PLAN DE TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

CORPOCESAR
CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR

SUBDIRECCIÓN GENERAL ÁREA DE PLANEACIÓN
OFICINA DE SISTEMAS Y TICS

TABLA DE CONTENIDO

1. OBJETIVO 4
2. ALCANCE 4
3. DEFINICIONES 4
4. FACTORES DE RIESGOS 18
4. CATÁLOGO DE RIESGOS 19
RIESGO 1: MODIFICACIÓN NO AUTORIZADA DE LA INFORMACIÓN 23
RIESGO 2: PÉRDIDA, DESTRUCCIÓN O DAÑO DE LA INFORMACIÓN 27
RIESGO 3: INDISPONIBILIDAD DE LA INFORMACIÓN 30
RIESGO 4: HURTO POR PARTE DE PROPIOS O TERCEROS 32
RIESGO 5: DAÑO O SABOTAJE POR PARTE DE PROPIOS O TERCEROS 33
RIESGO 6: USO Y DIVULGACIÓN NO AUTORIZADA DE INFORMACIÓN CONFIDENCIAL 35
RIESGO 7: INCONSISTENCIAS EN LA INFORMACIÓN 37
RIESGO 8: ACCESO NO AUTORIZADO A LA INFORMACIÓN 39
5. REVISIÓN DE LOS RIESGOS 40
6. CONTROL DE CAMBIOS 41

PLAN DE TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR
CORPOCESAR

2025

1. OBJETIVO

Identificar los riesgos en materia de seguridad de la información y establecer el Plan de Tratamiento con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos de información de la **CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR - CORPOCESAR**.

2. ALCANCE

El presente plan aplica a empleados, contratistas, terceros, usuarios y visitantes de la **CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR – CORPOCESAR** que por alguna razón tengan cualquier tipo de interacción con los activos de información y que propicien la manifestación de uno de los riesgos aquí identificados.

3. DEFINICIONES

- **Activos de información:** Los activos de información en la compañía se clasifican de la siguiente manera: Software (incluye parametrizaciones, licencias, software genérico y a la medida, entre otros), hardware tecnológico, hardware no tecnológico (muebles, activos físicos, instalaciones, maestro de llaves, entre otros), información digital, documentación física, personas, intangibles (reputación, imagen, marca, good will, activos financieros, entre otros).
- **Adware:** Software que se apoya en anuncios (normalmente para financiarse) como parte del propio programa. En algunos casos se les considera malware. Común en las versiones gratuitas en las aplicaciones.
- **AES:** Acrónimo en inglés de Advanced Encryption Standard (AES); en español, estándar de cifrado avanzado. Es un algoritmo de cifrado de acceso público basado en clave compartida (Algoritmo criptográfico

simétrico), en el que, tanto el tamaño de bloque como el de la clave, son fijos.

- **Alta disponibilidad:** Característica de un sistema o servicio que permite reducir al mínimo el tiempo de indisponibilidad en caso de fallo o incidente; es decir, el tiempo en el que no estará accesible.

- **Amenaza:** Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad de los sistemas o aprovechando su existencia, puede derivar en un incidente de seguridad.
- **Análisis de vulnerabilidades:** Consiste en la búsqueda y documentación de fallos, carencias o debilidades físicas (inundaciones, incendios, controles de acceso…) y lógicas (configuraciones, actualizaciones…) en un sistema informático, que puedan ser empleados por terceros con fines ilícitos, suponiendo un riesgo para la organización y los propios sistemas. El análisis propone vías de mitigación a implementar para subsanar las deficiencias encontradas y evitar ataques a los sistemas informáticos.
- **Antispyware:** Herramienta de software diseñada para detectar y eliminar programas maliciosos del tipo spyware cuyo objetivo es espiar y obtener de forma sigilosa información personal presente en el dispositivo sin consentimiento del usuario.
- **Antivirus**: Software de protección para evitar que ejecutemos algún tipo de software malicioso en nuestro equipo que infecte al equipo.
- **Ataque activo:** Tipo de ataque detectable que se caracteriza por la modificación del contenido de la información, así como de los recursos o funcionamiento del sistema, pudiendo causar daños a dicho sistema. Este tipo de ataques pone en riesgo los principios de la seguridad de la información: confidencialidad; integridad y disponibilidad.
- **Auditoría de seguridad:** Es el estudio que comprende el análisis y gestión de sistemas llevado a cabo por profesionales en tecnologías de la información (TI) con el objetivo de identificar, enumerar y describir las diversas vulnerabilidades que pudieran presentarse en una revisión

