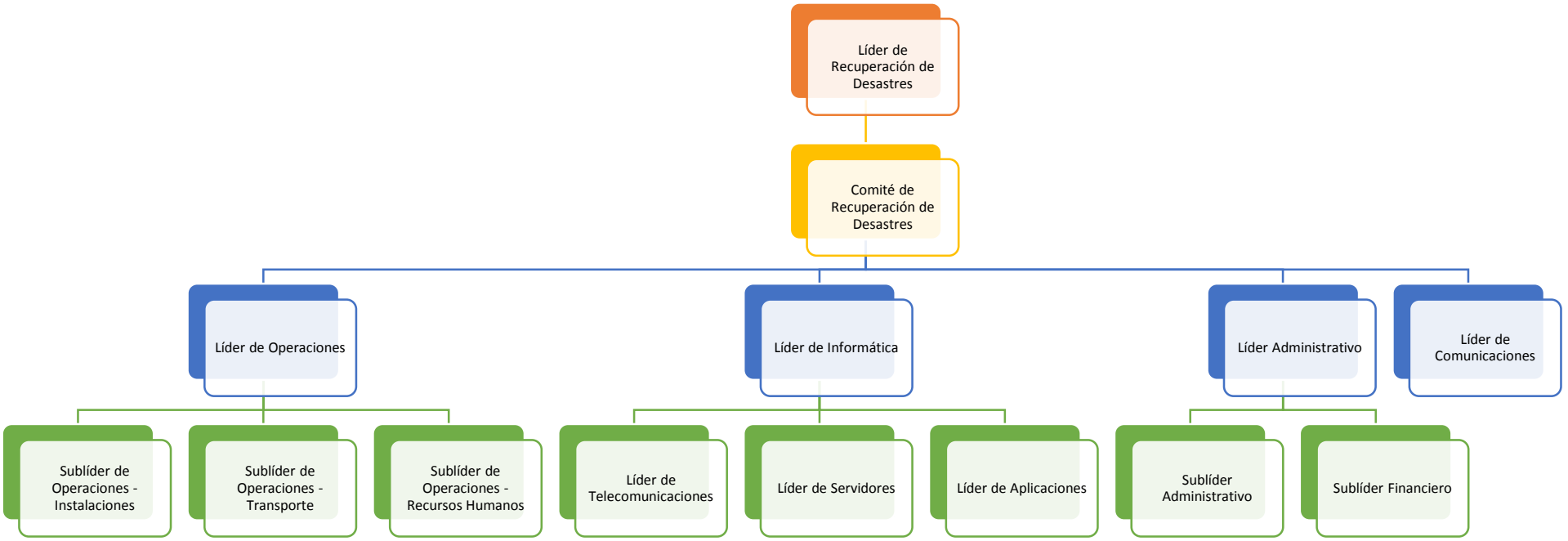
Información del Personal Involucrado

Al ocurrir un evento de desastre, diferentes equipos son necesarios para asistir a la Dirección de Tecnologías de Información para restaurar a la normalidad los servicios o procesos que brinda el Ministerio de Economía. Los líderes y sublíderes de estos equipos se detallan a continuación:

Rol	Nombre/ Cargo	Teléfono Oficina	Correo electrónico	Personal Alterno
Principales/ Miembros del Comité de Recuperación de Desastres				
Líder de Recuperación de Desastres	Ing. Rafael Barrientos DIRECTOR DE TECNOLOGÍAS DE INFORMACIÓN	2590-5431	rbarrientos@minec.gob.sv	Lic. Tharsis Salomón López MINISTRO DE ECONOMÍA
Líder de Operaciones	Ing. Jorge Alberto Posada DIRECTOR DE ADMINISTRACIÓN Y FINANZAS	2590-5676	gadmon@minec.gob.sv	Ing. Gloria Flores JEFE DE MANTENIMIENTO
				Ing. Delmo Blanco JEFE DE TRANSPORTE
				Licda. Guadalupe de Salazar GERENTE DE RECURSOS HUMANOS
Líder de Informática	Ing. Leonel Jiménez GERENTE DE INFORMÁTICA	2590-5529	ljimenez@minec.gob.sv	Ing. Orlando Arbaiza GERENTE DE SEGURIDAD Y TELECOMUNICACIONES
Líder de Telecomunicaciones /Líder de Servidores	Ing. Mario Pastori JEFE DE INFRAESTRUCTURA Y SOPORTE TÉCNICO	2590-5530	mpastori@minec.gob.sv	Ing. Mauricio Morales JEFE UNIDAD INFORMATICA HIDROCARBUROS
				Ing. Noel Navas JEFE DE DESARROLLO DE SISTEMAS
Líder de Aplicaciones	Ing. Noel Navas JEFE DE DESARROLLO DE SISTEMAS	2590-5520	nnavas@minec.gob.sv	Lic. Ernesto Lizano ANALISTA DE SISTEMAS
Líder Administrativo	Lic. Ángel Mario Vega GERENTE DE ADMINISTRACION	2590-5674	avega@minec.gob.sv	Licda. Marta Catalina de Menjívar JEFE DE DIVISIÓN DE OPERACIONES
				Lic. Wilfredo Mauricio GERENTE FINANCIERO
Líder de Comunicaciones	Lic. Liza Rocío Onofre GERENCIA DE COMUNICACIONES Y RR.PP	2590-5843	lonofre@minec.gob.sv	Lic. Armando Flores MINISTRO DE ECONOMÍA
Alternos				

Sublíder de Recuperación de Desastres	Lic. Tharsis Salomón López MINISTRO DE ECONOMÍA	2590-5283	tlopez@minec.gob.sv	
Sublíder de Operaciones - Instalaciones	Arq. Gloria Flores JEFE DE MANTENIMIENTO	2590-5640	gflores@minec.gob.sv	
Sublíder de Operaciones - Transporte	Ing. Delmo Blanco JEFE DE TRANSPORTE	2590-5643	dblanco@minec.gob.sv	
Sublíder de Operaciones -Recursos Humanos	Licda. Guadalupe de Salazar GERENTE DE RECURSOS HUMANOS	2590-5650	gsalazar@minec.gob.sv	
Sublíder de Informática	Ing. Orlando Arbaiza GERENTE DE SEGURIDAD Y TELECOMUNICACIONES	2590-5535	oarbaiza@minec.gob.sv	
Sublíder de Telecomunicaciones	Ing. Mauricio Morales JEFE UNIDAD INFORMATICA HIDROCARBUROS	2590-5536	mmorales@minec.gob.sv	
Sublíder de Aplicaciones	Lic. Ernesto Lizano ANALISTA DESARROLLADOR	2590-5538	elizano@minec.gob.sv	
Sublíder Administrativo	Licda. Morena de Cabrera GERENTE DE ADMINISTRACION	2590-5677	mcabrera@minec.gob.sv	
Sublíder Financiero	Lic. Wilfredo Mauricio GERENTE FINANCIERO	2590-5678	wmauricio@minec.gob.sv	

Su orden jerárquico se detalla a continuación:



La descripción de los Roles y Responsabilidades están descritos en el Anexo 1.

Evaluación de la Emergencia

Se cuenta con 5 elementos primarios para activar el DRP:

1. Criterio de activación: Identificar las condiciones de desastre específicos que desencadenan la activación del plan.
    a. Desastre natural con afectación total.
    b. Desastre natural con afectación parcial.
    c. Incendio total
    d. Incendio parcial en el centro de datos
    e. Vandalismo local
    f. Ataque cibernético
    g. Fallas eléctricas prolongadas

2. Procedimiento de evaluación: Para evaluar los posibles eventos de desastre a fin de asegurar que se han cumplido los criterios de activación.

