UNIVERSIDAD DON BOSCO
VICERRECTORÍA ACADÉMICA
FACULTAD DE INGENIERÍA

TRABAJO DE GRADUACIÓN PARA OPTAR AL GRADO DE

Maestro(a) en Seguridad y Gestión de Riesgos Informáticos

PROYECTO

Sistema de gestión de seguridad de la información y ciberseguridad para SOLTEC El Salvador, S.A. de C.V.

PRESENTADO POR

Escobar Avilés, Víctor Manuel	*EA970014*
Esperanza Bonilla, Ricardo Ernesto	*EB212417*
Santos Marcia, Oscar Enrique	*SS211944*

ASESOR

Mg. Virgilio Reyes

Antiguo Cuscatlán, La Libertad, El Salvador, Centro América

Julio 2023

PARTE I

POLÍTICA PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

PAGINAS DE LA 3 A LA 25

SOLTEC El Salvador S.A. de C.V.

POLÍTICA PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Código:	001
Versión:	1.0
Fecha de la versión:	4-05-2020
Creado por:	Víctor Manuel Escobar Avilés Ricardo Ernesto Esperanza Bonilla Oscar Enrique Santos Marcia
Aprobado por:	Luis Enrique Sánchez Flores
Nivel de confidencialidad:	Alto

TÉRMINOS Y CONDICIONES DE USO

Versión actual del documento: 1.0

El contenido de este texto es PRIVADO y la presente versión se considera un documento interno de trabajo.

NO SE AUTORIZA LA REPRODUCCIÓN O DIFUSIÓN POR NINGÚN MEDIO O MECANISMO SIN EL DEBIDO CONTROL Y AUTORIZACIÓN DE LA GERENCIA DE SOLTEC EL SALVADOR S.A. DE C.V.

Tabla de contenido

1. Introducción..... 5

2. Objetivo. 7

3. Alcances de la política de seguridad..... 8

4. Organización. 9

5. Responsabilidades 10

5.1. Junta Directiva. 10

5.2. Gerencia General. 10

5.3. Departamento de tecnologias de la informacion. 11

5.4. Centro de Monitoreo. 11

6. Identificacion, clasificacion y valoracion de activos de informacion. 11

7. Seguridad de la informacion en el Recurso Humano. 12

7.1. Responsabilidad de los empleados. 12

7.2. Responsabilidad de usuarios externos. 12

7.3. Responsabilidad de proveedores. 13

8. Seguridad Fisica y del entorno. 13

8.1. Acceso. 13

8.2. Seguridad de los equipos. 13

9. Administracion de las comunicaciones y operaciones 14

9.1. Reporte e investigacion de incidentes de seguridad. 14

9.2. Proteccion contra malware y brechas en la seguridad. 15

9.3. Respaldos de informacion. 17

9.4. Administracion de configuraciones de red. 17

9.5. Intercambio de informacion con dependencias de gobierno. 17

9.6. Uso de internet y otros servicios. 18

9.6.1. Acceso a internet. 18

9.6.2. Servicio de correo electronico 18

9.7. Instalacion de software. 19

10. Control de acceso. 20

10.1. Niveles de acceso. 20

10.2. Control de credenciales. 20

10.3. Dispositivos Móviles. 20

10.3.1. Operador de Centro de Monitoreo. 21

10.3.2. Administracion. 21

10.3.3. Entidades Externas. 21

10.4. Seguimiento del uso de los recursos tecnologicos. 21

10.5. Acceso Remoto. 21

11. Gestion de activos de información. 21

12. Seguro contra daños. 22

13. Tercerizacion de suministro y servicios criticos. 22

14. Adquisicion y mantenimiento de sistemas de software. 22

15. Administracion y continuidad del negocio. 23

1. Introducción.

Debido al aumento en la delincuencia común y el crimen organizado que experimentó nuestro país durante la última década, muchas de nuestras ciudades se vieron en la necesidad de reforzar las políticas de seguridad mediante la ejecución de programas que velaran por el bienestar de los ciudadanos y de esta forma, mejorar la imagen política del alcalde en funciones y su partido político. Estas municipalidades han reorientado muchos de los recursos económicos disponibles, para fortalecer la seguridad ciudadana, en detrimento de otros servicios, tales como el de iluminación publica, pavimentación, recolección de desechos, etc.

Uno de los programas más comunes realizados por las municipalidades, es la implementación de sistemas de video vigilancia, mediante la creación de sociedades de economía mixta entre la municipalidad y empresas privadas, estableciendo un contrato por servicios administrados. Estos sistemas de video vigilancia, con énfasis en las áreas llamadas “rojas” o de alta actividad criminal, usualmente están compuestos por: decenas o incluso, cientos de cámaras de video, instaladas en las calles y avenidas más importantes de la ciudad, una red de transmisión de datos, un centro de datos donde se recibe toda la información y un centro de monitoreo con estaciones de trabajo, cuya principal función, es la de observar continuamente, reaccionar y coordinar con las diferentes dependencias de gobierno (Policía nacional civil, Cuerpo de agentes metropolitanos, Viceministerio de transporte, Fiscalía general de la república, entre otras.) ante cualquier incidente o acto criminal observado mediante este sistema.

Para poder dar soporte a estos sistemas, es necesaria la adquisición, instalación y configuración de equipos de tecnología de la información, tales como servidores, routers, switches, firewall, unidades de almacenamiento. Todos estos dispositivos, compuestos tanto de hardware como de software, cuentan con vulnerabilidades

inherentes a cada uno de ellos, que introducen riesgos que amenazan la confidencialidad, disponibilidad e integridad de la información, lo cual podría suponer multas, pérdida de confianza e incluso, terminación de contrato, resultando en pérdidas económicas para la empresa que realizó la inversión.

Es por esto, que se hace necesaria una política de seguridad que reduzca el riesgo de un accidente de información, tratando de cubrir todos los aspectos relacionados a la información tanto generada como recibida durante las operaciones diarias.

2. Objetivo.

La presente política para la gestión de la seguridad de la información tiene como objetivo reducir el riesgo de un accidente que pueda afectar la confidencialidad, integridad y disponibilidad de la información generada y recibida por la empresa SOLTEC El Salvador.

3. Alcances de la política de seguridad.

Esta politica es de aplicación para:

- El conjunto de dependencias que componen la empresa SOLTEC El Salvador y sus recursos.

- Todo el personal de la empresa SOLTEC El Salvador, cualquiera que sea su situacion contractual, la dependencaia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe.

- Las entidades de gobierno que hacen uso de los servicios de video vigilancia prestados por la empresa SOLTEC El Salvador.

- Los proveedores de servicios que dan soporte a los procesos de la empresa a traves de contratos o acuerdos.

4. Organización.

A continuacion se muestra el organigrama de la empresa SOLTEC El Salvador S.A de C.V.

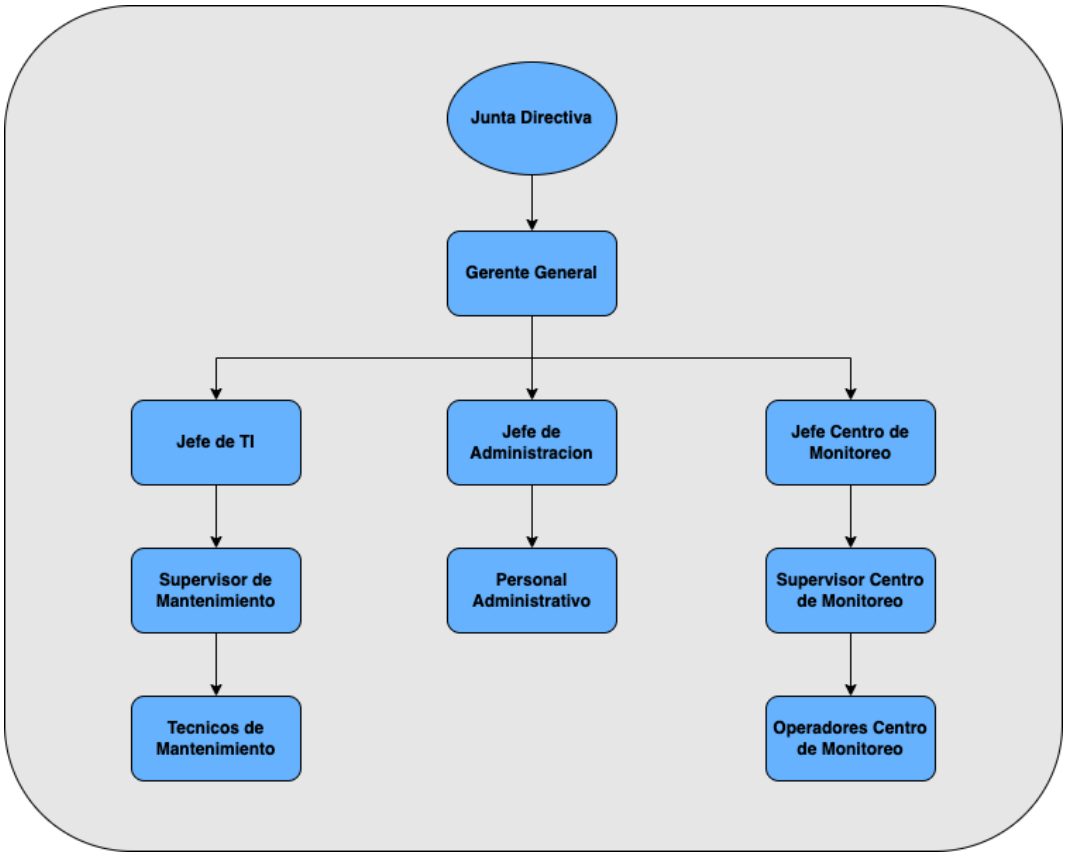


Ilustración 1 Organigrama de la Empresa

5. Responsabilidades

5.1. Junta Directiva.

Será la responsable de establecer un adecuado gobierno y gestión de la seguridad de la información por lo que deberá realizar como mínimo lo siguiente:

- Aprobar los recursos necesarios para el establecimiento, implementación, monitoreo y mantenimiento de la gestión de la seguridad de la información, a fin de contar con la infraestructura, metodología, tácticas y personal apropiados. Asimismo, deberá nombrar a una persona responsable de gestionar la seguridad de la información, el cual tendrá una comunicación permanente y directa con la Alta Gerencia, quien a su vez informará directamente a la Junta Directiva.
- Aprobar los programas de seguridad de la información.

5.2. Gerencia General.

Para implementar la gestión de la seguridad de la información conforme a las disposiciones de la Junta Directiva, la Alta Gerencia de las entidades deberá realizar al menos lo siguiente:

- Apoyar el programa de seguridad de la información.
- Promover la mejora de los programas de seguridad de la informacion y ciberseguridad y velar por su vigencia permanente.
- Apoyar al responsable de la seguridad de la información en la ejecución de estrategias y tácticas de seguridad de la información requeridas, ante un incidente de seguridad de la información.

5.3. Departamento de tecnologias de la informacion.

Encargado de llevar a cabo:

- La implementacion y ejecucion de los programas de seguridad de la informacion y ciber seguridad.
- Promover mejoras a los programas de seguridad de la informacion, tomando como criterio eventos y accidentes de la informacion observados en las operaciones diarias.
- El monitoreo del cumplimiento de las mismas por las diferentes areas.

5.4. Centro de Monitoreo.

Los miembros de este departamento, estan en la obligacion de cumplir todas las politicas de seguridad indicada por la alta gerencia.

6. Identificacion, clasificacion y valoracion de activos de informacion.

Cada una de las areas que componen la empresa, deben elaborar un inventario de los activos de informacion que poseen, tanto procesada como producida. Siendo dichas areas, las responsables de clasificar, valorar y ubicar esta informacion, asi como, controlar el acceso de la misma por entes ajenos al area propietaria.

La alta gerencia deberá aprobar el acceso a los activos de informacion de un area por parte de otra requiriente. Esta ultima debera justificar los motivos para el acceso a dicha informacion.

El area de tecnologías de la información, deberá además, realizar y mantener un inventario de los activos de los recursos de hardware y software de la institución.

7. Seguridad de la informacion en el Recurso Humano.

Todo el personal que labora en la empresa, independientemente de su situacion contractual, asi como del cargo que desempeñe, deberá tener un perfil de uso de los recursos de la información, incluyendo el hardware y software asociado. Es obligacion tanto del departamento de administracion como del centro de monitoreo, avisar de cualquier contratacion nueva o despido de personal, al departamento de tecnologias de información para garantizar el acceso a dichos recursos o removerlos según sea necesario.

7.1. Responsabilidad de los empleados.

Para que una persona pueda desempeñarse como empleado de la empresa, debe primero someterse a una serie de pruebas tales como:

- Prueba de poligrafo
- Examen psicologico
- Examen de aptitudes y conocimientos.
- Solvencia de antecedentes penales y otros documentos.

Esto para garantizar que las personas contratadas, puedan guardar la confidencialidad necesaria. Ademas, todos deben leer, comprender y firmar el “Acuerdo de confidencialidad” que les entregara el departamento de Recursos Humanos/Administracion.

7.2. Responsabilidad de usuarios externos.

Todos las personas que laboren en otras dependencias de gobierno ajenas a la empresa, tambien deben cumplir con las presentes politicas de seguridad de la informacion, las normas generales de conducta, asi como tambien, deben firmar el “Acuerdo de confidencialidad”.

7.3. Responsabilidad de proveedores.

Los proveedores de servicios tales como internet, mantenimiento de aires acondiciones deben leer, comprender y firmar el “Acuerdo de confidencialidad” para garantizar que lo que cualquier informacion que ellos puedan acceder durante su visitas a las oficinas, no sea divulgada a personas con intereses en dañar o desprestigiar a reputacion de la empresa.

8. Seguridad Fisica y del entorno.

8.1. Acceso.

Se debe controlar el acceso a las diferentes areas de la empresa, tales como:

- Islas de oficinas
- Centro de Monitoreo
- Cuarto de servidores

Para garantizar que solo las personas autorizadas por el departamento de recursos humanos, puedan ingresar a las oficinas, se deben contar con controles de acceso basados en datos biometricos tales como reconocimiento de rostros y/o tarjetas de acceso.

8.2. Seguridad de los equipos.

Los servidores y equipos de telecomunicaciones deben estar resguardados en un ambiente seguro y protegido con al menos los siguientes sistemas:

- Control de acceso biometrico
- Deteccion y control de incendios
- Control de humedad y temperatura
- Bajo riesgo de inundacion

- Sistemas de alimentacion ininterrumpidos tales como generadores de energia electrica y sistemas de respaldo (UPS)

Las estaciones de trabajo deben estar protegidas mediante sistema de respaldo como UPS y reguladores de energia. Así mismo, deben ser operadas por personal debidamente capacitado en el uso de los recursos.
Las camaras de video vigilancia instaladas en las calles y avenidas del municipio deben estar aseguradas mediante gabinetes metalicos con certificacion NEMA 4X, instalados a una altura suficiente para evitar vandalismo y asegurados mediante el uso de un sistema de llaves o cerraduras. Asi mismo, dentro del gabinete, al contarse con varios equipos conectados a la red de energia electrica comercial, debe hacerse uso de sistemas de proteccion tales como:

- Regulador de voltaje.
- Sistema de alimentacion de energia ininterrumpido (UPS).
- Protectores contra sobre voltajes.
- Protectores contra descargas electricas.
- Filtros contra particulas de polvo
- Ventiladores para evitar el sobrecalentamiento de los equipos.

9. Administracion de las comunicaciones y operaciones

9.1. Reporte e investigacion de incidentes de seguridad.

- Todos los empleados de la empresa deben reportar cualquier incidente o falta a estas politicas de seguridad de la informacion a la brevedad posible a su jefe inmediato. Este reporte debe ser manejado con discrecion por el personal que atiende el reporte y garantizar el anonimato del empleado que lo presentó.

- Las respectivas jefaturas estan obligadas a dar seguimiento e investigar el incidente, asi como tomar acciones de ser posible y necesario. En el caso de que el incidente involucre a personal de otras dependencias ajenas a la empresa, es necesario reportarlo a la gerencia general, quien deberá realizar las gestiones necesarias con la alcaldía municipal para llevar a cabo, las acciones y/o sanciones necesarias.
- Es la obligación del departamento de tecnologías de la información, tomar acciones correctivas, en caso de que estas sean posibles, tales como cambios en la configuracion, revocacion de accesos, limitar privilegios, etc. Asi mismo, tambien es obligacion de la gerencia general, la de proveer los recursos necesario para la adquisicion de hardware y/o software necesario para reducir el riesgo de que el incidente de seguridad, ocurra nuevamente.

9.2. Proteccion contra malware y brechas en la seguridad.

- Todas las estaciones de trabajo deben implementar controles de seguridad de acuerdo a las buenas practicas conocidas, y la complejidad de estos controles, dependerán del departamento en que se encuentre en uso.
- Las estaciones de trabajo que componen el centro de monitoreo, deberan tener acceso limitado a la red y especificamente, no deberan contar con acceso a la internet, ni el uso de dispositivos USB tales como unidades de almacenamiento, modems para comunicación con redes moviles, etc. Tampoco se permitirá la instalacion de software no autorizado por el departamento de tecnologías de la información.
- Unicamente los usuarios que, por sus asignaciones laborales asi lo requieran, podrán contar con acceso a internet y este deberá ser

solicitado formalmente por el jefe del departamento requiriente. Las estaciones de trabajo que no pertenezcan al centro de monitoreo, podrán contar con aplicaciones de software según las necesidades de cada empleado, pero deberan solicitar autorizacion al departamento de tecnologías de la informacion, quienes deberán validar que dicha aplicación es de utilidad para las labores encargadas al usuario de dicho equipo.