exhaustiva de las estaciones de trabajo, redes de comunicaciones, servidores o aplicaciones.

- **Autenticación:** Acción mediante la cual demostramos a otra persona o sistema que somos quien realmente decimos que somos, mediante un documento, una contraseña, rasgo biológico etc.
- **Aviso Legal:** Un aviso legal es un documento, en una página web, donde se recogen las cuestiones legales que son exigidas por la normativa de aplicación.
- **Bomba Lógica:** Trozo de código insertado intencionalmente en un programa informático que permanece oculto hasta cumplirse una o más condiciones preprogramadas, momento en el que se ejecuta una acción maliciosa.
- **Borrado seguro:** Método de borrado de archivos que se caracteriza por sobrescribir los datos con el propósito de impedir su recuperación. Esto es aplicable tanto para información en formato físico como digital.
- **Brecha de seguridad:** Violaciones de la seguridad que ocasionan la destrucción, pérdida o alteración accidental o deliberada de datos personales cuando están siendo transmitidos, están almacenados o son objeto de otros tratamientos. Las brechas de seguridad también afectan a la comunicación o acceso no autorizados a dichos datos.
- **Bug:** Es un error o fallo en un programa de dispositivo o sistema de software que desencadena un resultado indeseado.
- **BYOD:** Acrónimo en inglés de Bring Your Own Device; en español, trae tu propio dispositivo. Es una política de uso de la tecnología en las empresas que se caracteriza por permitir a los empleados el uso de sus propios dispositivos personales (portátiles, smartphones, tabletas) para el trabajo, así como el acceso desde los mismos a las redes corporativas, aceptando su uso compartido, tanto para las tareas profesionales como para las personales de los empleados.
- **Cadena de custodia:** Protocolo para la extracción segura y protección de las evidencias digitales, mediante cifrado y sellado de tiempo, para su presentación junto a una demanda o denuncia ante los tribunales o para procesos de auditoría.
- **Certificado de autenticidad:** El Certificado de autenticidad (COA) es una etiqueta especial de seguridad que acompaña a un software con licencia legal para impedir falsificaciones.

- **Certificado digital:** Es un fichero informático generado por una entidad denominada Autoridad Certificadora (CA) que asocia unos datos de identidad a una persona física, organismo o empresa confirmando de esta manera su identidad digital en Internet.
- **Ciberataque:** Intento deliberado de un ciberdelincuente de obtener acceso a un sistema informático sin autorización sirviéndose de diferentes técnicas y vulnerabilidades para la realización de actividades con fines maliciosos, como el robo de información, extorsión del propietario o simplemente daños al sistema.
- **Ciberdelincuente:** Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante robo, filtrado de información, deterioro de software o hardware, fraude y extorsión. Casi siempre están orientados a la obtención de fines económicos.
- **Ciberejercicio:** Actividades orientadas a la evaluación del estado de preparación de un individuo, equipo, empresa, sector o país, frente a posibles crisis de origen cibernético que mejoren la respuesta, cooperación y coordinación del personal involucrado.
- **Cifrado:** Proceso de codificación de información para poder evitar que esta llegue a personas no autorizadas. Solo quien posea la clave podrá acceder al contenido.
- **Cloud computing:** El término cloud computing o computación en la nube se refiere a un paradigma que permite ofrecer servicios de computación a través de una red, que usualmente es Internet.
- **Códigos de conducta:** En el ámbito de las TIC, los códigos de conducta son aquellas recomendaciones o reglas que tienen por finalidad determinar las normas deontológicas aplicables en el ámbito de la tecnología y la informática con el objeto de proteger los derechos fundamentales de los usuarios.
- **Confidencialidad:** Es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.
- **Continuidad de negocio:** La continuidad representa una serie de procesos coherentes encaminados a asegurar que la Entidad no experimente interrupciones inaceptables en cualquiera de sus operaciones esenciales,

las cuales acarreen consecuencias financieras y operacionales e impacten negativamente a las partes interesadas.