    En situaciones de emergencia la persona de mayor jerarquía en la cadena de mando que esté presente o en comunicación por cualquier vía:
    a. Asumirá el mando y la responsabilidad;
    b. Iniciará las acciones necesarias de acuerdo con el Plan;
    c. Se comunicará con una persona de mayor jerarquía en la cadena de mando;
    d. Convocará a una reunión al Comité de Desastre.
3. Mecanismos de aprobación: Para obtener las aprobaciones adecuadas para la activación del plan, teniendo en cuenta al personal técnico, mandos medios y autoridades.

    El Líder de Recuperación de Desastres se encargará de analizar y clasificar la emergencia a fin de informar a todo el Comité de Recuperación de Desastres la situación, pudiendo sugerir de ser necesario la activación de plan de recuperación.

4. Logística de activación: Para asegurar que todas las instalaciones y los sistemas estén disponibles cuando sea necesario activar el plan, incluyendo la ubicación del centro de operaciones para emergencias donde se tomarán la mayoría de decisiones y se realizarán tareas de recuperación.

    Luego de activar el plan es responsabilidad del Líder de Recuperación de Desastres coordinar con los diferentes equipos la puesta en marcha del plan, además de garantizar que todos los sistemas en el sitio de contingencia respondan como se planificó.

5. Procedimientos de comunicación: Para informar a todos los empleados y otras partes interesadas (clientes, proveedores, proveedores, el público) de todas las decisiones y actividades relacionados con la activación.

Procedimientos de Recuperación de Desastres

El Líder de Recuperación de Desastres se encargará de coordinar la ejecución de los diferentes procesos posterior a la situación de desastre que haya interrumpido la operación de los procesos críticos. Los procesos se detallan a continuación:

1. Identificará los procesos críticos afectados.

2. Convocará al Comité de Recuperación de Desastres para evaluar la situación y decidirán si es necesaria la activación del Plan de Recuperación de Desastres.

3. En caso de que se decida ejecutar el Plan, los encargados de reestablecer los servicios en el Sitio Alterno, deben verificar y asegurar el buen funcionamiento de los equipos alternos tal como se detalla en Activación del Sitio Alterno.

4. Respecto a las actividades del Negocio, los Líderes de los Equipos de Desastre deben ejecutar las labores que se consideren necesarias de acuerdo a la situación de desastre.

5. Posterior a la situación de desastre, el Comité de Recuperación de Desastres deberá evaluar volver a las operaciones normales, por lo tanto debe ejecutar el Proceso de Reconstrucción.

   Así también, deberá solicitar a los Líderes de los Equipos de Desastre respectivos la elaboración de los informes de resultados de la ejecución del Plan, y se deberán evaluar posibles mejoras al Plan para optimización ante futuros desastres.

Sitio Alterno

El Ministerio de Economía debe contratar un Sitio de Alterno de contingencia lo suficientemente alejado del lugar donde se procesa la información, esto garantizará que ante una situación de desastre, que afecte la ubicación geográfica del sitio central, se pueda seguir proveyendo los procesos críticos del Negocio.

Es recomendable que el Sitio Alterno sea provisto por una empresa con experiencia en el área, ya que estas empresas trabajan y están regidas por normas y estándares internacionales para asegurar las operaciones de sus clientes.

El Sitio Alterno deberá contar como mínimo con los siguientes aspectos:

- Telecomunicaciones: Cableado de armarios y horizontal, accesos redundantes, cuarto de entrada, área de distribución, backbone, elementos activos y alimentación redundantes, patch panels y patch cord, documentación.
- Arquitectura: Selección de ubicación, tipo de construcción, protección ignífuga y requerimientos NFPA 75(Sistemas de protección contra el fuego para información), barreras de vapor, techos y

pisos, áreas de oficina, salas de UPS y baterías, sala de generador, control de acceso, CCTV, NOC (Network Operations Center – Centro operativo).

- Sistema eléctrico: Número de accesos, puntos de fallo, cargas críticas, redundancia de UPS y topología de UPS, puesta a tierra, EPO (Emergency Power Off- sistemas de corte de emergencia) baterías, monitorización, generadores, sistemas de transferencia.
- Sistema mecánico: Climatización, presión positiva, tuberías y drenajes, CRACs y condensadores, control de HVAC (High Ventilating Air Conditionning), detección de incendios y sprinklers, extinción por agente limpio (NFPA 2001), detección por aspiración (ASD), detección de líquidos.