- No se permitira el uso, ni tenencia de dispositivos de comunicación movil tales como telefonos moviles celulares, tablets, etc., dentro del centro de monitoreo por parte de los operadores del mismo. Las unicas terminales móviles autorizadas deberán ser las proporcionadas por la empresa para comunicación con otros departamentos y entidades de gobierno y estaran asignadas al supervisor en turno y al jefe de area.
- Se podrá autorizar el uso de dispositivos moviles tales como telefonos moviles, a aquellos usuarios del centro de monitoreo que pertenecen a otras entidades de gobierno, tales como PNC, VMT, y CAM, siempre y cuando, cada una de estas dependencias realice la solicitud formal a la alcaldia municipal y sea esta ultima, quien haga la solicitud a la gerencia general. Adicionalmente, ambas partes deben firmar el acuerdo de confidencialidad establecido para garantizar el buen uso de dichos dispositivos dentro de la instalaciones de la empresa.

9.3. Respaldos de informacion.

- Es necesaria la Implementacion de un sitio de contingencia, que permita mantener la operación en funcionamiento durante un siniestro o incidente.
- Se deberá contar con un sistema de respaldo asignado al jefe del centro de monitoreo, con el objetivo que este lleve a cabo respaldos de la informacion considerada evidencia y que podría ser solicitada por las entidades de gobierno.

9.4. Administracion de configuraciones de red.

La configuración de enrutadores, switches, firewall, sistemas de detección de intrusos y otros dispositivos de seguridad de red; debe ser documentada, respaldada por copia de seguridad y mantenida por el departamento de tecnologías de la informacion de SOLTEC El Salvador.

Todo equipo informático debe ser revisado, registrado y aprobado por el departamento de tecnologias de la informacion de SOLTEC El Salvador, antes de conectarse a la red de datos de la empresa. Dicha dependencia debe desconectar aquellos dispositivos que no estén aprobados y reportar tal conexión como un incidente de seguridad a ser investigado.

9.5. Intercambio de informacion con dependencias de gobierno.

El acceso a los archivos de video generados por el sistema de video vigilancia, deben ser solicitados mediante carta oficial por parte de cada una de las dependencias de gobierno (FGR, PNC, VMT, Municipalidad, etc) y dirigidas al gerente de operaciones y al jefe del centro de monitoreo. Esta solicitud debe indicar el numero de archivo, en el caso que se requiera como evidencia de un acto penalizable por la ley y que puede ser considerado como evidencia.

Toda la informacion compartida con las diferentes dependencias de gobierno, debe ser cifrada para garantizar la confidencialidad e integridad de los archivos.

9.6. Uso de internet y otros servicios.

El acceso a internet y sus servicios dependerá del departamento para el cual, labore el empleado, de acuerdo a las siguientes condiciones:

9.6.1. Acceso a internet.

- Operadores del centro de monitoreo: no deberan tener acceso al servicio de internet desde los ordenadores de trabajo asignados.
- Supervisores del centro de monitoreo: Estos podrán contar con acceso a internet, seguiendo las normas de uso, establecidas por el jefe del centro de monitoreo, tales como evitar el uso de redes sociales, paginas deportivas, servicios de video en vivo, etc.
- Empleados administrativos: Solo aquellos empleados, que sus labores asi lo requiran, deberán contar con acceso a internet, siguiendo las normas de uso establecidas en el manual de operaciones.
- Entidades externas: Los usuarios pertenecientes a estas entidades, podrán contar con acceso a internet, cumpliendo las normas de uso establecidas en el manual de operaciones. Este acceso sera revisado y aprobado por el departamento de tecnologías de la información, a solicitud de la gerencia de operaciones.

9.6.2. Servicio de correo electronico

- Operadores del centro de monitoreo: Unicamente podran contar con servicio de correo electronico interno y para uso de sus labores diarias.

- Supervisores del centro de monitoreo: Estos podran contar con una cuenta de correo electronico para comunicarse con las diferentes areas de la empresa, asi como las dependencias externas.
- Empleados administrativos: Unicamente aquellos empleados, que sus tareas asignadas asi lo requieran, deberan contar con una cuenta de correo electrónico siguiendo las normas de uso establecidas en el manual de operaciones.
- Entidades Externas: Los usuarios de la red pertenencientes a otras dependencias, podran contar con una cuenta de correo electrónico interna para comunicación con los operadores de ser necesario y deberá ser solicitada por el jefe del centro de monitoreo al departamento de tecnologías de la información.

9.7. Instalacion de software.

- Unicamente el departamento de tecnologias de la informacion tendra autorización y privilegios de administracion para llevar a cabo la instalación de software en cualquiera de los ordenadores que componen la red de datos.
- El software instalado en los ordenadores usados por el personal de la empresa, será de acuerdo al perfil del usuario.
- El software instalado en los ordenadores usados por las diferentes entidades externas, deberá ser revisado y aprobado por el departamento de tecnologías de la información, a solicitud de la gerencia de operaciones.

10. Control de acceso.

10.1. Niveles de acceso.

El acceso a los recursos de tecnologías de la información de la empresa deberán estar restringidos según el cargo a desempeñar por el personal de la empresa, el cual deberá estar detallado en el manual de operaciones.

10.2. Control de credenciales.

- Unicamente el personal del departamento de tecnologias de la informacion, podrá contar con las credenciales para el acceso a los diferentes equipos de red, servidores, sistemas de software, etc.
- Unicamente el departamento de tecnologias de la informacion podrá generar, renovar y cancelar las credenciales necesarias para el acceso al sistema de gestion de video (VMS).
- Todas las credenciales deberan ser generadas, renovadas o eliminadas mediante solicitud generada por parte del encargado del departamento requiriente (centro de monitoreo, ventas, administracion, etc).
- Todas las credenciales deberan ser generadas siguiendo las buenas practicas para garantizar la seguridad de las mismas, tales como:
    - Longitud de la contraseña minima de 10 caracteres
    - Debe incluir al menos una letra Mayúscula
    - Debe incluir al menos 1 número
    - Debe incluir al menos 1 caractér especial.

10.3. Dispositivos Móviles.

El uso de dispositivos moviles dependerá del perfil del usuario, el cual estará establecido en el manual de operaciones.

10.3.1. Operador de Centro de Monitoreo.

Ningun operador del centro de monitoreo podrá hacer uso de dispositivos móviles durante el desarrollo de sus labores diarias.

10.3.2. Administracion.

Podrán hacer uso del servicio de internet, guardando las normas de uso establecidas en el manual de operaciones.

10.3.3. Entidades Externas.

Pueden hacer uso de dispositivos moviles dentro de las instalaciones de la empresa, asi como del centro de monitoreo, siempre y cuando sus funciones así lo requieran y este sea solicitado y aprobado por la gerencia de operaciones.

10.4. Seguimiento del uso de los recursos tecnologicos.

Se deberán establecer controles de acuerdo a las mejores practicas para dar seguimiento al acceso y uso de los recursos tecnologicos de la empresa.

10.5. Acceso Remoto.

El acceso remoto a los servicios de red, serán establecidos de acuerdo a las responsabilidades. Estos serán otrogados por el departamento de tecnologías de la información, a solicitud del gerente del area requiriente.

11. Gestion de activos de información.

El departamento de tecnologias de la informacion deberá mantener un inventario actualizado periodicamente de todos los activos de informacion de la empresa, asi como la siguiente informacion:

- Proveedor
- Fecha de compra
- Responsable del activo.

Asi mismo, la empresa debe garantizar la aplicación de los controles necesarios para garantizar la proteccion y resguardo de los mismos.

12. Seguro contra daños.

Debido a la naturaleza de las operaciones, la empresa deberá contar con un seguro contra daños y accidentes a los equipos informaticos y camaras de video vigilancia.

13. Tercerizacion de suministro y servicios criticos.

Todos los proveedores de bienes y/o servicios deberán firmar un acuerdo de confidencialidad y no divulgacion de informacion de la empresa para evitar riesgos a las operaciones y/o activos de informacion.

14. Adquisicion y mantenimiento de sistemas de software.

Para apoyar los procesos operativos y estratégicos la empresa, debe hacerse uso intensivo de las Tecnologías de la Información y las Comunicaciones. Los sistemas de software utilizados pueden ser adquiridos a través de terceras partes o desarrollados por personal propio.

El departamento de tecnologías de la información debe elegir, elaborar, mantener y difundir el “Método de Desarrollo de Sistemas Software” que incluya lineamientos, procesos, buenas prácticas, plantillas y demás artefactos que sirvan para regular los desarrollos de software internos en un ambiente de mitigación del riesgo y aseguramiento de la calidad.

Todo proyecto de desarrollo de software interno debe contar con un documento de Identificación y Valoración de Riesgos del proyecto. La emprese no debe emprender procesos de desarrollo – o mantenimiento – de sistemas software que tengan asociados riesgos altos no mitigados.

Los sistemas software adquiridos a través de terceras partes deben certificar el cumplimiento de estándares de calidad en el proceso de desarrollo.

15. Administracion y continuidad del negocio.

La Administración de Continuidad del Negocio debe ser parte integral del Plan de Administración de Riesgo de la empresa.

PARTE II

METODOLOGÍA DE EVALUACIÓN Y TRATAMIENTO DE RIESGOS

PAGINAS DE LA 27 A LA 88

SOLTEC El Salvador, S.A. de C.V.

METODOLOGÍA DE EVALUACIÓN Y TRATAMIENTO DE RIESGOS

Código:	002
Versión:	1.1
Fecha de la versión:	01-06-2023
Creado por:	Víctor Manuel Escobar Avilés Ricardo Ernesto Esperanza Bonilla Oscar Enrique Santos Marcia
Aprobado por:	Luis Enrique Sánchez Flores
Nivel de confidencialidad:	Alto

TÉRMINOS Y CONDICIONES DE USO

Versión actual del documento: 1.1

El contenido de este texto es PRIVADO y la presente versión se considera un documento interno de trabajo.

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
01/05/22	1.0	Vescobar	Creación del documento
01/06/23	1.1	Vescobar, Resperanza, Osantos	Modificaciones según requerimientos de gerencia.

Tabla de contenido

1. OBJETIVO, ALCANCE Y USUARIOS....4

2. DOCUMENTOS DE REFERENCIA....4

3. METODOLOGÍA DE EVALUACIÓN Y TRATAMIENTO DE RIESGOS....5

3.1. EVALUACIÓN DE RIESGOS....5

3.1.1. Organización....5

3.1.2. Activos, vulnerabilidades y amenazas....5

3.1.3. Impactos y probabilidades....8

3.1.4. Controles a implementar (ISO 27001 ver descripción del código Anexo 2)....18

4. ANEXOS....28

4.1. ANEXO 1: LISTADO DE AMENAZAS....28

4.2. ANEXO 2: AMENAZAS Y CONTROLES....31

4.3. ANEXO 3: LISTADO DE ACTIVOS DE TI QUE DAN SOPORTE A LOS PRODUCTOS INSTITUCIONALES....62

TABLAS

Tabla 1. Activos de datos....5

Tabla 2. Vulnerabilidades....6

Tabla 3. Amenazas (ver descripción del código Anexo 1)....7

1. Objetivo, alcance y usuarios

El objetivo del presente documento es definir la metodología para evaluar y tratar los riesgos de la información en SOLTEC El Salvador S.A. de C.V., empresa dedicada a la video vigilancia municipal y servicios de apoyo a la municipalidad, y definir el nivel aceptable de riesgo según la norma ISO/IEC 27001.

La evaluación y tratamiento de riesgos se aplica a todo el alcance del Sistema de gestión de seguridad de la información (SGSI); es decir, a todos los activos de información que se utilizan dentro de la organización o que pueden tener un impacto sobre la seguridad de la información en el ámbito del SGSI.

Los usuarios de este documento son todos los empleados de SOLTEC El Salvador S.A. de C.V. que participan en la evaluación y tratamiento de riesgos.

2. Documentos de referencia

- Norma ISO/IEC 27001, punto 4.2.1 c) y Anexo A
- Política para la gestión de la seguridad de la información y ciberseguridad
- Declaración de aplicabilidad

3. Metodología de evaluación y tratamiento de riesgos

3.1. Evaluación de riesgos

3.1.1. Organización

La evaluación de riesgos se implementa a través del Cuadro de evaluación de riesgos. El proceso de evaluación de riesgos es coordinado por Encargado de la seguridad de la información y la evaluación de riesgos para activos individuales es realizada por los propietarios de los activos.

3.1.2. Activos, vulnerabilidades y amenazas

Tabla 1. Activos de datos

N.º	Activo de datos	Responsable
1	Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	Jefaturas y Gerencia General
2	Finanzas	Unidad Financiera
3	Servicios bancarios	Unidad Financiera
4	RR. HH.	Unidad de Recursos Humanos
5	Productos Institucionales (Operaciones Tecnológicas, reportes de incidentes, archivos de video)	Unidad de Monitoreo
6	Correo Electrónico	Unidad de Tecnologías de la información
7	Base de datos internos	Unidad de Tecnologías de la información
8	Base de datos externa	Unidad de Tecnologías de la información
9	Respaldos	Unidad de Tecnologías de la información
10	Base de datos de contraseñas	Unidad de Tecnologías de la información

Tabla 2. Vulnerabilidades.

N.º	Activo de datos	Vulnerabilidad
1	Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	Fácil destrucción, sustracción y/o acceso a la Información. Información concentrada en un único punto.
2	Finanzas	Fácil acceso a la información, manejo inadecuado de fondos.
3	Servicios bancarios	Credenciales de acceso comprometidas.
4	RR. HH.	Información personal en físico.
5	Productos Institucionales (Operaciones tecnológicas, reportes de incidentes, archivos de video)	Video no cifrado. Sin control de reproducciones.
6	Correo Electrónico	Correo no cifrado.
7	Base de datos internos	Sistemas sin actualizar.
8	Base de datos externa	Información no cifrada. Medio de transmisión poco confiable.
9	Respaldos	Información no cifrada.
10	Base de datos de contraseñas	Unidad de Tecnologías de la información

Tabla 3. Amenazas (ver descripción del código Anexo 1)

N.º	Activo de datos	Amenazas
1	Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	A5, A8, A10, A11, A12, A16, A21, A22, A23, A24, A27, A29, A30, A38, A39, A41
2	Finanzas	A5, A8, A10, A11, A12, A16, A21, A22, A23, A24, A27, A29, A30, A38, A39, A41
3	Servicios bancarios	A5, A8, A10, A11, A12, A16, A21, A22, A23, A24, A27, A29, A30, A38, A39, A41
4	RR. HH.	A5, A8, A11, A16, A23, A24, A29
5	Productos Institucionales	A4, A5, A6, A8, A9, A10, A11, A12, A14, A15, A16, A20, A21, A22, A23, A24, A25, A27, A28, A29, A30, A31, A32, A33, A37, A38, A39, A40, A41, A42, A44, A45, A46, A47, A48.
6	Correo Electrónico	A9, A10, A11, A12, A22, A23, A24, A27, A29, A30, A39, A41
7	Base de datos internos	A5, A9, A10, A11, A12, A22, A23, A24, A27, A29, A30, A38, A39, A41, A45, A46, A47, A48
8	Base de datos externos	A24, A39, A45, A46
9	Respaldos	A24, A39, A45, A46
10	Base de datos de contraseñas	A24, A39, A45, A46

3.1.3. Impactos y probabilidades

1. Documentos Institucionales (Magnitud: 3)				
N.º	**Amenaza**	**Código Amenaza**	**Probabilidad de Amenaza**	**Riesgo**
1	**Daño por vandalismo**	**A5**	**3**	**9**
2	**Robo / Hurto (Físico)**	**A8**	**3**	**9**
3	**Intrusión a Red interna**	**A10**	**3**	**9**
4	**Infiltración**	**A11**	**3**	**9**
5	**Virus / Ejecución no autorizado de programas**	**A12**	**3**	**9**
6	**Sismo**	**A16**	**3**	**9**
7	**Falla de corriente (apagones)**	**A21**	**3**	**9**
8	**Falla de sistema / Daño disco duro**	**A22**	**3**	**9**
9	**Falta de inducción, capacitación y sensibilización sobre riesgos**	**A23**	**3**	**9**
10	**Mal manejo de sistemas y herramientas**	**A24**	**4**	**12**
11	**Perdida de datos**	**A27**	**3**	**3**
12	**Manejo inadecuado de datos críticos (codificar, borrar, etc.)**	**A29**	**3**	**3**

1. Documentos Institucionales (Magnitud: 3)				
N.º	**Amenaza**	**Código Amenaza**	**Probabilidad de Amenaza**	**Riesgo**
13	**Unidades portables con información sin cifrado**	**A30**	**3**	**3**

2. Finanzas (Magnitud de Daño: 3)				
N.º	**Amenaza**	**Código Amenaza**	**Probabilidad de Amenaza**	**Riesgo**
1	**Daño por vandalismo**	**A5**	**3**	**9**
2	**Robo / Hurto (Físico)**	**A8**	**3**	**9**
3	**Intrusión a Red interna**	**A10**	**3**	**9**
4	**Infiltración**	**A11**	**3**	**9**
5	**Virus / Ejecución no autorizado de programas**	**A12**	**3**	**9**
6	**Sismo**	**A16**	**3**	**9**
7	**Falla de corriente (apagones)**	**A21**	**3**	**9**
8	**Falla de sistema / Daño disco duro**	**A22**	**3**	**9**
9	**Falta de inducción, capacitación y sensibilización sobre riesgos**	**A23**	**3**	**9**