- **Contraseña:** Forma de autentificación de un usuario, a través de una clave secreta, para controlar el acceso a algún recurso o herramienta. En caso de que no se proporcione la clave correcta no se permitirá el acceso a dichos elementos.
- **Control de acceso:** Sistema de verificación que permite el acceso a un determinado recurso si la persona o entidad tiene los derechos necesarios para solicitarlo. Este acceso puede ser a recursos de tipo físico (por ejemplo, a un edificio o un departamento) o lógicos (por ejemplo, a un sistema o una aplicación software específica).
- **Controles:** Medida que permite reducir o mitigar un riesgo.
- **Cookie:** Es un pequeño fichero que almacena información enviada por un sitio web y que se almacena en el equipo del usuario, de manera que el sitio web puede consultar la actividad previa del usuario.
- **Copia de seguridad:** Proceso mediante el cual se duplica la información existente de un soporte a otro, con el fin de poder recuperar los datos contenidos en caso de fallo del primer soporte de alojamiento.
- **Correo de suplantación:** Mensaje de correo electrónico, en teoría legítimo, que usa el nombre de una persona u organismo de confianza con el objetivo de obtener información confidencial o personal de la persona u organización a la que se ha enviado.
- **Correo spam:** Tipo de correo electrónico que se caracteriza por ser no solicitado por el receptor y que se envía en grandes cantidades con fines publicitarios o como complemento de actividades maliciosas como los ataques de phishing.
- **Cortafuegos**: Sistema de seguridad compuesto o bien de programas (software) o de dispositivos hardware situados en los puntos limítrofes de una red que tienen el objetivo de permitir y limitar, el flujo de tráfico entre los diferentes ámbitos que protege sobre la base de un conjunto de normas y otros criterios.
- **Cracker:** Ciberdelincuente que se caracteriza por acceder de forma no autorizada a sistemas informáticos con la finalidad de menoscabar la integridad, la disponibilidad y el acceso a la información disponible en un sitio web o en un dispositivo electrónico.

- **Credenciales:** Conjunto de datos, generalmente nombre de usuario y contraseña, pudiendo ser también un certificado de usuario, tarjeta inteligente o un token, entre otros. Estos datos posibilitan, por un lado, uno la identificación del individuo como usuario del sistema, y por otro, la autenticación o verificación de la identidad del individuo para obtener acceso a recursos localizados en equipos locales y en red.
- **Criptografía:** Es la técnica que consiste en cifrar un mensaje, conocido como texto en claro, convirtiéndolo en un mensaje cifrado o criptograma, que resulta ilegible para todo aquel que no conozca el sistema mediante el cual ha sido cifrado.
- **Criticidad:** Atributo que mide el riesgo que provoca un comportamiento erróneo o negligente respecto a las condiciones normales de funcionamiento al que está sometido un proceso, sistema o equipo. A mayor nivel de criticidad, mayor gravedad de los hechos ocurridos.
- **Cuarentena:** Acción que desarrollan los antivirus para aislar un archivo infectado del resto del sistema. De este modo, se evita que el archivo aislado provoque daños en el sistema hasta que sea posible desinfectarlo con todas las garantías por parte del antivirus. En ocasiones esto no es posible, por lo que se procedería continuando la cuarentena o eliminándolo directamente del sistema.
- **Datos personales:** Información relativa a una persona física viva que puede ser identificada o identificable a través de la recopilación de una serie de datos de carácter personal, que establezcan de forma directa o indirecta un perfil más o menos detallado de su identidad personal, familiar o profesional.
- **Denegación de servicio:** Ataque a un sistema, aplicación o dispositivo para dejarlo fuera de servicio debido a una saturación de peticiones.
- **Descifrado:** Acción de eliminar la codificación de una serie de datos que los convierte en ilegibles, mediante una clave conocida o por medio de técnicas de prueba error. El descifrado convierte el texto oculto por el cifrado en texto claro y legible.
- **Dirección IP:** Las direcciones IP (del acrónimo inglés IP para Internet Protocol) son un número único e irrepetible con el cual se identifica a todo sistema conectado a una red.
- **Dirección MAC:** Una dirección MAC, también conocida como dirección física, es un valor de 48 bits único e irrepetible que identifica todo