Estas características están basadas en la TIA-942, el cual es un estándar de telecomunicaciones e infraestructura para centros de datos.

Respecto al nivel de fiabilidad del Sitio Alterno, un centro de datos es medido por uno de los cuatro niveles de fiabilidad existentes llamados TIER, este nivel viene dado en función de la redundancia del centro de datos. A mayor número de TIER, mayor disponibilidad, y por tanto mayor costo de construcción y mantenimiento.

TIER	% Disponibilidad	% Parada	Tiempo anual de parada
TIER I	99,67%	0,33%	28,82 horas
TIER II	99,74%	0,25%	22,68 horas
TIER III	99, 982 %	0,02%	1,57 horas
TIER IV	100,00%	0,01%	52,56 minutos

Para el Sitio Alterno del Ministerio de Economía se recomienda que este en el nivel de TIER II como mínimo. El TIER II, presenta las siguientes características:

- Disponibilidad del 99,741 %.
- Menor sensibilidad a las interrupciones.
- Un solo pasó de corriente y distribución de aire acondicionado, con un componente redundante.
- Incluye piso elevado, UPS y generador.
- Plazo de implementación: 3 meses.
- Tiempo de inactividad anual: 28,82 horas.
- Plazo de implementación: 3 a 6 meses.
- Tiempo de inactividad anual: 22,0 horas.
- El mantenimiento de la alimentación y otras partes de la infraestructura requieren de un cierre de procesamiento.

Activación de Sitio Alterno

Después de haber activado el Plan de Recuperación de Desastres los Equipos de Desastres encargados de restablecer los procesos críticos del Negocio en el Sitio Alterno, deben:

- Verificar y asegurar el buen funcionamiento de los equipos del Sitio Alterno.

- Verificar que la replicación de la información se haya realizado correctamente o si existe la necesidad de restaurar un respaldo previo.
- Verificar que las aplicaciones contengan sus debidas actualizaciones o si existe la necesidad de actualizarlas.
- Coordinar con los proveedores el enrutamiento al Sitio Alterno de operaciones.

Una vez el Sitio Alterno haya iniciado su funcionamiento, los Equipos de Desastres encargados deben efectuar el monitoreo en sus áreas correspondientes, los cuales se detallan a continuación:

Equipo	Tarea
Equipo de Telecomunicaciones	Monitorear el acceso a los servicios y que este se realice en niveles aceptables.
Equipo de Servidores	Verificar que el rendimiento de los equipos cumpla con las condiciones mínimas de uso.
Equipo de Aplicaciones	Monitorear que las aplicaciones respondan adecuadamente.

En caso de existir alguna falla en cualquier área, el Equipo afectado se encargará de solventarla o escalarla de acuerdo a su necesidad.

Proceso de Reconstrucción

Para retornar las operaciones a su normalidad se seguirá el siguiente proceso:

1. Se esperará a que el Equipo de Operaciones dé el aval de entrar al Centro de Datos, en caso de ser seguro. Si no es seguro, el Equipo de Operaciones debe coordinar con el Gobierno Central la reubicación hacia nuevas instalaciones.

2. El Equipo de Servidores, Telecomunicaciones y Aplicaciones evaluarán el daño causado y en caso de ser necesario coordinará con el Equipo Administrativo la compra de nuevos equipos.

    a. Cada Equipo de Informática deberá proponer una solución de la restauración de sus áreas.
    b. El Líder de Informática será el encargado de unificar los requerimientos y presentar un presupuesto para la reconstrucción de la infraestructura tecnológica.
    c. El Equipo Administrativo Financiero ejecutará la compra de la infraestructura necesaria.

    Asimismo, en el caso que el sitio original debe ser restaurado o reemplazado, evaluarán:
    a. La disponibilidad proyectada de todo el equipo informático necesario.
    b. La eficacia y eficiencia de actualizar los sistemas informáticos con equipos más modernos.
    c. El tiempo estimado necesario para la reparación o construcción del Centro de Datos.