2. Finanzas (Magnitud de Daño: 3)				
N.º	**Amenaza**	**Código Amenaza**	**Probabilidad de Amenaza**	**Riesgo**
10	Mal manejo de sistemas y herramientas	A24	4	12
11	Perdida de datos	A27	3	3
12	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	A29	3	3
13	Unidades portables con información sin cifrado	A30	3	3

3. Servicios Bancarios (Magnitud: 3)				
N.º	**Amenaza**	**Código Amenaza**	**Probabilidad de Amenaza**	**Riesgo**
1	Daño por vandalismo	A5	3	9
2	Robo / Hurto (Físico)	A8	3	9
3	Intrusión a Red interna	A10	3	9
4	Infiltración	A11	3	9
5	Virus / Ejecución no autorizado de programas	A12	3	9
6	Sismo	A16	3	9

3. Servicios Bancarios (Magnitud: 3)				
N.º	Amenaza	Código Amenaza	Probabilidad de Amenaza	Riesgo
7	Falla de corriente (apagones)	A21	3	9
8	Falla de sistema / Daño disco duro	A22	3	9
9	Falta de inducción, capacitación y sensibilización sobre riesgos	A23	3	9
10	Mal manejo de sistemas y herramientas	A24	4	12
11	Perdida de datos	A27	3	3
12	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	A29	3	3
13	Unidades portables con información sin cifrado	A30	3	3

4. Recursos Humanos (Magnitud: 2)				
N.º	Amenaza	Código Amenaza	Probabilidad de Amenaza	Riesgo
1	Daño por vandalismo	A5	3	6
2	Robo / Hurto (Físico)	A8	2	4
3	Infiltración	A11	3	6
4	Sismo	A16	3	6

4. Recursos Humanos (Magnitud: 2)				
N.º	Amenaza	Código Amenaza	Probabilidad de Amenaza	Riesgo
5	Falta de inducción, capacitación y sensibilización sobre riesgos	A23	3	6
6	Mal manejo de sistemas y herramientas	A24	4	8
7	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	A29	3	6

5. Productos Institucionales (Magnitud: 4). Ver tabla en anexo para una lista de activos de TI que dan soporte a estos productos				
N.º	Amenaza	Código Amenaza	Probabilidad de Amenaza	Riesgo
1	Sabotaje (ataque físico y electrónico)	A4	2	8
2	Daño por vandalismo	A5	3	12
3	Extorsión	A6	2	8
4	Robo / Hurto de información electrónica	A9	3	12
5	Intrusión a Red interna	A10	3	12
6	Infiltración	A11	3	12
7	Virus / Ejecución no autorizado de programas	A12	3	12
8	Incendio	A14	2	8

5. Productos Institucionales (Magnitud: 4). Ver tabla en anexo para una lista de activos de TI que dan soporte a estos productos				
N.º	**Amenaza**	**Código Amenaza**	**Probabilidad de Amenaza**	**Riesgo**
9	Inundación / deslave	A15	2	8
10	Sismo	A16	3	12
11	Sobrecarga eléctrica	A20	2	8
12	Falla de corriente (apagones)	A21	3	12
13	Falla de sistema / Daño disco duro	A22	3	12
14	Falta de inducción, capacitación y sensibilización sobre riesgos	A23	3	12
15	Mal manejo de sistemas y herramientas	A24	4	16
16	Utilización de programas no autorizados / software 'pirateado'	A25	2	8
17	Perdida de datos	A27	3	12
18	Infección de sistemas a través de unidades portables sin escaneo	A28	2	8
19	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	A29	3	12
20	Unidades portables con información sin cifrado	A30	3	12
21	Transmisión no cifrada de datos críticos	A31	2	8

5. Productos Institucionales (Magnitud: 4). Ver tabla en anexo para una lista de activos de TI que dan soporte a estos productos				
N.º	**Amenaza**	**Código Amenaza**	**Probabilidad de Amenaza**	**Riesgo**
22	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, B.D. centralizada)	A32	2	8
23	Compartir contraseñas o permisos a terceros no autorizados	A33	2	8
24	Falta de definición de perfil, privilegios y restricciones del personal	A37	2	8
25	Falta de mantenimiento físico (proceso, repuestos e insumos)	A38	3	12
26	Falta de actualización de software (proceso y recursos)	A39	4	16
27	Fallas en permisos de usuarios (acceso a archivos)	A40	2	8
28	Acceso electrónico no autorizado a sistemas externos	A41	3	12
29	Acceso electrónico no autorizado a sistemas internos	A42	2	8
30	Red inalámbrica expuesta al acceso no autorizado	A44	2	8
31	Dependencia a servicio técnico externo	A45	4	16
32	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	A46	4	16
33	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	A47	3	12
34	Ausencia de documentación	A48	3	12

6. Correo Electrónico (Magnitud de daño: 2)				
N.º	**Amenaza**	**Código Amenaza**	**Probabilidad de Amenaza**	**Riesgo**
1	Robo / Hurto de información electrónica	A9	3	6
2	Intrusión a red interna	A10	3	6
3	Infiltración	A11	3	6
4	Virus / Ejecución no autorizado de programas	A12	3	6
5	Falla de sistema / Daño disco duro	A22	3	6
6	Falta de inducción, capacitación y sensibilización sobre riesgos	A23	3	6
7	Falta de inducción, capacitación y sensibilización sobre riesgos	A24	4	8
8	Perdida de datos	A27	3	6
9	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	A29	3	6
10	Unidades portables con información sin cifrado	A30	3	6
11	Falta de actualización de software (proceso y recursos)	A39	4	8
12	Acceso electrónico no autorizado a sistemas externos	A41	3	6

7. Base de datos interna (Magnitud de daño: 3)				
N.º	**Amenaza**	**Código Amenaza**	**Probabilidad de Amenaza**	**Riesgo**
1	Daños por vandalismo	A5	3	9
2	Robo / Hurto de información electrónica	A9	3	9
3	Intrusión a Red interna	A10	3	9
4	Virus / Ejecución no autorizado de programas	A12	3	9
5	Falla de sistema / Daño disco duro	A22	3	9
6	Falta de inducción, capacitación y sensibilización sobre riesgos	A23	3	9
7	Falta de inducción, capacitación y sensibilización sobre riesgos	A24	4	12
8	Perdida de datos	A27	3	9
9	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	A29	3	9
10	Unidades portables con información sin cifrado	A30	3	9
11	Falta de mantenimiento físico (proceso, repuestos e insumos)	A38	3	9
12	Falta de actualización de software (proceso y recursos)	A39	4	12
13	Acceso electrónico no autorizado a sistemas internos	A41	2	6
14	Dependencia a servicio técnico externo	A45	4	12
15	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	A46	4	12
16	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	A47	3	9
17	Ausencia de documentación	A48	3	9

8. Base de datos Externos (Magnitud de daño: 2)				
N.º	**Amenaza**	**Código Amenaza**	**Probabilidad de Amenaza**	**Riesgo**
1	Falta de inducción, capacitación y sensibilización sobre riesgos	A24	4	8
2	Falta de actualización de software (proceso y recursos)	A39	4	8
3	Dependencia a servicio técnico externo	A45	4	8
4	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	A46	4	8

9. Respaldos (Magnitud de daño: 2)				
N.º	**Amenaza**	**Código Amenaza**	**Probabilidad de Amenaza**	**Riesgo**
1	Falta de inducción, capacitación y sensibilización sobre riesgos	A24	4	8
2	Falta de actualización de software (proceso y recursos)	A39	4	8
3	Dependencia a servicio técnico externo	A45	4	8
4	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	A46	4	8

10. Base de datos de contraseñas (Magnitud de daño: 2)				
N.º	**Amenaza**	**Código Amenaza**	**Probabilidad de Amenaza**	**Riesgo**
1	Falta de inducción, capacitación y sensibilización sobre riesgos	A24	4	8
2	Falta de actualización de software (proceso y recursos)	A39	4	8
3	Dependencia a servicio técnico externo	A45	4	8
4	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	A46	4	8

3.1.4. Controles a implementar (ISO 27001 ver descripción del código Anexo 2)

1. Documentos Institucionales (Magnitud: 3)			
N.º	**Amenaza**	**Código Amenaza**	**Código de controles a implementar**
1	**Daño por vandalismo**	**A5**	A.11.1.1, A.11.1.2
2	**Robo / Hurto (Físico)**	**A8**	A.11.1.1, A.11.1.2, A.8.1.1
3	**Intrusión a Red interna**	**A10**	A.9.1.1, A.9.1.2, A.13.1.1, A.13.1.2, A.13.1.3
4	**Infiltración**	**A11**	A.9.1.1, A.9.1.2, A.13.1.1, A.13.1.2, A.13.1.3,
5	**Virus / Ejecución no autorizado de programas**	**A12**	A.12.2.1, A.12.6.1, A.12.6.2
6	**Sismo**	**A16**	A.12.3.1, A.17.2.1, A.11.1.4
7	**Falla de corriente (apagones)**	**A21**	A.11.2.2, A.11.2.3
8	**Falla de sistema / Daño disco duro**	**A22**	A.12.3.1, A.17.2.1
9	**Falta de inducción, capacitación y sensibilización sobre riesgos**	**A23**	A.7.2.2
10	**Mal manejo de sistemas y herramientas**	**A24**	A.7.2.2, A.9.3.1
11	**Perdida de datos**	**A27**	A.12.3.1, A.17.2.1
12	**Manejo inadecuado de datos críticos (codificar, borrar, etc.)**	**A29**	A.7.2.2, A.9.4.1
13	**Unidades portables con información sin cifrado**	**A30**	A.8.3.1, A.10.1.1, A.10.1.2,

2. Finanzas (Magnitud de Daño: 3)			
N.º	**Amenaza**	**Código Amenaza**	**Código de controles a implementar**
1	**Daño por vandalismo**	**A5**	A.11.1.1, A.11.1.2
2	**Robo / Hurto (Físico)**	**A8**	A.11.1.1, A.11.1.2, A.8.1.1
3	**Intrusión a Red interna**	**A10**	A.9.1.1, A.9.1.2, A.13.1.1, A.13.1.2, A.13.1.3
4	**Infiltración**	**A11**	A.9.1.1, A.9.1.2, A.13.1.1, A.13.1.2, A.13.1.3,
5	**Virus / Ejecución no autorizado de programas**	**A12**	A.12.2.1, A.12.6.1, A.12.6.2
6	**Sismo**	**A16**	A.12.3.1, A.17.2.1, A.11.1.4
7	**Falla de corriente (apagones)**	**A21**	A.11.2.2, A.11.2.3
8	**Falla de sistema / Daño disco duro**	**A22**	A.12.3.1, A.17.2.1
9	**Falta de inducción, capacitación y sensibilización sobre riesgos**	**A23**	A.7.2.2
10	**Mal manejo de sistemas y herramientas**	**A24**	A.7.2.2, A.9.3.1
11	**Perdida de datos**	**A27**	A.12.3.1, A.17.2.1
12	**Manejo inadecuado de datos críticos (codificar, borrar, etc.)**	**A29**	A.7.2.2, A.9.4.1
13	**Unidades portables con información sin cifrado**	**A30**	A.8.3.1, A.10.1.1, A.10.1.2,

3. Servicios Bancarios (Magnitud: 3)			
N.º	**Amenaza**	**Código Amenaza**	**Código de controles a implementar**
1	**Daño por vandalismo**	**A5**	A.11.1.1, A.11.1.2
2	**Robo / Hurto (Físico)**	**A8**	A.11.1.1, A.11.1.2, A.8.1.1
3	**Intrusión a Red interna**	**A10**	A.9.1.1, A.9.1.2, A.13.1.1, A.13.1.2, A.13.1.3
4	**Infiltración**	**A11**	A.9.1.1, A.9.1.2, A.13.1.1, A.13.1.2, A.13.1.3,
5	**Virus / Ejecución no autorizado de programas**	**A12**	A.12.2.1, A.12.6.1, A.12.6.2
6	**Sismo**	**A16**	A.12.3.1, A.17.2.1, A.11.1.4
7	**Falla de corriente (apagones)**	**A21**	A.11.2.2, A.11.2.3
8	**Falla de sistema / Daño disco duro**	**A22**	A.12.3.1, A.17.2.1
9	**Falta de inducción, capacitación y sensibilización sobre riesgos**	**A23**	A.7.2.2
10	**Mal manejo de sistemas y herramientas**	**A24**	A.7.2.2, A.9.3.1
11	**Perdida de datos**	**A27**	A.12.3.1, A.17.2.1
12	**Manejo inadecuado de datos críticos (codificar, borrar, etc.)**	**A29**	A.7.2.2, A.9.4.1
13	**Unidades portables con información sin cifrado**	**A30**	A.8.3.1, A.10.1.1, A.10.1.2,

4. Recursos Humanos (Magnitud: 2)			
N.º	**Amenaza**	**Código Amenaza**	**Código de controles a implementar**
1	**Daño por vandalismo**	**A5**	A.11.1.1, A.11.1.2
2	**Robo / Hurto (Físico)**	**A8**	A.11.1.1, A.11.1.2, A.8.1.1
3	**Infiltración**	**A11**	A.9.1.1, A.9.1.2, A.13.1.1, A.13.1.2, A.13.1.3,
4	**Sismo**	**A16**	A.12.3.1, A.17.2.1, A.11.1.4
5	**Falta de inducción, capacitación y sensibilización sobre riesgos**	**A23**	A.7.2.2
6	**Mal manejo de sistemas y herramientas**	**A24**	A.7.2.2, A.9.3.1
7	**Manejo inadecuado de datos críticos (codificar, borrar, etc.)**	**A29**	A.7.2.2, A.9.4.1

5. Productos Institucionales (Magnitud: 4)			
N.º	**Amenaza**	**Código Amenaza**	**Código de controles a implementar**
1	**Sabotaje (ataque físico y electrónico)**	**A4**	A.11.1.1, A.11.1.2, A.7.1.1 A.7.1.2
2	**Daño por vandalismo**	**A5**	A.11.1.1, A.11.1.2
3	**Extorsión**	**A6**	A.7.1.1 A.7.1.2
4	**Robo / Hurto de información electrónica**	**A9**	A.9.1.1, A.9.1.2, A.8.3.1, A.8.3.2, A.8.3.3
5	**Intrusión a Red interna**	**A10**	A.9.1.1, A.9.1.2, A.13.1.1, A.13.1.2, A.13.1.3
6	**Infiltración**	**A11**	A.9.1.1, A.9.1.2, A.13.1.1, A.13.1.2, A.13.1.3,

5. Productos Institucionales (Magnitud: 4)			
N.º	**Amenaza**	**Código Amenaza**	**Código de controles a implementar**
7	**Virus / Ejecución no autorizado de programas**	**A12**	A.12.2.1, A.12.6.1, A.12.6.2
8	**Incendio**	**A14**	A.11.1.4, A.11.2.1, A.12.3.1
9	**Inundación / deslave**	**A15**	A.11.1.4, A.11.2.1, A.12.3.1
10	**Sismo**	**A16**	A.12.3.1, A.17.2.1, A.11.1.4
11	**Sobrecarga eléctrica**	**A20**	A.11.2.2, A.11.2.3
12	**Falla de corriente (apagones)**	**A21**	A.11.2.2, A.11.2.3
13	**Falla de sistema / Daño disco duro**	**A22**	A.12.3.1
14	**Falta de inducción, capacitación y sensibilización sobre riesgos**	**A23**	A.7.2.2
15	**Mal manejo de sistemas y herramientas**	**A24**	A.7.2.2, A.9.3.1
16	**Utilización de programas no autorizados / software 'pirateado'**	**A25**	A.12.6.2
17	**Perdida de datos**	**A27**	A.12.3.1, A.17.2.1
18	**Infección de sistemas a través de unidades portables sin escaneo**	**A28**	A.12.2.1, A.8.3.1, A.8.3.2
19	**Manejo inadecuado de datos críticos (codificar, borrar, etc.)**	**A29**	A.7.2.2, A.9.4.1
20	**Unidades portables con información sin cifrado**	**A30**	A.8.3.1, A.10.1.1, A.10.1.2
21	**Transmisión no cifrada de datos críticos**	**A31**	A.10.1.1, A.10.1.2

5. Productos Institucionales (Magnitud: 4)			
N.º	**Amenaza**	**Código Amenaza**	**Código de controles a implementar**
22	**Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)**	**A32**	A.9.4.3, A.9.4.2, A.9.3.1
23	**Compartir contraseñas o permisos a terceros no autorizados**	**A33**	A.13.2.1, A.13.2.2, A13.2.4
24	**Falta de definición de perfil, privilegios y restricciones del personal**	**A37**	A.9.2.3, A.9.2.5, A.9.4.1, A.9.4.4
25	**Falta de mantenimiento físico (proceso, repuestos e insumos)**	**A38**	A.11.2.4
26	**Falta de actualización de software (proceso y recursos)**	**A39**	A.11.2.4
27	**Fallas en permisos de usuarios (acceso a archivos)**	**A40**	A.9.2.2, A.9.2.3, A.9.2.5
28	**Acceso electrónico no autorizado a sistemas externos**	**A41**	A.9.2.3, A.9.2.5, A.9.4.1, A.9.4.4, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.1, A.9.2.6
29	**Acceso electrónico no autorizado a sistemas internos**	**A42**	A.9.2.3, A.9.2.5, A.9.4.1, A.9.4.4, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.1, A.9.2.6
30	**Red inalámbrica expuesta al acceso no autorizado**	**A44**	A.9.1.1, A.9.1.2, A.13.1.1, A.13.1.2, A.13.1.3
31	**Dependencia a servicio técnico externo**	**A45**	A.15.1.3
32	**Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)**	**A46**	A.5.1.1
33	**Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control**	**A47**	A.5.1.2, A.18.2.1, A.18.2.2
34	**Ausencia de documentación**	**A48**	A.5.1.1