dispositivo conectado a una red. Cada dispositivo tiene su propia dirección MAC determinada que es única a nivel mundial ya que es escrita directamente, en forma binaria, en el hardware del interfaz de red en el momento de su fabricación.

- **Disponibilidad:** Propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.
- **Doble factor de autenticación:** Esquema de autenticación básica a la que se añade otro factor como puede ser un código enviado a un móvil, huella dactilar, sistema OTP, etc., más seguro que la autenticación simple.
- **Fichero ejecutable:** Archivo diseñado para inicializar un programa (instalación, ejecución, etc.) debido a que en su interior están las instrucciones precisas para poder ejecutar un software determinado.
- **Firma electrónica:** La firma electrónica (o digital) se define como el conjunto de datos electrónicos que acompañan o que están asociados a un documento electrónico. Esta firma se basa en la Ley 59/2003, de 19 de diciembre, donde se indica que la «firma electrónica» reconocida debe cumplir las siguientes propiedades o requisitos:

  -Identificar al firmante
  -Verificar la integridad del documento firmado
  -Garantizar el no repudio en el origen
  -Contar con la participación de un tercero de confianza
  -Estar basada en un certificado electrónico reconocido
  -Debe de ser generada con un dispositivo seguro de creación de firma

  Una firma electrónica de un documento se consigue calculando el valor «hash» del documento y adjuntándolo al final de este, para a continuación cifrarlo con la clave pública de la persona a la que enviaremos el documento.

- **Firmware:** Tipo de software que permite proporcionar un control a bajo nivel de un dispositivo o componente electrónico, siendo capaz de proveer un entorno de operación para las funciones más complejas del componente o comportándose como sistema operativo interno en armonía con otros dispositivos o componentes.

- **FTP:** Por FTP (del acrónimo inglés File Transfer Protocol) se hace referencia a un servicio de transferencia de ficheros a través de una red, así como a los servidores que permiten prestar este servicio.
- **Fuga de datos:** La fuga de datos o fuga de información es la pérdida de la confidencialidad de la información privada de una persona o empresa. Información que, a priori, no debería ser conocida más que por un grupo de personas, en el ámbito de una organización, área o actividad, y que termina siendo visible o accesible para otros.
- **Fuga de información:** Proceso por el cual se produce una fuga de la información almacenada en una red interna o en dispositivos físicos provocada por un atacante malintencionado y que es volcada o publicada en Internet para su libre consulta por parte de terceros sin autorización.
- **Gestión de incidentes:** Listado de procedimientos previamente documentados sobre los pasos a seguir en caso de detectar una amenaza de ciberseguridad en la empresa. La gestión de incidentes está orientada a mitigar en el menor tiempo posible un incidente de seguridad identificándolo y asignando el personal que dará respuesta al mismo dentro de unos parámetros predefinidos.
- **Gestor de contraseñas:** Programa o aplicación que se puede integrar en los principales navegadores y que permite generar contraseñas robustas y almacenarlas cifradas junto con los nombres de usuario para diferentes sitios web y aplicaciones, con la facilidad de tener que recordar solo la contraseña de acceso al gestor. Esto permite tener diferentes contraseñas por cada sitio para incrementar así la seguridad.
- **Hacker:** Persona con grandes conocimientos en el manejo de las tecnologías de la información que investiga un sistema informático para reportar fallos de seguridad y desarrollar técnicas que previenen accesos no autorizados.
- **Hacktivista:** Ciberdelincuente que haciendo uso de sus conocimientos en materia informática y herramientas digitales los usa para promover su ideología política. Entre las acciones que realizan destacan las modificaciones de webs (defacement), redirecciones, ataques de denegación de servicio (DoS), robo de información privilegiada o parodias de sitios web, entre otras. Estos actos son llevados a cabo por estas personas bajo la premisa de potenciar otros actos como la desobediencia civil con el fin último de lograr sus propósitos políticos.