3. El Equipo de Telecomunicaciones, Servidores y Aplicaciones procederán a iniciar los servidores, bases de datos, telecomunicaciones y demás servicios informáticos afectados durante la situación desastre para volver a la operación normal.
    a. El Equipo de Telecomunicaciones se encargará de velar porque la red esté funcionando de acuerdo al diagrama de red.
    b. El Equipo de Servidores será el encargado de la instalación física de los servidores y su correcto funcionamiento.
    c. El Equipo de Aplicaciones será el encargado de la instalación de los Sistemas Operativos y la configuración de todas las aplicaciones de acuerdo al plan de distribución de aplicaciones.

Probar el Plan de Recuperación de Desastres

Las pruebas sobre el Plan de Recuperación de Desastres deberán realizarse por lo menos 1 vez al año para garantizar el correcto funcionamiento del mismo.

Mantenimiento y Mejora Continua

Este documento deberá ser revisado anualmente o al ser requerido, por el Despacho Ministerial (Alta Gerencia) junto con el Director de Tecnologías de Información, quien a su vez deberá revisarlo con todo el personal involucrado en los planes de acción, con el fin de establecer su actualización, vigencia y ajuste de acuerdo con los requerimientos del Negocio, resultados obtenidos en las pruebas del Plan de Recuperación de Desastres, y adecuación ante nuevas necesidades para garantizar que continúe siendo adecuado, suficiente y eficaz.

Anexos

Anexo1: Equipos de Desastre

Los roles y responsabilidades de los Equipos de Desastre se detallan a continuación, sin embargo antes de continuar es de notar que en cualquier momento durante el desastre los miembros de los equipos pueden ser llamados a realizar tareas diferentes a las descritas en esta sección. Además, se recomienda que los Líderes de Equipo no sean miembros de ningún otro equipo.

Equipo de Desastre	Descripción	Roles y Responsabilidades
Comité de Recuperación de Desastres	Es responsable de supervisar todo el proceso de recuperación de desastres. Es el primer equipo que tendrá que tomar medidas en el caso de un desastre. Este equipo evaluará el desastre y determinará los pasos a seguir para que la organización vuelva a la normalidad.	• Pone en marcha el DRP, luego que el Líder de Recuperación de Desastres ha declarado el desastre. • Declara la magnitud y la clase del desastre. • Determina que sistemas y procesos se han visto afectados por el desastre. • Comunica el desastre al resto de equipos. • Determina los primeros pasos a tomar por los equipos. • Mantiene alineados a los equipos con actividades y expectativas predeterminadas. • Mantiene un registro del dinero gastado durante el proceso de Recuperación de Desastres. • Se asegura que todas las decisiones adoptadas sean acordes al DRP y las políticas internas del MINEC. • Se asegura que el Sitio Alterno sea completamente funcional y seguro.
Líder de Recuperación de Desastres	Es responsable de tomar todas las decisiones relacionadas a la recuperación ante un desastre. Su principal función es la de guiar los procesos de recuperación de desastres, todos los individuos involucrados en la gestión de recuperación ante desastres le deben reportar a él, en caso un desastre ocurra, sin importar el departamento al que pertenezcan o sus gerentes directos.	• Determinar que un desastre ha ocurrido y disparar el DRP y los procesos relacionados. • Ser el único punto de contacto que supervise a todos los equipos de Desastre. • Organizar y presidir reuniones regulares con los Líderes de los equipos de Desastre a lo largo del Desastre. • Presentar al Comité de Recuperación de Desastres el estado del Desastre e informar sobre las decisiones que se deben tomar.