6. Correo Electrónico (Magnitud de daño: 2)			
N.º	**Amenaza**	**Código Amenaza**	**Código de controles a implementar**
1	**Robo / Hurto de información electrónica**	**A9**	A.9.1.1, A.9.1.2, A.8.3.1, A.8.3.2, A.8.3.3
2	**Intrusión a red interna**	**A10**	A.9.1.1, A.9.1.2, A.13.1.1, A.13.1.2, A.13.1.3
3	**Infiltración**	**A11**	A.9.1.1, A.9.1.2, A.13.1.1, A.13.1.2, A.13.1.3,
4	**Virus / Ejecución no autorizado de programas**	**A12**	A.12.2.1, A.12.6.1, A.12.6.2
5	**Falla de sistema / Daño disco duro**	**A22**	A.12.3.1
6	**Falta de inducción, capacitación y sensibilización sobre riesgos**	**A23**	A.7.2.2
7	**Mal manejo de sistemas y herramientas**	**A24**	A.7.2.2, A.9.3.1
8	**Perdida de datos**	**A27**	A.12.3.1, A.17.2.1
9	**Manejo inadecuado de datos críticos (codificar, borrar, etc.)**	**A29**	A.7.2.2, A.9.4.1
10	**Unidades portables con información sin cifrado**	**A30**	A.8.3.1, A.10.1.1, A.10.1.2
11	**Falta de actualización de software (proceso y recursos)**	**A39**	A.11.2.4
12	**Acceso electrónico no autorizado a sistemas externos**	**A41**	A.9.2.3, A.9.2.5, A.9.4.1, A.9.4.4, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.1, A.9.2.6

7. Base de datos interna (Magnitud de daño: 3)			
N.º	**Amenaza**	**Código Amenaza**	**Código de controles a implementar**
1	**Daños por vandalismo**	**A5**	A.11.1.1, A.11.1.2
2	**Robo / Hurto de información electrónica**	**A9**	A.9.1.1, A.9.1.2, A.8.3.1, A.8.3.2, A.8.3.3
3	**Intrusión a Red interna**	**A10**	A.9.1.1, A.9.1.2, A.13.1.1, A.13.1.2, A.13.1.3
4	**Virus / Ejecución no autorizado de programas**	**A12**	A.12.2.1, A.12.6.1, A.12.6.2
5	**Falla de sistema / Daño disco duro**	**A22**	A.12.3.1
6	**Falta de inducción, capacitación y sensibilización sobre riesgos**	**A23**	A.7.2.2
7	**Mal manejo de sistemas y herramientas**	**A24**	A.7.2.2, A.9.3.1
8	**Perdida de datos**	**A27**	A.12.3.1, A.17.2.1
9	**Manejo inadecuado de datos críticos (codificar, borrar, etc.)**	**A29**	A.7.2.2, A.9.4.1
10	**Unidades portables con información sin cifrado**	**A30**	A.8.3.1, A.10.1.1, A.10.1.2
11	**Falta de mantenimiento físico (proceso, repuestos e insumos)**	**A38**	A.11.2.4
12	**Falta de actualización de software (proceso y recursos)**	**A39**	A.11.2.4
13	**Acceso electrónico no autorizado a sistemas internos**	**A41**	A.9.2.3, A.9.2.5, A.9.4.1, A.9.4.4, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.1, A.9.2.6
14	**Dependencia a servicio técnico externo**	**A45**	A.15.1.3
15	**Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)**	**A46**	A.5.1.1
16	**Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control**	**A47**	A.5.1.2, A.18.2.1, A.18.2.2

7. Base de datos interna (Magnitud de daño: 3)			
N.º	**Amenaza**	**Código Amenaza**	**Código de controles a implementar**
17	**Ausencia de documentación**	**A48**	A.5.1.1

8. Base de datos Externos (Magnitud de daño: 2)			
N.º	**Amenaza**	**Código Amenaza**	**Código de controles a implementar**
1	**Falta de inducción, capacitación y sensibilización sobre riesgos**	**A24**	A.7.2.2
2	**Falta de actualización de software (proceso y recursos)**	**A39**	A.11.2.4
3	**Dependencia a servicio técnico externo**	**A45**	A.15.1.3
4	**Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)**	**A46**	A.5.1.1

9. Respaldos (Magnitud de daño: 2)			
N.º	**Amenaza**	**Código Amenaza**	**Código de controles a implementar**
1	**Falta de inducción, capacitación y sensibilización sobre riesgos**	**A24**	A.7.2.2
2	**Falta de actualización de software (proceso y recursos)**	**A39**	A.11.2.4
3	**Dependencia a servicio técnico externo**	**A45**	A.15.1.3
4	**Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)**	**A46**	A.5.1.1

10. Base de datos de contraseñas (Magnitud de daño: 2)			
N.º	**Amenaza**	**Código Amenaza**	**Código de controles a implementar**
1	**Falta de inducción, capacitación y sensibilización sobre riesgos**	**A24**	A.7.2.2
2	**Falta de actualización de software (proceso y recursos)**	**A39**	A.11.2.4
3	**Dependencia a servicio técnico externo**	**A45**	A.15.1.3
4	**Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)**	**A46**	A.5.1.1

4. Anexos

4.1. Anexo 1: Listado de amenazas

Categoría	Amenaza	Código
Actos originados por la criminalidad común y motivación política	Allanamiento (ilegal, legal)	A1
	Persecución (civil, fiscal, penal)	A2
	Orden de secuestro / Detención	A3
	Sabotaje (ataque físico y electrónico)	A4
	Daños por vandalismo	A5
	Extorsión	A6
	Fraude / Estafa	A7
	Robo / Hurto (físico)	A8
	Robo / Hurto de información electrónica	A9
	Intrusión a Red interna	A10
	Infiltración	A11
	Virus / Ejecución no autorizado de programas	A12
	Violación a derechos de autor	A13
Sucesos de origen físico	Incendio	A14
	Inundación / deslave	A15
	Sismo	A16
	Polvo	A17
	Falta de ventilación	A18
	Electromagnetismo	A19
	Sobrecarga eléctrica	A20
	Falla de corriente (apagones)	A21

Categoría	Amenaza	Código
	Falla de sistema / Daño disco duro	A22
Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales	Falta de inducción, capacitación y sensibilización sobre riesgos	A23
	Falta de inducción, capacitación y sensibilización sobre riesgos	A24
	Utilización de programas no autorizados / software 'pirateado'	A25
	Falta de pruebas de software nuevo con datos productivos	A26
	Perdida de datos	A27
	Infección de sistemas a través de unidades portables sin escaneo	A28
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	A29
	Unidades portables con información sin cifrado	A30
	Transmisión no cifrada de datos críticos	A31
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	A32
	Compartir contraseñas o permisos a terceros no autorizados	A33
	Transmisión de contraseñas por teléfono	A34
	Exposición o extravío de equipo, unidades de almacenamiento, etc	A35
	Sobrepasar autoridades	A36
	Falta de definición de perfil, privilegios y restricciones del personal	A37
	Falta de mantenimiento físico (proceso, repuestos e insumos)	A38
	Falta de actualización de software (proceso y recursos)	A39
	Fallas en permisos de usuarios (acceso a archivos)	A40
	Acceso electrónico no autorizado a sistemas externos	A41
	Acceso electrónico no autorizado a sistemas internos	A42
	Red cableada expuesta para el acceso no autorizado	A43
	Red inalámbrica expuesta al acceso no autorizado	A44

Categoría	Amenaza	Código
	Dependencia a servicio técnico externo	A45
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	A46
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	A47
	Ausencia de documentación	A48

4.2. Anexo 2: Amenazas y controles

1. DOCUMENTOS INSTITUCIONALES / MAGNITUD DE DAÑO: 3				
Código Amenaza	Amenaza	Código ISO	Descripción	Control
A5	Daño por vandalismo	A.11.1.1	Perímetro de seguridad física	Se deben utilizar perímetros de seguridad para proteger las áreas que contienen información sensible, así como los recursos de tratamiento de la información.
		A.11.1.2	Controles físicos de entrada	Las áreas seguras deben estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.
A8	Robo / Hurto (Físico)	A.8.1.1	Inventario	La información y otros activos asociados a la información y a los recursos para el tratamiento de la información deben estar claramente identificados y debe elaborarse y mantenerse un inventario.
		A.11.1.1	Perímetro de seguridad física	Se deben utilizar perímetros de seguridad para proteger las áreas que contienen información sensible, así como los recursos de tratamiento de la información.
		A.11.1.2	Controles físicos de entrada	Las áreas seguras deben estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.
A10	Intrusión a Red interna	A.9.1.1	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.
		A.9.1.2	Acceso a las redes y a los servicios de red	Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.
		A.13.1.1	Controles de red	Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.
		A.13.1.2	Seguridad de los servicios de red	Se deben identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.
		A.13.1.3	Segregación en redes	Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en redes distintas.
A11	Infiltración	A.9.1.1	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.
		A.9.1.2	Acceso a las redes y a los servicios de red	Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.
		A.13.1.1	Controles de red	Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.

1. DOCUMENTOS INSTITUCIONALES / MAGNITUD DE DAÑO: 3				
Código Amenaza	Amenaza	Código ISO	Descripción	Control
		A.13.1.2	Seguridad de los servicios de red	Se deben identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.
		A.13.1.3	Segregación en redes	Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en redes distintas.
A12	Virus / Ejecución no autorizado de programas	A.12.2.1	Controles contra el código malicioso	Se deben implementar los controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso, así como procedimientos adecuados de concienciación al usuario.
		A.12.6.1	Gestión de las vulnerabilidades técnicas	Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.
		A.12.6.2	Restricción en la instalación de software	Se deben establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios.
A16	Sismo	A.11.1.4	Protección contra las amenazas externas y ambientales	Se debe diseñar y aplicar una protección física contra desastres naturales, ataques provocados por el hombre o accidentes.
		A.12.3.1	Copias de seguridad de la información	Se deben realizar copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo a la política de copias de seguridad acordada.
		A.17.2.1	Disponibilidad de los recursos de tratamiento de la información	Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.
A21	Falla de corriente (apagones)	A.11.2.2	Instalaciones de suministro	Los equipos deben estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.
		A.11.2.3	Seguridad del cableado	El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información debe estar protegido frente a interceptaciones, interferencias o daños.
A22	Falla de sistema / Daño de disco duro	A.12.3.1	Copias de seguridad de la información	Se deben realizar copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo a la política de copias de seguridad acordada.

1. DOCUMENTOS INSTITUCIONALES / MAGNITUD DE DAÑO: 3				
Código Amenaza	Amenaza	Código ISO	Descripción	Control
		A.17.2.1	Disponibilidad de los recursos de tratamiento de la información	Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.
A23	Falta de inducción, capacitación y sensibilización sobre riesgos	A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.
A24	Mal manejo de sistemas y herramientas	A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.
		A.9.3.1	Uso de la información secreta de autenticación	Se debe requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.
A27	Perdida de datos	A.12.3.1	Copias de seguridad de la información	Se deben realizar copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo a la política de copias de seguridad acordada.
		A.17.2.1	Disponibilidad de los recursos de tratamiento de la información	Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.
A29	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.
		A.9.4.1	Restricción del acceso a la información	Se debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.
A30	Unidades portables con información sin cifrado	A.8.3.1	Gestión de soportes extraíbles	Se deben implementar procedimientos para la gestión de los soportes extraíbles, de acuerdo con el esquema de clasificación adoptado por la organización.
		A.10.1.1	Política de uso de los controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de los controles criptográficos para proteger la información.

1. DOCUMENTOS INSTITUCIONALES / MAGNITUD DE DAÑO: 3				
Código Amenaza	Amenaza	Código ISO	Descripción	Control
		A.10.1.2	Gestión de claves	Se debe desarrollar e implementar una política sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida.

2. FINANZAS / MAGNITUD DE DAÑO: 3				
Código Amenaza	Amenaza	Código ISO	Descripción	Control
A5	Daño por vandalismo	A.11.1.1	Perímetro de seguridad física	Se deben utilizar perímetros de seguridad para proteger las áreas que contienen información sensible, así como los recursos de tratamiento de la información.
		A.11.1.2	Controles físicos de entrada	Las áreas seguras deben estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.
A8	Robo / Hurto (Físico)	A.8.1.1	Inventario	La información y otros activos asociados a la información y a los recursos para el tratamiento de la información deben estar claramente identificados y debe elaborarse y mantenerse un inventario.
		A.11.1.1	Perímetro de seguridad física	Se deben utilizar perímetros de seguridad para proteger las áreas que contienen información sensible, así como los recursos de tratamiento de la información.
		A.11.1.2	Controles físicos de entrada	Las áreas seguras deben estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.
A10	Intrusión a Red interna	A.9.1.1	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.
		A.9.1.2	Acceso a las redes y a los servicios de red	Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.
		A.13.1.1	Controles de red	Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.

2. FINANZAS / MAGNITUD DE DAÑO: 3				
Código Amenaza	Amenaza	Código ISO	Descripción	Control
		A.13.1.2	Seguridad de los servicios de red	Se deben identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.
		A.13.1.3	Segregación en redes	Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en redes distintas.
A11	Infiltración	A.9.1.1	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.
		A.9.1.2	Acceso a las redes y a los servicios de red	Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.
		A.13.1.1	Controles de red	Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.
		A.13.1.2	Seguridad de los servicios de red	Se deben identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.
		A.13.1.3	Segregación en redes	Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en redes distintas.
A12	Virus / Ejecución no autorizado de programas	A.12.2.1	Controles contra el código malicioso	Se deben implementar los controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso, así como procedimientos adecuados de concienciación al usuario.
		A.12.6.1	Gestión de las vulnerabilidades técnicas	Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.
		A.12.6.2	Restricción en la instalación de software	Se deben establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios.
A16	Sismo	A.11.1.4	Protección contra las amenazas externas y ambientales	Se debe diseñar y aplicar una protección física contra desastres naturales, ataques provocados por el hombre o accidentes.

2. FINANZAS / MAGNITUD DE DAÑO: 3				
Código Amenaza	Amenaza	Código ISO	Descripción	Control
		A.12.3.1	Copias de seguridad de la información	Se deben realizar copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo a la política de copias de seguridad acordada.
		A.17.2.1	Disponibilidad de los recursos de tratamiento de la información	Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.
A21	Falla de corriente (apagones)	A.11.2.2	Instalaciones de suministro	Los equipos deben estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.
		A.11.2.3	Seguridad del cableado	El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información debe estar protegido frente a interceptaciones, interferencias o daños.
A22	Falla de sistema / Daño de disco duro	A.12.3.1	Copias de seguridad de la información	Se deben realizar copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo a la política de copias de seguridad acordada.
		A.17.2.1	Disponibilidad de los recursos de tratamiento de la información	Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.
A23	Falta de inducción, capacitación y sensibilización sobre riesgos	A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.
A24	Mal manejo de sistemas y herramientas	A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.
		A.9.3.1	Uso de la información secreta de autenticación	Se debe requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.

2. FINANZAS / MAGNITUD DE DAÑO: 3				
Código Amenaza	Amenaza	Código ISO	Descripción	Control
A27	Perdida de datos	A.12.3.1	Copias de seguridad de la información	Se deben realizar copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo a la política de copias de seguridad acordada.
		A.17.2.1	Disponibilidad de los recursos de tratamiento de la información	Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.
A29	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.
		A.9.4.1	Restricción del acceso a la información	Se debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.
A30	Unidades portables con información sin cifrado	A.8.3.1	Gestión de soportes extraíbles	Se deben implementar procedimientos para la gestión de los soportes extraíbles, de acuerdo con el esquema de clasificación adoptado por la organización.
		A.10.1.1	Política de uso de los controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de los controles criptográficos para proteger la información.
		A.10.1.2	Gestión de claves	Se debe desarrollar e implementar una política sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida.

3. SERVICIOS BANCARIOS / MAGNITUD DE DAÑO: 3				
Código Amenaza	Amenaza	Código ISO	Descripción	Control
A5	Daño por vandalismo	A.11.1.1	Perímetro de seguridad física	Se deben utilizar perímetros de seguridad para proteger las áreas que contienen información sensible, así como los recursos de tratamiento de la información.
		A.11.1.2	Controles físicos de entrada	Las áreas seguras deben estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.
A8	Robo / Hurto (Físico)	A.8.1.1	Inventario	La información y otros activos asociados a la información y a los recursos para el tratamiento de la información deben estar claramente identificados y debe elaborarse y mantenerse un inventario.
		A.11.1.1	Perímetro de seguridad física	Se deben utilizar perímetros de seguridad para proteger las áreas que contienen información sensible, así como los recursos de tratamiento de la información.
		A.11.1.2	Controles físicos de entrada	Las áreas seguras deben estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.
A10	Intrusión a Red interna	A.9.1.1	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.
		A.9.1.2	Acceso a las redes y a los servicios de red	Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.
		A.13.1.1	Controles de red	Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.
		A.13.1.2	Seguridad de los servicios de red	Se deben identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.
		A.13.1.3	Segregación en redes	Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en redes distintas.
A11	Infiltración	A.9.1.1	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.