- **Hash:** Operación criptográfica que genera identificadores alfanuméricos, únicos e irrepetibles a partir de los datos introducidos inicialmente en la función. Los hashes son una pieza clave para certificar la autenticidad de los datos, almacenar de forma segura contraseñas o firmar documentos electrónicos, entre otras acciones.
- **HTTP:** HTTP son las siglas en inglés de Protocolo de Transferencia de Hipertexto. Se trata del protocolo más utilizado para la navegación web. Se trata de un protocolo que sigue un esquema petición-respuesta. El navegador realiza peticiones de los recursos que necesita (la web, las imágenes, los videos...) y el servidor se los envía si dispone de ellos. A cada pieza de información transmitida se la identifica mediante un identificador llamado URL (del inglés Uniform Resource Locator).
- **Identificación:** Acción mediante la cual le decimos a otra persona o sistema quiénes somos.
- **Incidente de seguridad:** Cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa, por ejemplo: acceso o intento de acceso a los sistemas, uso, divulgación, modificación o destrucción no autorizada de información.
- **Información sensible:** Nombre que recibe la información privada y que debe protegerse del acceso de personas no autorizadas sin importar el soporte en el que se encuentre o transmita.
- **Informática forense:** La informática forense consiste en un proceso de investigación de los sistemas de información para detectar toda evidencia que pueda ser presentada como prueba fehaciente en un procedimiento judicial.
- **Infraestructura crítica:** Activos de carácter esencial e indispensable cuyo funcionamiento es imprescindible y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.
- **Ingeniería social:** Conjunto de técnicas que los delincuentes usan para engañar a los usuarios de sistemas/servicios TIC para que les faciliten datos que les aporten valor, ya sean credenciales, información sobre los sistemas, servicios instalados etc.
- **Integridad:** Es la propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma

accidental o intencionada, por errores de software o hardware o por condiciones medioambientales.

- **Intranet:** Red de comunicación interna de una organización que usa la tecnología del protocolo de Internet para compartir información, dispositivos o software.
- **Intrusión:** Acción provocada por un atacante o usuario malintencionado, que se aprovecha de una vulnerabilidad en el sistema para conseguir acceder a un área o dispositivo sin autorización con el objetivo de realizar actividades ilegítimas.
- **IoT:** Abreviación del término en inglés Internet of Things; en español, Internet de las cosas, es un concepto que se refiere a la interconexión digital de objetos cotidiano.
- **LAN:** Una LAN (del inglés Local Area Network) o Red de Área Local es una red informática de pequeña amplitud geográfica, que suele limitarse a espacios como una oficina, una vivienda o un edificio.
- **Login:** Mecanismo de acceso a un sistema o servicio a través de la identificación mediante credenciales del usuario.
- **Malware:** Es un tipo de software que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información. Palabra que nace de la unión de los términos en inglés de software malintencionado: malicious software.
- **Metadatos:** Son el conjunto de datos relacionados con un documento y que recogen información fundamentalmente descriptiva del mismo, así como información de administración y gestión.
- **Mitigación:** Reducción o atenuación de los daños potenciales sobre los sistemas, aplicaciones y dispositivos causados por un evento, como una vulnerabilidad o ataque.
- **No repudio:** El no repudio en el envío de información a través de las redes es capacidad de demostrar la identidad del emisor de esa información. El objetivo que se pretende es certificar que los datos, o la información, provienen realmente de la fuente que dice ser.
- **Parche de seguridad:** Es un conjunto de cambios que se aplican a un software para corregir errores de seguridad en programas o sistemas operativos. Generalmente los parches de seguridad son desarrollados por el fabricante del software tras la detección de una vulnerabilidad en el

software y pueden instalarse de forma automática o manual por parte del usuario.