Equipo de Desastre	Descripción	Roles y Responsabilidades
	Se debe hacer el esfuerzo para asegurarse que el Líder este separado y no pertenezca a ningún equipo de gestión de desastres para mantener sus decisiones imparciales.	
Equipo de Operaciones	Es responsable de proveer a los empleados de la institución las herramientas o equipo necesario para realizar sus labores, de la manera más rápida y eficiente como sea posible. Incluso cuando los empleados deban hacer sus funciones fuera de la institución. Además, debe solventar cualquier problema que exista con las instalaciones físicas de la institución, priorizando las instalaciones que soporten los procesos críticos de la institución y ayudar al personal a funcionar bien.	• Identificar y mantener los suministros (herramientas, equipos, etc.) necesarios que se pueden requerir ante un desastre. • Priorizar la entrega de suministros al personal según su rol y funciones que ejecuten dentro del proceso. • Asegurarse que las herramientas o equipos sean suministrados apropiadamente al personal correspondiente. • Asegurarse que el equipo que es entregado contenga las herramientas o software que se vayan a utilizar según el rol de la persona. • Llevar una bitácora de las personas a las que se les entrega el equipo. • Asegurar que las instalaciones estén en orden. • Gestionar el transporte de los empleados. • Asegurar que los equipos tengan suficiente comida, bebida y otro tipo de suministros. • Trabajar con las compañías de seguro para valer las pólizas.

Líder de Informática	Es responsable de asegurar que todos los equipos de trabajo de informática se comuniquen entre sí para lograr restaurar los servicios en el tiempo estipulado previamente.	• Sirve de mediador entre los diferentes equipos informáticos para resolver conflictos en un momento de crisis.
		• Administra los equipos de:
		  ○ Telecomunicaciones
		  ○ Servidores
		  ○ Aplicaciones

Equipo de Telecomunicaciones	Es responsable de la evaluación de daños específicos a la infraestructura de red así como la verificación de servicios de voz y datos incluyendo WAN, LAN y conexiones telefónicas internas y externas. Su responsabilidad primaria será proveer	• En el caso de un desastre que no requiera moverse al sitio de recuperación (Sitio Alterno), el equipo de telecomunicaciones determinará qué servicios de red no están funcionando en el sitio del desastre. • Si varios servicios de red fueron afectados, el equipo priorizara la

Equipo de Desastre	Descripción	Roles y Responsabilidades
	interconexiones a fin de asistir a otros equipos IT en la recuperación ante desastre.	recuperación de servicios de manera que tenga menor impacto para la institución. • Si los servicios de red son provistos por terceras partes, el equipo se comunicara y coordinara con las terceras partes a fin de asegurar el restablecimiento de la conectividad. • En caso de un desastre que requiera mover los servicios al sitio de contingencia el equipo se asegurara que todos los servicios de red se encuentren disponibles. • Una vez los servicios críticos han sido restablecidos, los empleados dispondrán de conectividad de acuerdo al siguiente orden: ○ Todos los miembros de los equipos de incidentes ○ Las altas autoridades ○ Los empleados de TI ○ El resto de empleados • Instalar e implementar cualquier herramienta, hardware, software y Sistema requerido en el Sitio Alterno. • Instalar e implementar cualquier herramienta, software y Sistema requerido en el sitio principal. • Después que el Ministerio de Economía vuelva a la normalidad en la prestación de servicios, este equipo contabilizara los costos y proveerá un reporte de todas las actividades realizadas durante el desastre.
Equipo de Servidores	Es responsable de proveer la infraestructura física requerida para ejecutar las operaciones de TI durante un desastre. Este equipo será el responsable principal de mantener la funcionalidad en servidores y pueden ayudar a otros equipos de TI según se necesite.	• Durante un desastre que no requiere migración al sitio de contingencia, el equipo determinará cuales servidores no son funcionales en el sitio primario. • Si múltiples servidores son afectados, el equipo deberá priorizar la recuperación de los equipos de manera que cause menos impacto a la institución. La recuperación deberá incluir: ○ Evaluación del daño de los equipos ○ Reinicio de servidores de ser necesario • Garantizar que los equipos virtuales o físicos ubicados en el sitio de contingencia se encuentren actualizados y con los parches de seguridad debidamente aplicados.