3. SERVICIOS BANCARIOS / MAGNITUD DE DAÑO: 3				
Código Amenaza	Amenaza	Código ISO	Descripción	Control
		A.9.1.2	Acceso a las redes y a los servicios de red	Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.
		A.13.1.1	Controles de red	Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.
		A.13.1.2	Seguridad de los servicios de red	Se deben identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.
		A.13.1.3	Segregación en redes	Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en redes distintas.
A12	Virus / Ejecución no autorizado de programas	A.12.2.1	Controles contra el código malicioso	Se deben implementar los controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso, así como procedimientos adecuados de concienciación al usuario.
		A.12.6.1	Gestión de las vulnerabilidades técnicas	Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.
		A.12.6.2	Restricción en la instalación de software	Se deben establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios.
A16	Sismo	A.11.1.4	Protección contra las amenazas externas y ambientales	Se debe diseñar y aplicar una protección física contra desastres naturales, ataques provocados por el hombre o accidentes.
		A.12.3.1	Copias de seguridad de la información	Se deben realizar copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo a la política de copias de seguridad acordada.
		A.17.2.1	Disponibilidad de los recursos de tratamiento de la información	Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.
A21	Falla de corriente (apagones)	A.11.2.2	Instalaciones de suministro	Los equipos deben estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.

3. SERVICIOS BANCARIOS / MAGNITUD DE DAÑO: 3				
Código Amenaza	Amenaza	Código ISO	Descripción	Control
		A.11.2.3	Seguridad del cableado	El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información debe estar protegido frente a interceptaciones, interferencias o daños.
A22	Falla de sistema / Daño de disco duro	A.12.3.1	Copias de seguridad de la información	Se deben realizar copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo a la política de copias de seguridad acordada.
		A.17.2.1	Disponibilidad de los recursos de tratamiento de la información	Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.
A23	Falta de inducción, capacitación y sensibilización sobre riesgos	A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.
A24	Mal manejo de sistemas y herramientas	A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.
		A.9.3.1	Uso de la información secreta de autenticación	Se debe requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.
A27	Perdida de datos	A.12.3.1	Copias de seguridad de la información	Se deben realizar copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo a la política de copias de seguridad acordada.
		A.17.2.1	Disponibilidad de los recursos de tratamiento de la información	Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.

3. SERVICIOS BANCARIOS / MAGNITUD DE DAÑO: 3				
Código Amenaza	Amenaza	Código ISO	Descripción	Control
A29	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.
		A.9.4.1	Restricción del acceso a la información	Se debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.
A30	Unidades portables con información sin cifrado	A.8.3.1	Gestión de soportes extraíbles	Se deben implementar procedimientos para la gestión de los soportes extraíbles, de acuerdo con el esquema de clasificación adoptado por la organización.
		A.10.1.1	Política de uso de los controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de los controles criptográficos para proteger la información.
		A.10.1.2	Gestión de claves	Se debe desarrollar e implementar una política sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida.

4. RECURSOS HUMANOS / MAGNITUD DE DAÑO: 2				
Código Amenaza	Amenaza	Código ISO	Descripción	Control
A5	Daño por vandalismo	A.11.1.1	Perímetro de seguridad física	Se deben utilizar perímetros de seguridad para proteger las áreas que contienen información sensible, así como los recursos de tratamiento de la información.
		A.11.1.2	Controles físicos de entrada	Las áreas seguras deben estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.
A8	Robo / Hurto (Físico)	A.8.1.1	Inventario	La información y otros activos asociados a la información y a los recursos para el tratamiento de la información deben estar claramente identificados y debe elaborarse y mantenerse un inventario.
		A.11.1.1	Perímetro de seguridad física	Se deben utilizar perímetros de seguridad para proteger las áreas que contienen información sensible, así como los recursos de tratamiento de la información.
		A.11.1.2	Controles físicos de entrada	Las áreas seguras deben estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.
A11	Infiltración	A.9.1.1	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.
		A.9.1.2	Acceso a las redes y a los servicios de red	Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.
		A.13.1.1	Controles de red	Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.
		A.13.1.2	Seguridad de los servicios de red	Se deben identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.
		A.13.1.3	Segregación en redes	Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en redes distintas.
A16	Sismo	A.11.1.4	Protección contra las amenazas externas y ambientales	Se debe diseñar y aplicar una protección física contra desastres naturales, ataques provocados por el hombre o accidentes.
		A.12.3.1	Copias de seguridad de la información	Se deben realizar copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo a la política de copias de seguridad acordada.

4. RECURSOS HUMANOS / MAGNITUD DE DAÑO: 2				
Código Amenaza	Amenaza	Código ISO	Descripción	Control
		A.17.2.1	Disponibilidad de los recursos de tratamiento de la información	Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.
A23	Falta de inducción, capacitación y sensibilización sobre riesgos	A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.
A24	Mal manejo de sistemas y herramientas	A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.
		A.9.3.1	Uso de la información secreta de autenticación	Se debe requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.
A29	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.
		A.9.4.1	Restricción del acceso a la información	Se debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.

5. PRODUCTOS INSTITUCIONALES / MAGNITUD DE DAÑO: 4				
Código Amenaza	Amenaza	Código ISO	Descripción	Control
A4	Sabotaje (ataque físico y electrónico)	A.7.1.1	Investigación de antecedentes	La comprobación de los antecedentes de todos los candidatos al puesto de trabajo se debe llevar a cabo de acuerdo con las leyes, normativa y códigos éticos que sean de aplicación y debe ser proporcional a las necesidades del negocio, la clasificación de la información a la que se accede y los riesgos percibidos.
		A.7.1.2	Términos y condiciones del empleo	Cómo parte de sus obligaciones contractuales, los empleados y contratistas deben establecer los términos y condiciones en su contrato de trabajo en lo que respecta a la seguridad de la información, tanto hacia el empleado como hacia la organización.
		A.11.1.1	Perímetro de seguridad física	Se deben utilizar perímetros de seguridad para proteger las áreas que contienen información sensible, así como los recursos de tratamiento de la información.
		A.11.1.2	Controles físicos de entrada	Las áreas seguras deben estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.
A5	Daño por vandalismo	A.11.1.1	Perímetro de seguridad física	Se deben utilizar perímetros de seguridad para proteger las áreas que contienen información sensible, así como los recursos de tratamiento de la información.
		A.11.1.2	Controles físicos de entrada	Las áreas seguras deben estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.
A6	Extorsión	A.7.1.1	Investigación de antecedentes	La comprobación de los antecedentes de todos los candidatos al puesto de trabajo se debe llevar a cabo de acuerdo con las leyes, normativa y códigos éticos que sean de aplicación y debe ser proporcional a las necesidades del negocio, la clasificación de la información a la que se accede y los riesgos percibidos.
		A.7.1.2	Términos y condiciones del empleo	Cómo parte de sus obligaciones contractuales, los empleados y contratistas deben establecer los términos y condiciones en su contrato de trabajo en lo que respecta a la seguridad de la información, tanto hacia el empleado como hacia la organización.
A9	Robo / Hurto (Físico)	A.8.1.1	Inventario	La información y otros activos asociados a la información y a los recursos para el tratamiento de la información deben estar claramente identificados y debe elaborarse y mantenerse un inventario.
		A.11.1.1	Perímetro de seguridad física	Se deben utilizar perímetros de seguridad para proteger las áreas que contienen información sensible así como los recursos de tratamiento de la información.

5. PRODUCTOS INSTITUCIONALES / MAGNITUD DE DAÑO: 4				
Código Amenaza	Amenaza	Código ISO	Descripción	Control
		A.11.1.2	Controles físicos de entrada	Las áreas seguras deben estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.
A10	Intrusión a Red interna	A.9.1.1	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.
		A.9.1.2	Acceso a las redes y a los servicios de red	Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.
		A.13.1.1	Controles de red	Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.
		A.13.1.2	Seguridad de los servicios de red	Se deben identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.
		A.13.1.3	Segregación en redes	Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en redes distintas.
A11	Infiltración	A.9.1.1	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.
		A.9.1.2	Acceso a las redes y a los servicios de red	Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.
		A.13.1.1	Controles de red	Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.
		A.13.1.2	Seguridad de los servicios de red	Se deben identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.
		A.13.1.3	Segregación en redes	Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en redes distintas.
A12	Virus / Ejecución no autorizado de programas	A.12.2.1	Controles contra el código malicioso	Se deben implementar los controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso, así como procedimientos adecuados de concienciación al usuario.
		A.12.6.1	Gestión de las vulnerabilidades técnicas	Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.

5. PRODUCTOS INSTITUCIONALES / MAGNITUD DE DAÑO: 4				
Código Amenaza	Amenaza	Código ISO	Descripción	Control
		A.12.6.2	Restricción en la instalación de software	Se deben establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios.
A15	Inundación / deslave	A.11.1.4	Protección contra las amenazas externas y ambientales	Se debe diseñar y aplicar una protección física contra desastres naturales, ataques provocados por el hombre o accidentes.
		A.11.2.1	Emplazamiento y protección de equipos	Los equipos deben situarse o protegerse de forma que se reduzcan los riesgos de las amenazas y los riesgos ambientales, así como las oportunidades de que se produzcan accesos no autorizados.
		A.12.3.1	Copias de seguridad de la información	Se deben realizar copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo con la política de copias de seguridad acordada.
A16	Sismo	A.11.1.4	Protección contra las amenazas externas y ambientales	Se debe diseñar y aplicar una protección física contra desastres naturales, ataques provocados por el hombre o accidentes.
		A.12.3.1	Copias de seguridad de la información	Se deben realizar copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo a la política de copias de seguridad acordada.
		A.17.2.1	Disponibilidad de los recursos de tratamiento de la información	Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.
A20	Sobrecarga eléctrica	A.11.2.2	Instalaciones de suministro	Los equipos deben estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.
		A.11.2.3	Seguridad del cableado	El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información debe estar protegido frente a interceptaciones, interferencias o daños.
A21	Falla de corriente (apagones)	A.11.2.2	Instalaciones de suministro	Los equipos deben estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.
		A.11.2.3	Seguridad del cableado	El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información debe estar protegido frente a interceptaciones, interferencias o daños.
A22	Falla de sistema / Daño de disco duro	A.12.3.1	Copias de seguridad de la información	Se deben realizar copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo con la política de copias de seguridad acordada.

5. PRODUCTOS INSTITUCIONALES / MAGNITUD DE DAÑO: 4				
Código Amenaza	Amenaza	Código ISO	Descripción	Control
		A.17.2.1	Disponibilidad de los recursos de tratamiento de la información	Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.
A23	Falta de inducción, capacitación y sensibilización sobre riesgos	A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.
A24	Mal manejo de sistemas y herramientas	A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.
		A.9.3.1	Uso de la información secreta de autenticación	Se debe requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.
A25	Utilización de programas no autorizados / software 'pirateado'	A.12.6.2	Restricción en la instalación de software	Se deben establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios.
A27	Perdida de datos	A.12.3.1	Copias de seguridad de la información	Se deben realizar copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo con la política de copias de seguridad acordada.
		A.17.2.1	Disponibilidad de los recursos de tratamiento de la información	Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.
A28	Infección de sistemas a través de unidades portables sin escaneo	A.8.3.1	Gestión de soportes extraíbles	Se deben implementar procedimientos para la gestión de los soportes extraíbles, de acuerdo con el esquema de clasificación adoptado por la organización.
		A.8.3.2	Eliminación de soportes	Los soportes deben eliminarse de forma segura cuando ya no vayan a ser necesarios, mediante procedimientos formales.

5. PRODUCTOS INSTITUCIONALES / MAGNITUD DE DAÑO: 4				
Código Amenaza	Amenaza	Código ISO	Descripción	Control
		A.12.2.1	Controles contra el código malicioso	Se deben implementar los controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso, así como procedimientos adecuados de concienciación al usuario.
A29	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.
		A.9.4.1	Restricción del acceso a la información	Se debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.
A30	Unidades portables con información sin cifrado	A.8.3.1	Gestión de soportes extraíbles	Se deben implementar procedimientos para la gestión de los soportes extraíbles, de acuerdo con el esquema de clasificación adoptado por la organización.
		A.10.1.1	Política de uso de los controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de los controles criptográficos para proteger la información.
		A.10.1.2	Gestión de claves	Se debe desarrollar e implementar una política sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida.
A31	Transmisión no cifrada de datos críticos	A.10.1.1	Política de uso de los controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de los controles criptográficos para proteger la información.
		A.10.1.2	Gestión de claves	Se debe desarrollar e implementar una política sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida.
A32	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	A.9.3.1	Uso de la información secreta de autenticación	Se debe requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.
		A.9.4.2	Procedimientos seguros de inicio de sesión	Cuando así se requiera en la política de control de acceso, el acceso a los sistemas y a las aplicaciones se debe controlar por medio de un procedimiento seguro de inicio de sesión.
		A.9.4.3	Sistema de gestión de contraseñas	Los sistemas para la gestión de contraseñas deben ser interactivos y establecer contraseñas seguras y robustas
A33	Compartir contraseñas o permisos a terceros no autorizados	A.13.2.1	Políticas y procedimientos de intercambio de información	Deben establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación.

5. PRODUCTOS INSTITUCIONALES / MAGNITUD DE DAÑO: 4				
Código Amenaza	Amenaza	Código ISO	Descripción	Control
		A.13.2.2	Acuerdos de intercambio de información	Deben establecerse acuerdos para el intercambio seguro de información del negocio y software entre la organización y terceros.
		A.13.2.4	Acuerdos de confidencialidad o no revelación	Deben identificarse, documentarse y revisarse regularmente los requisitos de los acuerdos de confidencialidad o no revelación
A37	Falta de definición de perfil, privilegios y restricciones del personal	A.9.2.3	Gestión de privilegios de acceso	La asignación y el uso de privilegios de acceso debe estar restringida y controlada.
		A.9.2.5	Revisión de los derechos de acceso de usuario	Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares.
		A.9.4.1	Restricción del acceso a la información	Se debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.
		A.9.4.4	Uso de utilidades con privilegios del sistema	Se debe restringir y controlar rigurosamente el uso de utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación.
A38	Falta de mantenimiento físico (proceso, repuestos e insumos)	A.11.2.4	Mantenimiento de los equipos	Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas.
A39	Falta de actualización de software (proceso y recursos)	A.11.2.4	Mantenimiento de los equipos	Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas.
A40	Fallas en permisos de usuarios (acceso a archivos)	A.9.2.2	Provisión de acceso de usuario	Debe implantarse un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios.
		A.9.2.3	Gestión de privilegios de acceso	La asignación y el uso de privilegios de acceso debe estar restringida y controlada.
		A.9.2.5	Revisión de los derechos de acceso de usuario	Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares.
A41	Acceso electrónico no autorizado a	A.9.2.1	Registro y baja de usuario	Debe implantarse un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso.

5. PRODUCTOS INSTITUCIONALES / MAGNITUD DE DAÑO: 4				
Código Amenaza	Amenaza	Código ISO	Descripción	Control
	sistemas externos	A.9.2.2	Provisión de acceso de usuario	Debe implantarse un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios.
		A.9.2.3	Gestión de privilegios de acceso	La asignación y el uso de privilegios de acceso debe estar restringida y controlada.
		A.9.2.5	Revisión de los derechos de acceso de usuario	Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares.
		A.9.2.6	Retirada o reasignación de los derechos de acceso	Los derechos de acceso de todos los empleados y terceras partes, a la información y a los recursos de tratamiento de la información deben ser retirados a la finalización del empleo, del contrato o del acuerdo, o ajustados en caso de cambio.
		A.9.4.1	Restricción del acceso a la información	Se debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.
		A.9.4.4	Uso de utilidades con privilegios del sistema	Se debe restringir y controlar rigurosamente el uso de utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación.
A42	Acceso electrónico no autorizado a sistemas internos	A.9.2.1	Registro y baja de usuario	Debe implantarse un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso.
		A.9.2.2	Provisión de acceso de usuario	Debe implantarse un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios.
		A.9.2.3	Gestión de privilegios de acceso	La asignación y el uso de privilegios de acceso debe estar restringida y controlada.
		A.9.2.5	Revisión de los derechos de acceso de usuario	Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares.
		A.9.2.6	Retirada o reasignación de los derechos de acceso	Los derechos de acceso de todos los empleados y terceras partes, a la información y a los recursos de tratamiento de la información deben ser retirados a la finalización del empleo, del contrato o del acuerdo, o ajustados en caso de cambio.
		A.9.4.1	Restricción del acceso a la información	Se debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.

5. PRODUCTOS INSTITUCIONALES / MAGNITUD DE DAÑO: 4				
Código Amenaza	Amenaza	Código ISO	Descripción	Control
		A.9.4.4	Uso de utilidades con privilegios del sistema	Se debe restringir y controlar rigurosamente el uso de utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación.
A44	Red inalámbrica expuesta al acceso no autorizado	A.9.1.1	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.
		A.9.1.2	Acceso a las redes y a los servicios de red	Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.
		A.13.1.1	Controles de red	Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.
		A.13.1.2	Seguridad de los servicios de red	Se deben identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.
		A.13.1.3	Segregación en redes	Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en redes distintas.
A45	Dependencia a servicio técnico externo	A.15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	Los acuerdos con proveedores deben incluir requisitos para hacer frente a los riesgos de seguridad de la información relacionados con las tecnologías de la información y las comunicaciones y con la cadena de suministro de productos.
A46	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	A.5.1.1	Políticas para la seguridad de la información	Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.
A47	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	A.5.1.2	Revisión de las políticas para la seguridad de la información	Las políticas de seguridad de la información deben revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.
		A.18.2.1	Revisión independiente de la seguridad de la información	El enfoque de la organización para la gestión de la seguridad de la información y su implantación, es decir, objetivos de control, contr oles, políticas, procesos y procedimientos para la seguridad de la información, debe someterse a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos en la implantación de la seguridad.