- **Plan de contingencia:** Un Plan de Contingencia de las Tecnologías de la Información y las Comunicaciones (TIC) consiste en una estrategia planificada en fases, constituida por un conjunto de recursos de respaldo, una organización de emergencia y unos procedimientos de actuación, encaminados a conseguir una restauración ordenada, progresiva y ágil de los sistemas de información que soportan la información y los procesos de negocio considerados críticos en el Plan de Continuidad de Negocio de la compañía.
- **Plan de continuidad:** Es un conjunto formado por planes de actuación, planes de emergencia, planes financieros, planes de comunicación y planes de contingencias destinados a mitigar el impacto provocado por la concreción de determinados riesgos sobre la información y los procesos de negocio de una compañía.
- **Plugin:** También conocida como extensión, complemento o add-on es una aplicación que se relaciona con otra para agregarle una función nueva y generalmente muy específica. Las extensiones son un tipo de software que permite personalizar entre otros los navegadores web.
- **Política de seguridad:** Son las decisiones o medidas de seguridad que una empresa ha decidido tomar respecto a la seguridad de sus sistemas de información después de evaluar el valor de sus activos y los riegos a los que están expuestos.
- **Privacidad:** Derecho de las personas y usuarios a proteger sus datos en Internet, además de controlar el acceso a los mismos y decidir qué información es visible para el resto de los actores.
- **Protocolo:** Es un sistema de reglas que permiten que dos o más entidades se comuniquen entre ellas para transmitir información por medio de cualquier tipo de medio físico.
- **Proveedor de acceso:** Se denomina proveedor de acceso (a Internet) a todos los prestadores de servicios de la Sociedad de la Información que proporcionan a sus usuarios/clientes acceso a redes de telecomunicaciones, tanto fijas como móviles.
- **Puerta de enlace:** Dispositivo que actúa como intermediario permitiendo conectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación y compartir recursos entre varios dispositivos.

- **Puerta trasera:** Se denomina backdoor o puerta trasera a cualquier punto débil de un programa o sistema mediante el cual una persona no autorizada puede acceder a un sistema.
- **Puerto:** Es una interfaz o «puerta» a través de la cual se pueden enviar y recibir datos. Existen dos tipos de puertos: los físicos, que serían los conectores de un equipo que permiten la comunicación entre dispositivos, y que a su vez se dividen en varios tipos según el conector y su función; y los lógicos, generalmente implementados por software, que son aquellos que permiten la comunicación entre dos máquinas en una red, mediante áreas de memoria reservadas en un sistema.
- **Ransomware:** Malware cuya funcionalidad es «secuestrar» un dispositivo (en sus inicios) o la información que contiene de forma que, si la víctima no paga el rescate, no podrá acceder a ella.
- **Red privada virtual:** Una red privada virtual, también conocida por sus siglas VPN (Virtual Private Network) es una tecnología de red que permite una extensión segura de una red local (LAN) sobre una red pública o no controlada como Internet.
- **Redundancia:** Propiedad consistente en un determinado fichero o sistema para que en caso de caída de uno se pueda seguir proporcionando el servicio.
- **Repudio:** Denegación realizada por una de las partes intervinientes en una comunicación, por lo que no se puede garantizar la fuente de la información o de los datos.
- **Resiliencia:** Capacidad de una organización de resistir ante una situación adversa, como, por ejemplo, un incidente de ciberseguridad. La resiliencia empresarial debería ir acompañada de un plan de contingencia y continuidad para hacer frente a posibles situaciones de crisis en la empresa.
- **Respuesta de incidentes:** Se trata de un plan o guía con el que poder dar respuesta a posibles incidentes de ciberseguridad en la empresa.
- **Riesgo:** Es la posibilidad de que una amenaza o vulnerabilidad se convierta en un daño real para la empresa, que resulte en una pérdida o robo de información o en una detención de su actividad como consecuencia del daño ocasionado.
- **SaaS:** Son las siglas de Software as a Service, es decir la utilización de software como un servicio.