Equipo de Desastre	Descripción	Roles y Responsabilidades
		• Garantizar que las bases de datos del sitio de contingencia se encuentren sincronizadas y permitan el restablecimiento de los servicios según lo planificado. • Garantizar la continuidad del Sitio Alterno con la creación de respaldos mientras dure su operación. • Asegurar que todos los servicios que se ejecuten en el Sitio Alterno cumplan con las políticas establecidas. • Instalar e implementar cualquier herramienta, hardware, software y Sistema requerido en el Sitio Alterno. • Instalar e implementar cualquier herramienta, software y Sistema requerido en el sitio principal. • Después que el Ministerio de Economía vuelva a la normalidad en la prestación de servicios, este equipo contabilizara los costos y proveerá un reporte de todas las actividades realizadas durante el desastre.
Equipo de Aplicaciones	Es responsable de asegurar que todas las aplicaciones y servicios de la institución que están soportados sobre las aplicaciones funcionen para cumplir con los objetivos que el negocio requiere durante y después de un desastre. Además de validar, asegurar y garantizar un rendimiento apropiado de las aplicaciones.	• Identificar que las aplicaciones que soportan los procesos críticos del Negocio estén en correcto funcionamiento. • Si alguna o varias de las aplicaciones no se encuentra funcionando como el Negocio lo requiere, es necesario priorizar en función del BIA la recuperación y la estabilización del servicio/aplicación. • Asegurar que el Sitio Alterno contenga la última versión o actualización de la aplicación. • Asegurar que el Sitio Alterno contenga la última versión o actualización de la información. • Realizar pruebas de rendimiento para garantizar el buen funcionamiento de las aplicaciones. • Indicar al Equipo de Servidores que la aplicación está instalada y configurada para que funcione correctamente. • Documentar las labores.
Equipo Administrativo	Es responsable de tomar cualquier decisión de negocios que esté fuera de alcance del Líder de Recuperación de	• Asegurar que el Comité de Recuperación de Desastres rinda cuentas sobre el desempeño de su rol. • Asistir al Líder de Recuperación de Desastres en las

Equipo de Desastre	Descripción	Roles y Responsabilidades

	Desastres. Decide sobre la construcción de un nuevo centro de datos, reubicación del sitio primario, ente otros.
	
	Además, es responsable de asegurar que las finanzas del MINEC sean tratadas en forma adecuada y oportuna en caso de que ocurra un desastre. El equipo financiero se asegurará que exista dinero disponible para los gastos necesarios que resulten del desastre, así como los gastos de las funciones de negocio que se realizan día con día.
		responsabilidades de su rol, según se requiera.
		• Tomar decisiones que impactarán la organización. Esto puede incluir decisiones tales como:
		  ○ Reconstrucción de las instalaciones principales.
		  ○ Reconstrucción del centro de datos.
		• Inversiones significativas en Hardware, Software y actualizaciones.
		• Asegurar disponibilidad suficiente de dinero efectivo o mecanismos accesibles para tratar pequeños gastos causados por el desastre.
		• Asegurar una disponibilidad de crédito o maneras accesibles de tratar gastos de mayor escala causados por el desastre. Esto incluye pagos para nuevos equipos, reparaciones de instalaciones primarias, etc.
		• Asegurar la planilla pago y que los empleados sean pagados normalmente, siempre que sea posible.
		• Comunicarse con los banqueros para obtener cheques, libros, etc. que se puedan llegar a necesitar para reemplazarlos como resultado del desastre.
		• Otras decisiones de negocio y financieras.

Equipo de Comunicaciones	Es responsable de toda la comunicación durante un desastre. Específicamente, ellos se comunicaran con los empleados del MINEC, clientes, proveedores, bancos, e incluso medios de comunicación de ser necesario.	• Comunicar a las autoridades del MINEC, a los empleados y clientes de la ocurrencia de un desastre y su correspondiente impacto. • Comunicar a los medios de comunicación, en caso de ser requerido, de la ocurrencia del desastre y su correspondiente impacto