5. PRODUCTOS INSTITUCIONALES / MAGNITUD DE DAÑO: 4				
Código Amenaza	Amenaza	Código ISO	Descripción	Control
		A.18.2.2	Cumplimiento de las políticas y normas de seguridad	Los directivos deben asegurarse que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente con el fin de cumplir las políticas y normas de seguridad y cualquier otro requisito de seguridad aplicable
A48	Ausencia de documentación	A.5.1.1	Políticas para la seguridad de la información	Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.

6. CORREO ELECTRÓNICO / MAGNITUD DE DAÑO: 2				
Código Amenaza	Amenaza	Código ISO	Descripción	Control
A9	Robo / Hurto de información electrónica	A.8.3.1	Gestión de soportes extraíbles	Se deben implementar procedimientos para la gestión de los soportes extraíbles, de acuerdo con el esquema de clasificación adoptado por la organización.
		A.8.3.2	Eliminación de soportes	Los soportes deben eliminarse de forma segura cuando ya no vayan a ser necesarios, mediante procedimientos formales.
		A.8.3.3	Soportes físicos en tránsito	Durante el transporte fuera de los límites físicos de la organización, los soportes que contengan información deben estar protegidos contra accesos no autorizados, usos indebidos o deterioro.
		A.9.1.1	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.
		A.9.1.2	Acceso a las redes y a los servicios de red	Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.
A10	Intrusión a red interna	A.9.1.1	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.
		A.9.1.2	Acceso a las redes y a los servicios de red	Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.
		A.13.1.1	Controles de red	Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.
		A.13.1.2	Seguridad de los servicios de red	Se deben identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.

6. CORREO ELECTRÓNICO / MAGNITUD DE DAÑO: 2				
Código Amenaza	Amenaza	Código ISO	Descripción	Control
		A.13.1.3	Segregación en redes	Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en redes distintas.
A11	Infiltración	A.9.1.1	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.
		A.9.1.2	Acceso a las redes y a los servicios de red	Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.
		A.13.1.1	Controles de red	Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.
		A.13.1.2	Seguridad de los servicios de red	Se deben identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.
		A.13.1.3	Segregación en redes	Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en redes distintas.
A12	Virus / Ejecución no autorizado de programas	A.12.1.1	Documentación de procedimientos operacionales	Deben documentarse y mantenerse procedimientos operacionales y ponerse a disposición de todos los usuarios que los necesiten.
		A.12.6.1	Gestión de las vulnerabilidades técnicas	Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.
		A.12.6.2	Restricción en la instalación de software	Se deben establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios.
A22	Falla de sistema / Daño disco duro	A.12.3.1	Copias de seguridad de la información	Se deben realizar copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo a la política de copias de seguridad acordada.
A23	Falta de inducción, capacitación y sensibilización sobre riesgos	A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.

6. CORREO ELECTRÓNICO / MAGNITUD DE DAÑO: 2				
Código Amenaza	Amenaza	Código ISO	Descripción	Control
A24	Mal manejo de sistemas y herramientas	A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.
		A.9.3.1	Uso de la información secreta de autenticación	Se debe requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.
A27	Perdida de datos	A.12.3.1	Copias de seguridad de la información	Se deben realizar copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo a la política de copias de seguridad acordada.
		A.17.2.1	Disponibilidad de los recursos de tratamiento de la información	Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.
A29	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.
		A.9.4.1	Restricción del acceso a la información	Se debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.
A30	Unidades portables con información sin cifrado	A.8.3.1	Gestión de soportes extraíbles	Se deben implementar procedimientos para la gestión de los soportes extraíbles, de acuerdo con el esquema de clasificación adoptado por la organización.
		A.10.1.1	Política de uso de los controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de los controles criptográficos para proteger la información.
		A.10.1.2	Gestión de claves	Se debe desarrollar e implementar una política sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida.
A39	Falta de actualización de software (proceso y recursos)	A.11.2.4	Mantenimiento de los equipos	Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas.
A41	Acceso electrónico no autorizado a	A.9.2.1	Registro y baja de usuario	Debe implantarse un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso.

6. CORREO ELECTRÓNICO / MAGNITUD DE DAÑO: 2				
Código Amenaza	Amenaza	Código ISO	Descripción	Control
	sistemas externos	A.9.2.2	Provisión de acceso de usuario	Debe implantarse un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios.
		A.9.2.3	Gestión de privilegios de acceso	La asignación y el uso de privilegios de acceso debe estar restringida y controlada.
		A.9.2.5	Revisión de los derechos de acceso de usuario	Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares.
		A.9.2.6	Retirada o reasignación de los derechos de acceso	Los derechos de acceso de todos los empleados y terceras partes, a la información y a los recursos de tratamiento de la información deben ser retirados a la finalización del empleo, del contrato o del acuerdo, o ajustados en caso de cambio.
		A.9.4.1	Restricción del acceso a la información	Se debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.
		A.9.4.4	Uso de utilidades con privilegios del sistema	Se debe restringir y controlar rigurosamente el uso de utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación.

7. BASE DE DATOS INTERNOS / MAGNITUD DE DAÑO: 3				
Código Amenaza	Amenaza	Código ISO	Descripción	Control
A5	Daño por vandalismo	A.11.1.1	Perímetro de seguridad física	Se deben utilizar perímetros de seguridad para proteger las áreas que contienen información sensible, así como los recursos de tratamiento de la información.
		A.11.1.2	Controles físicos de entrada	Las áreas seguras deben estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.
A9	Robo / Hurto de información electrónica	A.8.3.1	Gestión de soportes extraíbles	Se deben implementar procedimientos para la gestión de los soportes extraíbles, de acuerdo con el esquema de clasificación adoptado por la organización.
		A.8.3.2	Eliminación de soportes	Los soportes deben eliminarse de forma segura cuando ya no vayan a ser necesarios, mediante procedimientos formales.
		A.8.3.3	Soportes físicos en tránsito	Durante el transporte fuera de los límites físicos de la organización, los soportes que contengan información deben estar protegidos contra accesos no autorizados, usos indebidos o deterioro.

7. BASE DE DATOS INTERNOS / MAGNITUD DE DAÑO: 3				
Código Amenaza	Amenaza	Código ISO	Descripción	Control
		A.9.1.1	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.
		A.9.1.2	Acceso a las redes y a los servicios de red	Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.
A10	Intrusión a red interna	A.9.1.1	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.
		A.9.1.2	Acceso a las redes y a los servicios de red	Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.
		A.13.1.1	Controles de red	Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.
		A.13.1.2	Seguridad de los servicios de red	Se deben identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.
		A.13.1.3	Segregación en redes	Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en redes distintas.
A12	Virus / Ejecución no autorizado de programas	A.12.1.1	Documentación de procedimientos operacionales	Deben documentarse y mantenerse procedimientos operacionales y ponerse a disposición de todos los usuarios que los necesiten.
		A.12.6.1	Gestión de las vulnerabilidades técnicas	Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.
		A.12.6.2	Restricción en la instalación de software	Se deben establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios.
A22	Falla de sistema / Daño disco duro	A.12.3.1	Copias de seguridad de la información	Se deben realizar copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo a la política de copias de seguridad acordada.
A23	Falta de inducción, capacitación y sensibilización sobre riesgos	A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.

7. BASE DE DATOS INTERNOS / MAGNITUD DE DAÑO: 3				
Código Amenaza	Amenaza	Código ISO	Descripción	Control
A24	Mal manejo de sistemas y herramientas	A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.
		A.9.3.1	Uso de la información secreta de autenticación	Se debe requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.
A27	Perdida de datos	A.12.3.1	Copias de seguridad de la información	Se deben realizar copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo a la política de copias de seguridad acordada.
		A.17.2.1	Disponibilidad de los recursos de tratamiento de la información	Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.
A29	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.
		A.9.4.1	Restricción del acceso a la información	Se debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.
A30	Unidades portables con información sin cifrado	A.8.3.1	Gestión de soportes extraíbles	Se deben implementar procedimientos para la gestión de los soportes extraíbles, de acuerdo con el esquema de clasificación adoptado por la organización.
		A.10.1.1	Política de uso de los controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de los controles criptográficos para proteger la información.
		A.10.1.2	Gestión de claves	Se debe desarrollar e implementar una política sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida.
A38	Falta de mantenimiento físico (proceso, repuestos e insumos)	A.11.2.4	Mantenimiento de los equipos	Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas.

7. BASE DE DATOS INTERNOS / MAGNITUD DE DAÑO: 3				
Código Amenaza	Amenaza	Código ISO	Descripción	Control
A39	Falta de actualización de software (proceso y recursos)	A.11.2.4	Mantenimiento de los equipos	Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas.
A41	Acceso electrónico no autorizado a sistemas externos	A.9.2.1	Registro y baja de usuario	Debe implantarse un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso.
		A.9.2.2	Provisión de acceso de usuario	Debe implantarse un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios.
		A.9.2.3	Gestión de privilegios de acceso	La asignación y el uso de privilegios de acceso debe estar restringida y controlada.
		A.9.2.5	Revisión de los derechos de acceso de usuario	Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares.
		A.9.2.6	Retirada o reasignación de los derechos de acceso	Los derechos de acceso de todos los empleados y terceras partes, a la información y a los recursos de tratamiento de la información deben ser retirados a la finalización del empleo, del contrato o del acuerdo, o ajustados en caso de cambio.
		A.9.4.1	Restricción del acceso a la información	Se debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.
		A.9.4.4	Uso de utilidades con privilegios del sistema	Se debe restringir y controlar rigurosamente el uso de utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación.
A45	Dependencia a servicio técnico externo	A.15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	Los acuerdos con proveedores deben incluir requisitos para hacer frente a los riesgos de seguridad de la información relacionados con las tecnologías de la información y las comunicaciones y con la cadena de suministro de productos.
A46	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	A.5.1.1	Políticas para la seguridad de la información	Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.
A47	Falta de mecanismos de verificación de normas y reglas / Análisis	A.5.1.2	Revisión de las políticas para la seguridad de la información	Las políticas de seguridad de la información deben revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

7. BASE DE DATOS INTERNOS / MAGNITUD DE DAÑO: 3				
Código Amenaza	Amenaza	Código ISO	Descripción	Control
	inadecuado de datos de control	A.18.2.1	Revisión independiente de la seguridad de la información	El enfoque de la organización para la gestión de la seguridad de la información y su implantación, es decir, objetivos de control, contr oles, políticas, procesos y procedimientos para la seguridad de la información, debe someterse a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos en la implantación de la seguridad.
		A.18.2.2	Cumplimiento de las políticas y normas de seguridad	Los directivos deben asegurarse que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente con el fin de cumplir las políticas y normas de seguridad y cualquier otro requisito de seguridad aplicable
A48	Ausencia de documentación	A.5.1.1	Políticas para la seguridad de la información	Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.

8. BASE DE DATOS EXTERNOS / MAGNITUD DE DAÑO: 2				
Código Amenaza	**Amenaza**	**Código ISO**	**Descripción**	**Control**
A24	Mal manejo de sistemas y herramientas	A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.
A39	Falta de actualización de software (proceso y recursos)	A.11.2.4	Mantenimiento de los equipos	Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas.
A45	Dependencia a servicio técnico externo	A.15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	Los acuerdos con proveedores deben incluir requisitos para hacer frente a los riesgos de seguridad de la información relacionados con las tecnologías de la información y las comunicaciones y con la cadena de suministro de productos.
A46	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	A.5.1.1	Políticas para la seguridad de la información	Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.

9. RESPALDOS / MAGNITUD DE DAÑO: 2				
Código Amenaza	**Amenaza**	**Código ISO**	**Descripción**	**Control**
A24	Mal manejo de sistemas y herramientas	A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.
A39	Falta de actualización de software (proceso y recursos)	A.11.2.4	Mantenimiento de los equipos	Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas.
A45	Dependencia a servicio técnico externo	A.15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	Los acuerdos con proveedores deben incluir requisitos para hacer frente a los riesgos de seguridad de la información relacionados con las tecnologías de la información y las comunicaciones y con la cadena de suministro de productos.
A46	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	A.5.1.1	Políticas para la seguridad de la información	Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.

10. BASE DE DATOS DE CONTRASEÑAS / MAGNITUD DE DAÑO: 2				
Código Amenaza	**Amenaza**	**Código ISO**	**Descripción**	**Control**
A24	Mal manejo de sistemas y herramientas	A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.
A39	Falta de actualización de software (proceso y recursos)	A.11.2.4	Mantenimiento de los equipos	Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas.
A45	Dependencia a servicio técnico externo	A.15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	Los acuerdos con proveedores deben incluir requisitos para hacer frente a los riesgos de seguridad de la información relacionados con las tecnologías de la información y las comunicaciones y con la cadena de suministro de productos.

10. BASE DE DATOS DE CONTRASEÑAS / MAGNITUD DE DAÑO: 2				
Código Amenaza	**Amenaza**	**Código ISO**	**Descripción**	**Control**
A46	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	A.5.1.1	Políticas para la seguridad de la información	Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.

4.3. Anexo 3: Listado de activos de TI que dan soporte a los productos institucionales

Activos de TI que dan soporte a productos institucionales		
N.º	**Descripción**	**Responsable**
1	Switch Core	Jefe de IT
2	Nodo FO	Jefe de IT
3	Switch LAN	Jefe de IT
4	Clúster Servidores	Jefe de IT
5	Planta Telefónica	Jefe de IT
6	Switch Telefonía	Jefe de IT
7	Firewall	Jefe de IT
8	Sistema de control de acceso	RR. HH.
9	CCTV Interno	RR. HH.
10	NAS	Centro de Monitoreo
11	Cámaras	Supervisor Mantenimiento
12	Estaciones de trabajo	Centro de Monitoreo
13	UPS	Supervisor Mantenimiento
14	Aire Acondicionado	Supervisor Mantenimiento

PARTE III

RESULTADOS Y RECOMENDACIONES DE REMEDIACIÓN DEL ESCANEO DE VULNERABILIDADES DE LOS ACTIVOS TECNOLÓGICOS

PAGINAS DE LA 90 A LA 130

SOLTEC El Salvador, SA de CV

RESULTADOS Y RECOMENDACIONES DE REMEDIACIÓN DEL ESCANEO DE VULNERABILIDADES DE LOS ACTIVOS TECNOLÓGICOS

Código:	003
Versión:	1.0
Fecha de la versión:	20-06-2023
Creado por:	Víctor Manuel Escobar Avilés Ricardo Ernesto Esperanza Bonilla Oscar Enrique Santos Marcia
Aprobado por:	Luis Enrique Sánchez Flores
Nivel de confidencialidad:	Alto

TÉRMINOS Y CONDICIONES DE USO

Versión actual del documento: 1.0

El contenido de este texto es PRIVADO y la presente versión se considera un documento interno de trabajo.

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
20/06/23	1.0	Vescobar, Resperanza, Osantos	Modificaciones según requerimientos de gerencia.

Tabla de contenido

GLOSARIO DE TÉRMINOS 5

1. OBJETIVO 6

2. ALCANCE 6

3. EQUIPOS EVALUADOS 6

4. EJECUCIÓN DE ESCANEO DE VULNERABILIDADES 7

4.1 RESULTADOS OBTENIDOS MEDIANTE LA HERRAMIENTA TENABLE NESSUS ESSENTIALS. 7

A CONTINUACIÓN, SE MUESTRAN LOS RESULTADOS OBTENIDOS DEL ANÁLISIS DE VULNERABILIDADES DE CADA ACTIVO ESCANEADO. 7

4.1.1 Activo: AP01 8

4.1.2 Activo: CORE01 9

9

4.1.3 Activo: DATOS01 10

4.1.4 Activo: IVS3800-CSP 12

4.1.5 Activo: MAILSRVR01 13

13

4.1.6 Activo: NAGIOS01 15

16

4.1.7 Activo: OLT01 17

4.1.8 Activo: VMSRVR01 18

19

4.1.9 Activo: VOIP01 20

21

5. RECOMENDACIONES DE REMEDIACIÓN A LAS VULNERABILIDADES ENCONTRADAS. 23

Tabla de Ilustraciones

Ilustración 1 Escaneo de vulnerabilidaes AP01 8
Ilustración 2 Escaneo de vulnerabilidades CORE01 9
Ilustración 3 Escaneo de vulnerabilidades DATOS01 11
Ilustración 4 Escaneo de vulnerabilidades IVS3800-CSP 12
Ilustración 5 Escaneo de vulnerabilidades MAILSRVR01 14
Ilustración 6 Escaneo de vulnerabilidades NAGIOS01 16
Ilustración 7 Escaneo de vulnerabilidades OLT01 17
Ilustración 8 Escaneo de vulnerabilidades VMSRVR01 19
Ilustración 9 Escaneo de vulnerabilidades VOIP01 22

Tablas

Tabla 1 Listado de equipos evaluados. 6
Tabla 2 Recomendaciones para el activo DATOS01 (01) 23
Tabla 3 Recomendaciones para el activo DATOS01 (02) 24
Tabla 4 Recomendaciones para el activo MAILSRVR01 (01) 25
Tabla 5 Recomendaciones para el activo MAILSRVR01 (02) 26
Tabla 6 Recomendaciones para el activo MAILSRVR01 (03) 27
Tabla 7 Recomendaciones para el activo MAILSRVR01 (04) 28
Tabla 8 Recomendaciones para el activo NAGIOS01 (01) 29
Tabla 9 Recomendaciones para el activo NAGIOS01 (02) 30
Tabla 10 Recomendaciones para el activo NAGIOS01 (03) 31
Tabla 11 Recomendaciones para el activo NAGIOS01 (04) 32
Tabla 12 Recomendaciones para el activo NAGIOS01 (05) 33
Tabla 13 Recomendaciones para el activo NAGIOS01 (06) 34
Tabla 14 Recomendaciones para el activo OLT01 35
Tabla 15 Recomendaciones para el activo VMSRVR01 36
Tabla 16 Recomendaciones para el activo VOIP01(01) 37
Tabla 17 Recomendaciones para el activo VOIP01(02) 38
Tabla 18 Recomendaciones para el activo VOIP01(03) 39
Tabla 19 Recomendaciones para el activo VOIP01(04) 40
Tabla 20 Recomendaciones para el activo VOIP01(05) 41

Glosario de términos

- CVE (Common Vulnerabilities and Exposures): El CVE (Common Vulnerabilities and Exposures) es la lista de vulnerabilidades de seguridad de la información públicamente conocidas. Para llevar un control de esta lista a cada vulnerabilidad que se identifica se le asigna un código de identificación único conocido como identificador CVE (CVE-ID). Este identificador está formado por las siglas ID seguidas por el año en que es registrada la vulnerabilidad y un número consecutivo de cuatro dígitos.

- Tenable Nessus Essentials: es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en un Daemon, que realiza el escaneo en el sistema objetivo, y Nessus, el cliente (basado en consola o gráfico) que muestra el avance e informa sobre el estado de los escaneos.

- CVSS V3.0: es un sistema de puntuación que proporciona un método estándar y abierto para estimar el impacto de una vulnerabilidad y que se compone tres grupos principales de métricas: Base, Temporal y de Entorno (Environmental). Cada uno de estos grupos se compone a su vez de un conjunto de métricas. La primera versión del CVSS se lanzó en 2004 seguida de la versión 2 en 2007. En 2012 se inicia el proceso de actualización a la versión 3, en respuesta a observaciones realizadas por distintas organizaciones que mantienen bases de datos de referencia de vulnerabilidades como la National Vulnerability Database (NVDB) y Open Source Vulnerability Database (OSVD).

1. Objetivo

El objetivo de este documento es presentar de forma ejecutiva el resultado del Escaneo de Vulnerabilidades, realizado en los activos tecnológicos que dan soporte a los procesos de negocio de la empresa SOLTEC El Salvador S.A. de C.V., esto incluye: la descripción del escaneo realizado, los elementos evaluados y las vulnerabilidades identificadas junto con su nivel de criticidad como línea base de seguimiento, así como las conclusiones y recomendaciones de remediación.

2. Alcance

El escaneo realizado tuvo como alcance los activos tecnológicos de la Red Interna de acuerdo con el listado de equipos que posee la empresa SOLTEC El Salvador S.A. de C.V. El detalle de los equipos evaluados se presenta en la sección.

3. Equipos evaluados

A continuación, se presenta el listado de equipos evaluados:

Tabla 1 Listado de equipos evaluados.

N.º	Nombre de Activo	Propietario	Responsable	Tipo	Descripción
1	AP01	Jefe de TI	Jefe de TI	Hardware	Punto de acceso red Inalámbrica.
2	CORE01	Jefe de TI	Jefe de TI	Hardware	Switch central que concentra todo el tráfico de red.
3	DATOS01	Jefe de TI	Jefe de TI	Hardware	Switch para red interna.
4	IVS3800	Jefe de TI	Jefe de TI	Hardware	Servidores para aplicación de video y analítica.
5	MAILSRVR01	Jefe de TI	Jefe de TI	Virtualizado	Servidor de correo electrónico SMTP/POP3 interno.
6	NAGIOS01	Jefe de TI	Jefe de TI	Virtualizado	Servidor para el monitoreo de cámaras de video vigilancia.

N.º	Nombre de Activo	Propietario	Responsable	Tipo	Descripción
7	OLT01	Jefe de TI	Jefe de TI	Hardware	Nodo para red GPON.
8	VMSRVR01	Jefe de TI	Jefe de TI	Hardware	Servidor que provee múltiples servicios mediante virtualización.
9	VOIP01	Jefe de TI	Jefe de TI	Hardware	Switch para telefonía IP.

4. Ejecución de escaneo de vulnerabilidades

4.1 Resultados obtenidos mediante la herramienta Tenable Nessus Essentials.

A continuación, se muestran los resultados obtenidos del análisis de vulnerabilidades de cada activo escaneado.

4.1.1 Activo: AP01

192.168.50.18

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	1	13

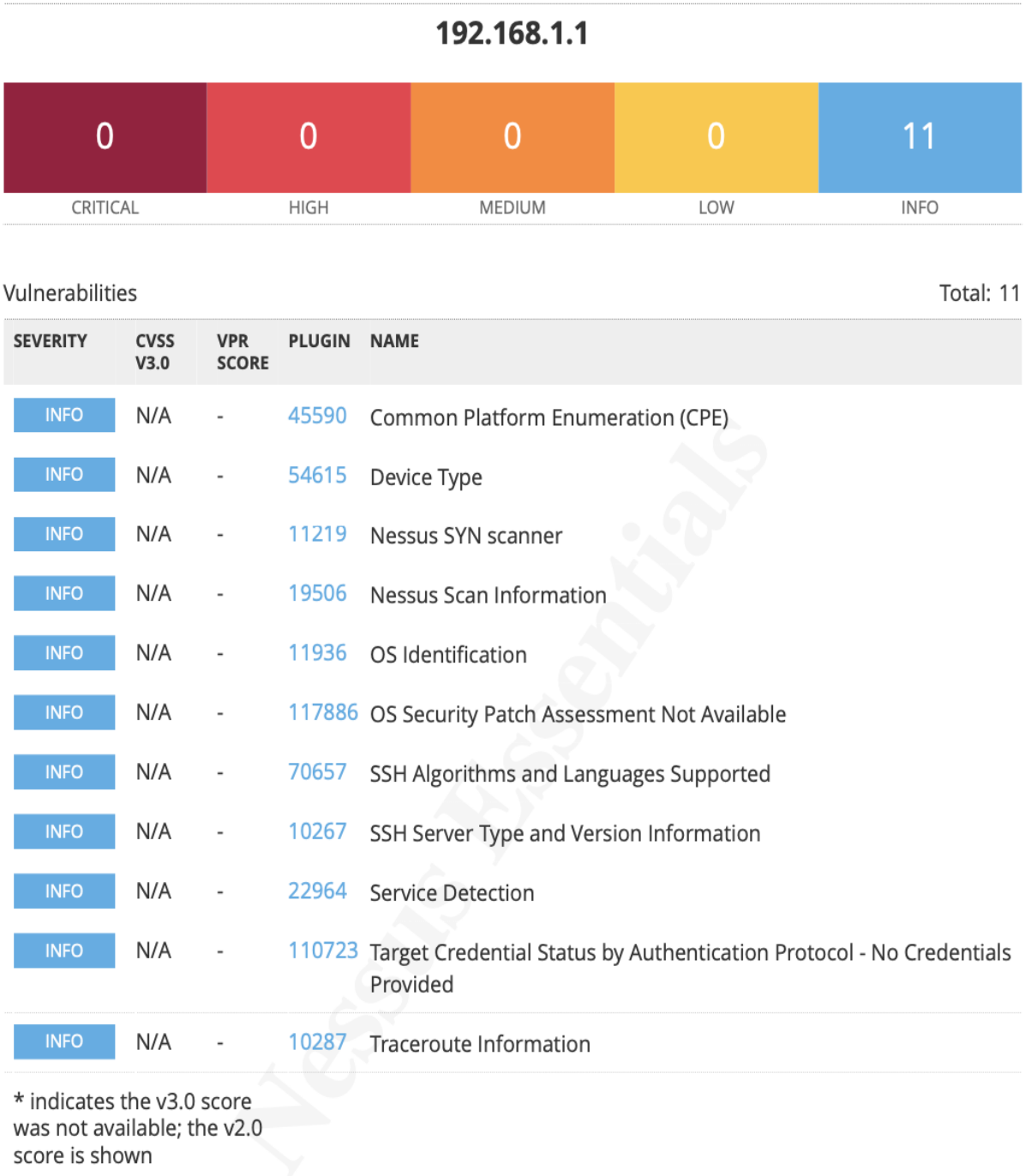
Vulnerabilities Total: 14

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	10267	SSH Server Type and Version Information
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information

* indicates the v3.0 score was not available; the v2.0 score is shown

Ilustración 1 Escaneo de vulnerabilidaes AP01

4.1.2 Activo: CORE01



192.168.1.1

0	0	0	0	11
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 11

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	10267	SSH Server Type and Version Information
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information

* indicates the v3.0 score was not available; the v2.0 score is shown

Ilustración 2 Escaneo de vulnerabilidades CORE01

4.1.3 Activo: DATOS01

10.10.1.12

0	0	2	1	24
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 27

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	42263	Unencrypted Telnet Server
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	42823	Non-compliant Strict Transport Security (STS)
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	10267	SSH Server Type and Version Information
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	21643	SSL Cipher Suites Supported

INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	42822	Strict Transport Security (STS) Detection
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10281	Telnet Server Detection
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	10386	Web Server No 404 Error Code Check

* indicates the v3.0 score was not available; the v2.0 score is shown

Ilustración 3 Escaneo de vulnerabilidades DATOS01

4.1.4 Activo: IVS3800-CSP

192.168.5.5

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	0	13

Vulnerabilities Total: 13

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	10267	SSH Server Type and Version Information
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information

* indicates the v3.0 score was not available; the v2.0 score is shown

Ilustración 4 Escaneo de vulnerabilidades IVS3800-CSP

4.1.5 Activo: MAILSRVR01

192.168.1.112

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	4	0	34

Vulnerabilities Total: 38

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	157288	TLS Version 1.1 Protocol Deprecated
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	11414	IMAP Service Banner Retrieval
INFO	N/A	-	42085	IMAP Service STARTTLS Command Support
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	50350	OS Identification Failed
INFO	N/A	-	50845	OpenSSL Detection
INFO	N/A	-	10185	POP Server Detection
INFO	N/A	-	42087	POP3 Service STLS Command Support
INFO	N/A	-	10263	SMTP Server Detection
INFO	N/A	-	42088	SMTP Service STARTTLS Command Support
INFO	N/A	-	70657	SSH Algorithms and Languages Supported

INFO	N/A	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	10267	SSH Server Type and Version Information
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	94761	SSL Root Certification Authority Certificate Information
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	62564	TLS Next Protocols Supported
INFO	N/A	-	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	138330	TLS Version 1.3 Protocol Detection
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	10302	Web Server robots.txt Information Disclosure
INFO	N/A	-	106375	nginx HTTP Server Detection

* indicates the v3.0 score was not available; the v2.0 score is shown

Ilustración 5 Escaneo de vulnerabilidades MAILSRVR01

4.1.6 Activo: NAGIOS01

192.168.1.111

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	6	0	36

Vulnerabilities Total: 42

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	157288	TLS Version 1.1 Protocol Deprecated
MEDIUM	5.9	3.6	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.3	-	15901	SSL Certificate Expiry
INFO	N/A	-	10223	RPC portmapper Service Detection
INFO	N/A	-	48204	Apache HTTP Server Version
INFO	N/A	-	39521	Backported Security Patch Detection (WWW)
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available

INFO	N/A	-	50845	OpenSSL Detection
INFO	N/A	-	11111	RPC Services Enumeration
INFO	N/A	-	53335	RPC portmapper (TCP)
INFO	N/A	-	10263	SMTP Server Detection
INFO	N/A	-	42088	SMTP Service STARTTLS Command Support
INFO	N/A	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	10267	SSH Server Type and Version Information
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	138330	TLS Version 1.3 Protocol Detection
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	10386	Web Server No 404 Error Code Check

* indicates the v3.0 score was not available; the v2.0 score is shown

Ilustración 6 Escaneo de vulnerabilidades NAGIOS01

4.1.7 Activo: OLT01

10.10.1.11

0	0	1	1	14
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 16

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	-	42263	Unencrypted Telnet Server
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	10267	SSH Server Type and Version Information
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10281	Telnet Server Detection
INFO	N/A	-	10287	Traceroute Information

* indicates the v3.0 score was not available; the v2.0 score is shown

Ilustración 7 Escaneo de vulnerabilidades OLT01

4.1.8 Activo: VMSRVR01

192.168.1.110

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	1	0	23

Vulnerabilities Total: 24

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	2.5	18405	Remote Desktop Protocol Server Man-in-the-Middle Weakness
INFO	N/A	-	10223	RPC portmapper Service Detection
INFO	N/A	-	48204	Apache HTTP Server Version
INFO	N/A	-	39521	Backported Security Patch Detection (WWW)
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	11111	RPC Services Enumeration
INFO	N/A	-	53335	RPC portmapper (TCP)
INFO	N/A	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	10881	SSH Protocol Versions Supported

INFO	N/A	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	10267	SSH Server Type and Version Information
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information

* indicates the v3.0 score was not available; the v2.0 score is shown

Ilustración 8 Escaneo de vulnerabilidades VMSRVR01

4.1.9 Activo: VOIP01

192.168.30.250

Vulnerabilities Total: 46

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	157288	TLS Version 1.1 Protocol Deprecated
MEDIUM	5.9	3.6	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.3	-	15901	SSL Certificate Expiry
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	2.6*	2.5	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
LOW	N/A	-	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	20834	Inter-Asterisk eXchange Protocol Detection
INFO	N/A	-	106658	JQuery Detection
INFO	N/A	-	20870	LDAP Server Detection
INFO	N/A	-	42329	LDAP Service STARTTLS Command Support

INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	10267	SSH Server Type and Version Information
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	62563	SSL Compression Methods Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	94761	SSL Root Certification Authority Certificate Information
INFO	N/A	-	35297	SSL Service Requests Client Certificate
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	17975	Service Detection (GET request)
INFO	N/A	-	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	10386	Web Server No 404 Error Code Check

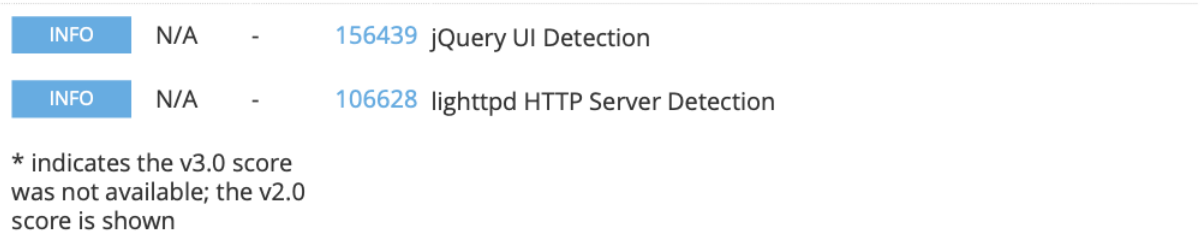


Ilustración 9 Escaneo de vulnerabilidades VOIP01

5. Recomendaciones de remediación a las vulnerabilidades encontradas.

A continuación, se detallan los equipos con severidades críticas, altas y medias, encontradas en el escaneo de vulnerabilidad.

Tabla 2 Recomendaciones para el activo DATOS01 (01)

Nombre del Activo y dirección IP	Vulnerabilidad y severidad
DATOS01 10.10.1.12	SSL Certificate Cannot Be Trusted (No se puede confiar en el certificado SSL para este servicio) MEDIA
Descripción	
No se puede confiar en el certificado X.509 del servidor. Esta situación puede darse de tres formas distintas, en las que se puede romper la cadena de confianza, como se expone a continuación: • En primer lugar, es posible que la parte superior de la cadena de certificados enviada por el servidor no descienda de una autoridad de certificación pública conocida. Esto puede ocurrir cuando la parte superior de la cadena es un certificado autofirmado no reconocido, o cuando faltan certificados intermedios que conectarían la parte superior de la cadena de certificados con una autoridad de certificación pública conocida. • En segundo lugar, la cadena de certificados puede contener un certificado que no sea válido en el momento de la exploración. Esto puede ocurrir cuando la exploración ocurre antes de una de las fechas 'notBefore' del certificado o después de una de las fechas 'notAfter' del certificado. • En tercer lugar, la cadena de certificados puede contener una firma que no coincide con la información del certificado o que no se pudo verificar. Las malas firmas se pueden corregir haciendo que el emisor vuelva a firmar el certificado con la mala firma. Las firmas que no se pudieron verificar son el resultado de que el emisor del certificado utilizó un algoritmo de firma que Nessus no admite o no reconoce. Si el host remoto es un host público en producción, cualquier interrupción en la cadena dificulta que los usuarios verifiquen la autenticidad y la identidad del servidor web. Esto podría facilitar la realización de ataques man-in-the-middle contra el host remoto.	

Solución

Compre o genere un certificado SSL adecuado para este servicio.

Tabla 3 Recomendaciones para el activo DATOS01 (02)

Nombre del Activo y dirección IP	Vulnerabilidad y severidad
DATOS01 10.10.1.12	Unencrypted Telnet Server (El servidor Telnet remoto transmite el tráfico en texto claro) MEDIA
Descripción	
El host remoto ejecuta un servidor Telnet a través de un canal no cifrado. No se recomienda usar Telnet en un canal sin cifrar, ya que los inicios de sesión, las contraseñas y los comandos se transfieren en texto no cifrado. Esto permite que un atacante remoto intermediario espíe una sesión de Telnet para obtener credenciales u otra información confidencial y modificar el tráfico intercambiado entre un cliente y un servidor. Se prefiere SSH a Telnet, ya que protege las credenciales de escuchas ilegales y puede canalizar flujos de datos adicionales, como una sesión X11.	

Solución

Deshabilite el servicio Telnet y use SSH en su lugar.

Tabla 4 Recomendaciones para el activo MAILSRVR01 (01)

Nombre del Activo y dirección IP	Vulnerabilidad y severidad
MAILSRVR01 192.168.1.112	SSL Certificate Cannot Be Trusted (No se puede confiar en el certificado SSL para este servicio) MEDIA
Descripción	
No se puede confiar en el certificado X.509 del servidor. Esta situación puede darse de tres formas distintas, en las que se puede romper la cadena de confianza, como se expone a continuación: • En primer lugar, es posible que la parte superior de la cadena de certificados enviada por el servidor no descienda de una autoridad de certificación pública conocida. Esto puede ocurrir cuando la parte superior de la cadena es un certificado autofirmado no reconocido, o cuando faltan certificados intermedios que conectarían la parte superior de la cadena de certificados con una autoridad de certificación pública conocida. • En segundo lugar, la cadena de certificados puede contener un certificado que no sea válido en el momento de la exploración. Esto puede ocurrir cuando la exploración ocurre antes de una de las fechas 'notBefore' del certificado o después de una de las fechas 'notAfter' del certificado. • En tercer lugar, la cadena de certificados puede contener una firma que no coincide con la información del certificado o que no se pudo verificar. Las malas firmas se pueden corregir haciendo que el emisor vuelva a firmar el certificado con la mala firma. Las firmas que no se pudieron verificar son el resultado de que el emisor del certificado utilizó un algoritmo de firma que Nessus no admite o no reconoce. Si el host remoto es un host público en producción, cualquier interrupción en la cadena dificulta que los usuarios verifiquen la autenticidad y la identidad del servidor web. Esto podría facilitar la realización de ataques man-in-the-middle contra el host remoto.	

Solución

Compre o genere un certificado SSL adecuado para este servicio.

Tabla 5 Recomendaciones para el activo MAILSRVR01 (02)

Nombre del Activo y dirección IP	Vulnerabilidad y severidad
MAILSRVR01 192.168.1.112	SSL Self-Signed Certificate (La cadena de certificados SSL para este servicio termina en un certificado autofirmado no reconocido) MEDIA
Descripción	
La cadena de certificados X.509 para este servicio no está firmada por una autoridad de certificación reconocida. Si el host remoto es un host público en producción, esto anula el uso de SSL, ya que cualquiera podría establecer un ataque de intermediario contra el host remoto. Tenga en cuenta que este complemento no comprueba las cadenas de certificados que terminan en un certificado que no está autofirmado, sino que está firmado por una autoridad de certificación no reconocida.	

Solución

Compre o genere un certificado SSL adecuado para este servicio.

Tabla 6 Recomendaciones para el activo MAILSRVR01 (03)

Nombre del Activo y dirección IP	Vulnerabilidad y severidad
MAILSRVR01 192.168.1.112	TLS Version 1.0 Protocol Detection (El servicio remoto encripta el tráfico utilizando una versión anterior de TLS) MEDIA
Descripción	
El servicio remoto acepta conexiones cifradas mediante TLS 1.0. TLS 1.0 tiene varios defectos de diseño criptográfico. Las implementaciones modernas de TLS 1.0 mitigan estos problemas, pero las versiones más nuevas de TLS como 1.2 y 1.3 están diseñadas para estos defectos y deben usarse siempre que sea posible. A partir del 31 de marzo de 2020, los puntos finales que no estén habilitados para TLS 1.2 y superior ya no funcionarán correctamente con los principales navegadores web y los principales proveedores. PCI DSS v3.2 requiere que TLS 1.0 se deshabilite por completo antes del 30 de junio de 2018, excepto para terminales POS POI (y los puntos de terminación SSL/TLS a los que se conectan) que se puede verificar que no son susceptibles a ningún exploit conocido.	

Solución

Habilite la compatibilidad con TLS 1.2 y 1.3 y deshabilite la compatibilidad con TLS 1.0.

Tabla 7 Recomendaciones para el activo MAILSRVR01 (04)

Nombre del Activo y dirección IP	Vulnerabilidad y severidad
MAILSRVR01 192.168.1.112	TLS Version 1.1 Protocol Deprecated (El servicio remoto encripta el tráfico utilizando una versión anterior de TLS) MEDIA
Descripción	
El servicio remoto acepta conexiones cifradas mediante TLS 1.1. TLS 1.1 no es compatible con los conjuntos de cifrado actuales y recomendados. Los cifrados que admiten el cifrado antes del cálculo MAC y los modos de cifrado autenticado, como GCM, no se pueden usar con TLS 1.1 A partir del 31 de marzo de 2020, los puntos finales que no estén habilitados para TLS 1.2 y superior ya no funcionarán correctamente con los principales navegadores web y los principales proveedores.	

Solución

Habilite la compatibilidad con TLS 1.2 y/o 1.3 y deshabilite la compatibilidad con TLS 1.1.

Tabla 8 Recomendaciones para el activo NAGIOS01 (01)

Nombre del Activo y dirección IP	Vulnerabilidad y severidad
NAGIOS01 192.168.1.111	SSL Certificate Cannot Be Trusted (No se puede confiar en el certificado SSL para este servicio) MEDIA
Descripción	
No se puede confiar en el certificado X.509 del servidor. Esta situación puede darse de tres formas distintas, en las que se puede romper la cadena de confianza, como se expone a continuación: • En primer lugar, es posible que la parte superior de la cadena de certificados enviada por el servidor no descienda de una autoridad de certificación pública conocida. Esto puede ocurrir cuando la parte superior de la cadena es un certificado autofirmado no reconocido, o cuando faltan certificados intermedios que conectarían la parte superior de la cadena de certificados con una autoridad de certificación pública conocida. • En segundo lugar, la cadena de certificados puede contener un certificado que no sea válido en el momento de la exploración. Esto puede ocurrir cuando la exploración ocurre antes de una de las fechas 'notBefore' del certificado o después de una de las fechas 'notAfter' del certificado. • En tercer lugar, la cadena de certificados puede contener una firma que no coincide con la información del certificado o que no se pudo verificar. Las malas firmas se pueden corregir haciendo que el emisor vuelva a firmar el certificado con la mala firma. Las firmas que no se pudieron verificar son el resultado de que el emisor del certificado utilizó un algoritmo de firma que Nessus no admite o no reconoce. Si el host remoto es un host público en producción, cualquier interrupción en la cadena dificulta que los usuarios verifiquen la autenticidad y la identidad del servidor web. Esto podría facilitar la realización de ataques man-in-the-middle contra el host remoto.	

Solución

Compre o genere un certificado SSL adecuado para este servicio.

Tabla 9 Recomendaciones para el activo NAGIOS01 (02)

Nombre del Activo y dirección IP	Vulnerabilidad y severidad
NAGIOS01 192.168.1.111	SSL Self-Signed Certificate (La cadena de certificados SSL para este servicio termina en un certificado autofirmado no reconocido) MEDIA
Descripción	
La cadena de certificados X.509 para este servicio no está firmada por una autoridad de certificación reconocida. Si el host remoto es un host público en producción, esto anula el uso de SSL, ya que cualquiera podría establecer un ataque de intermediario contra el host remoto. Tenga en cuenta que este complemento no comprueba las cadenas de certificados que terminan en un certificado que no está autofirmado, sino que está firmado por una autoridad de certificación no reconocida.	

Solución

Compre o genere un certificado SSL adecuado para este servicio.

Tabla 10 Recomendaciones para el activo NAGIOS01 (03)

Nombre del Activo y dirección IP	Vulnerabilidad y severidad
NAGIOS01 192.168.1.111	TLS Version 1.0 Protocol Detection (El servicio remoto encripta el tráfico utilizando una versión anterior de TLS) MEDIA
Descripción	
El servicio remoto acepta conexiones cifradas mediante TLS 1.0. TLS 1.0 tiene varios defectos de diseño criptográfico. Las implementaciones modernas de TLS 1.0 mitigan estos problemas, pero las versiones más nuevas de TLS como 1.2 y 1.3 están diseñadas para estos defectos y deben usarse siempre que sea posible. A partir del 31 de marzo de 2020, los puntos finales que no estén habilitados para TLS 1.2 y superior ya no funcionarán correctamente con los principales navegadores web y los principales proveedores. PCI DSS v3.2 requiere que TLS 1.0 se deshabilite por completo antes del 30 de junio de 2018, excepto para terminales POS POI (y los puntos de terminación SSL/TLS a los que se conectan) que se puede verificar que no son susceptibles a ningún exploit conocido.	

Solución

Habilite la compatibilidad con TLS 1.2 y 1.3 y deshabilite la compatibilidad con TLS 1.0.

Tabla 11 Recomendaciones para el activo NAGIOS01 (04)

Nombre del Activo y dirección IP	Vulnerabilidad y severidad
NAGIOS01 192.168.1.111	TLS Version 1.1 Protocol Deprecated (El servicio remoto encripta el tráfico utilizando una versión anterior de TLS) MEDIA
Descripción	
El servicio remoto acepta conexiones cifradas mediante TLS 1.1. TLS 1.1 no es compatible con los conjuntos de cifrado actuales y recomendados. Los cifrados que admiten el cifrado antes del cálculo MAC y los modos de cifrado autenticado, como GCM, no se pueden usar con TLS 1.1 A partir del 31 de marzo de 2020, los puntos finales que no estén habilitados para TLS 1.2 y superior ya no funcionarán correctamente con los principales navegadores web y los principales proveedores.	

Solución

Habilite la compatibilidad con TLS 1.2 y/o 1.3 y deshabilite la compatibilidad con TLS 1.1.

Tabla 12 Recomendaciones para el activo NAGIOS01 (05)

Nombre del Activo y dirección IP	Vulnerabilidad y severidad
NAGIOS01 192.168.1.111	SSL Anonymous Cipher Suites Supported (El servicio remoto admite el uso de cifrados SSL anónimos) MEDIA
Descripción	
El host remoto admite el uso de cifrados SSL anónimos. Si bien esto permite que un administrador configure un servicio que encripta el tráfico sin tener que generar y configurar certificados SSL, no ofrece ninguna forma de verificar la identidad del host remoto y hace que el servicio sea vulnerable a un ataque de intermediario. Nota: Esto es considerablemente más fácil de explotar si el atacante está en la misma red física.	

Solución

Vuelva a configurar la aplicación afectada si es posible para evitar el uso de cifrados débiles.

Tabla 13 Recomendaciones para el activo NAGIOS01 (06)

Nombre del Activo y dirección IP	Vulnerabilidad y severidad
NAGIOS01 192.168.1.111	SSL Certificate Expiry (El certificado SSL del servidor remoto ya ha caducado) MEDIA
Descripción	
Este complemento comprueba las fechas de caducidad de los certificados asociados con los servicios habilitados para SSL en el destino e informa si alguno ya ha caducado.	

Solución

Compre o genere un nuevo certificado SSL para reemplazar el existente.

Tabla 14 Recomendaciones para el activo OLT01

Nombre del Activo y dirección IP	Vulnerabilidad y severidad
OLT01 10.10.1.11	Unencrypted Telnet Server (El servidor Telnet remoto transmite el tráfico en texto claro) MEDIA
Descripción	
El host remoto ejecuta un servidor Telnet a través de un canal no cifrado. No se recomienda usar Telnet en un canal sin cifrar, ya que los inicios de sesión, las contraseñas y los comandos se transfieren en texto no cifrado. Esto permite que un atacante remoto intermediario espíe una sesión de Telnet para obtener credenciales u otra información confidencial y modificar el tráfico intercambiado entre un cliente y un servidor. Se prefiere SSH a Telnet, ya que protege las credenciales de escuchas ilegales y puede canalizar flujos de datos adicionales, como una sesión X11.	

Solución

Deshabilite el servicio Telnet y use SSH en su lugar.

Tabla 15 Recomendaciones para el activo VMSRVR01

Nombre del Activo y dirección IP	Vulnerabilidad y severidad
VMSRVR01 192.168.1.110	Remote Desktop Protocol Server Man-in-the-Middle Weakness (La versión remota del servidor de protocolo de escritorio remoto (Terminal Service) es vulnerable a un ataque de intermediario (MiTM)) MEDIA
Descripción	
El cliente RDP no hace ningún esfuerzo por validar la identidad del servidor al configurar el cifrado. Un atacante con la capacidad de interceptar el tráfico del servidor RDP puede establecer el cifrado con el cliente y el servidor sin ser detectado. Un ataque MiTM de esta naturaleza permitiría al atacante obtener cualquier información confidencial transmitida, incluidas las credenciales de autenticación. Esta falla existe porque el servidor RDP almacena una clave privada RSA codificada públicamente conocida. Cualquier atacante en una ubicación de red privilegiada puede usar la clave para este ataque.	

Solución

- **Forzar el uso de SSL como capa de transporte para este servicio si es compatible.**

- **En los sistemas operativos Microsoft Windows, seleccione la configuración 'Permitir conexiones solo desde computadoras que ejecutan Escritorio remoto con autenticación de nivel de red' si está disponible.**

Tabla 16 Recomendaciones para el activo VOIP01(01)

Nombre del Activo y dirección IP	Vulnerabilidad y severidad
VOIP01 192.168.30.250	SSL Certificate Cannot Be Trusted (No se puede confiar en el certificado SSL para este servicio) MEDIA
Descripción	
No se puede confiar en el certificado X.509 del servidor. Esta situación puede darse de tres formas distintas, en las que se puede romper la cadena de confianza, como se expone a continuación: • En primer lugar, es posible que la parte superior de la cadena de certificados enviada por el servidor no descienda de una autoridad de certificación pública conocida. Esto puede ocurrir cuando la parte superior de la cadena es un certificado autofirmado no reconocido, o cuando faltan certificados intermedios que conectarían la parte superior de la cadena de certificados con una autoridad de certificación pública conocida. • En segundo lugar, la cadena de certificados puede contener un certificado que no sea válido en el momento de la exploración. Esto puede ocurrir cuando la exploración ocurre antes de una de las fechas 'notBefore' del certificado o después de una de las fechas 'notAfter' del certificado. • En tercer lugar, la cadena de certificados puede contener una firma que no coincide con la información del certificado o que no se pudo verificar. Las malas firmas se pueden corregir haciendo que el emisor vuelva a firmar el certificado con la mala firma. Las firmas que no se pudieron verificar son el resultado de que el emisor del certificado utilizó un algoritmo de firma que Nessus no admite o no reconoce. Si el host remoto es un host público en producción, cualquier interrupción en la cadena dificulta que los usuarios verifiquen la autenticidad y la identidad del servidor web. Esto podría facilitar la realización de ataques man-in-the-middle contra el host remoto.	

Solución

Compre o genere un certificado SSL adecuado para este servicio.

Tabla 17 Recomendaciones para el activo VOIP01(02)

Nombre del Activo y dirección IP	Vulnerabilidad y severidad
VOIP01 192.168.30.250	SSL Self-Signed Certificate (La cadena de certificados SSL para este servicio termina en un certificado autofirmado no reconocido) MEDIA
Descripción	
La cadena de certificados X.509 para este servicio no está firmada por una autoridad de certificación reconocida. Si el host remoto es un host público en producción, esto anula el uso de SSL, ya que cualquiera podría establecer un ataque de intermediario contra el host remoto. Tenga en cuenta que este complemento no comprueba las cadenas de certificados que terminan en un certificado que no está autofirmado, sino que está firmado por una autoridad de certificación no reconocida.	

Solución

Compre o genere un certificado SSL adecuado para este servicio.

Tabla 18 Recomendaciones para el activo VOIP01(03)

Nombre del Activo y dirección IP	Vulnerabilidad y severidad
VOIP01 192.168.30.250	TLS Version 1.1 Protocol Deprecated (El servicio remoto encripta el tráfico utilizando una versión anterior de TLS) MEDIA
Descripción	
El servicio remoto acepta conexiones cifradas mediante TLS 1.1. TLS 1.1 no es compatible con los conjuntos de cifrado actuales y recomendados. Los cifrados que admiten el cifrado antes del cálculo MAC y los modos de cifrado autenticado, como GCM, no se pueden usar con TLS 1.1 A partir del 31 de marzo de 2020, los puntos finales que no estén habilitados para TLS 1.2 y superior ya no funcionarán correctamente con los principales navegadores web y los principales proveedores.	

Solución

Habilite la compatibilidad con TLS 1.2 y/o 1.3 y deshabilite la compatibilidad con TLS 1.1.

Tabla 19 Recomendaciones para el activo VOIP01(04)

Nombre del Activo y dirección IP	Vulnerabilidad y severidad
VOIP01 192.168.30.250	SSL Anonymous Cipher Suites Supported (El servicio remoto admite el uso de cifrados SSL anónimos) MEDIA
Descripción	
El host remoto admite el uso de cifrados SSL anónimos. Si bien esto permite que un administrador configure un servicio que encripta el tráfico sin tener que generar y configurar certificados SSL, no ofrece ninguna forma de verificar la identidad del host remoto y hace que el servicio sea vulnerable a un ataque de intermediario. Nota: Esto es considerablemente más fácil de explotar si el atacante está en la misma red física.	

Solución

Vuelva a configurar la aplicación afectada si es posible para evitar el uso de cifrados débiles.

Tabla 20 Recomendaciones para el activo VOIP01(05)

Nombre del Activo y dirección IP	Vulnerabilidad y severidad
VOIP01 192.168.30.250	SSL Certificate Expiry (El certificado SSL del servidor remoto ya ha caducado) MEDIA
Descripción	
Este complemento comprueba las fechas de caducidad de los certificados asociados con los servicios habilitados para SSL en el destino e informa si alguno ya ha caducado.	

Solución

Compre o genere un nuevo certificado SSL para reemplazar el existente.