- **Sistema de Gestión de Seguridad de la Información:** Es el conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan dentro de una entidad.
- **Seguridad Lógica:** Establece e integra los mecanismos y procedimientos, que permiten monitorear el acceso a los activos de información lógicos, que incluyen los controles de administración de usuarios, definición de responsabilidades, perfiles de seguridad, control de acceso a los sistemas de información de acuerdo a las necesidades y funciones del usuario, análisis de incidentes de seguridad lógica y lecciones aprendidas de los mismos, monitoreo de aplicaciones críticas, análisis forense, documentación sobre sistemas, software malicioso, y además, participa en la definición de la arquitectura de las soluciones para garantizar el cumplimiento específico en los términos de seguridad de la información requeridos.
- **Seguridad Física:** Identifica los límites mínimos que se deben cumplir en cuanto a zonas seguras y perímetros de seguridad física, accesos físicos, control de ingreso y salida de activos, administración infraestructura locativa, entre otros, de forma que se puedan establecer controles que garanticen la seguridad de la información y del personal.
- **Servidor:** Puede entenderse como servidor tanto el software que realiza ciertas tareas en nombre de los usuarios, como el ordenador físico en el cual funciona ese software, una máquina cuyo propósito es proveer y gestionar datos de algún tipo de forma que estén disponibles para otras máquinas que se conecten a él.
- **SFTP:** Es la abreviatura en inglés de Secure File Transfer Protocol; en español, protocolo de transferencia segura de archivos.
- **SLA:** Un acuerdo de nivel de servicio o ANS (en inglés Service Level Agreement o SLA), es un contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio.
- **Software:** Conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en un dispositivo.
- **Spoofing:** Es una técnica de suplantación de identidad en la Red, llevada a cabo por un ciberdelincuente generalmente gracias a un proceso de investigación o con el uso de malware. Los ataques de seguridad en las

redes usando técnicas de spoofing ponen en riesgo la privacidad de los usuarios, así como la integridad de sus datos.

- **SSL:** Es un protocolo criptográfico seguro que proporciona comunicaciones seguras a través de una red (por ejemplo, Internet).
- **Suplantación de identidad:** Es la actividad maliciosa en la que un atacante se hace pasar por otra persona para cometer algún tipo de fraude, acoso (cyberbulling).
- **TCP/IP:** Por TCP/IP se conoce a una familia de protocolos sobre los cuales funciona Internet, permitiendo la comunicación entre todos los servidores conectados a dicha red.
- **Troyano:** Malware diseñado para tener múltiples utilidades, la más común es crear una puerta trasera en el equipo infectado, para poder descargar actualizaciones y nuevas funcionalidades.
- **Túnel:** Técnica que encapsula un protocolo de red sobre otro, lo que permite generar un túnel de comunicación para transportarlo a través de una red con seguridad.
- **URL:** Las siglas URL (Uniform Resource Locator) hacen referencia a la dirección que identifica un contenido colgado en Internet.
- **UTM:** Acrónimo en inglés de Unified Threat Management; en español, gestión unificada de amenazas, es el software de seguridad perimetral que permite la gestión centralizada de las amenazas que pueden afectar a una organización.
- **Virtualización:** La virtualización es un medio para crear una versión virtual de un dispositivo o recurso, como un servidor, o una red, en una máquina física, generalmente con el apoyo de un software que implementa una capa de abstracción para que la maquina física y la virtual puedan comunicarse y compartir recursos.
- **Virus:** Malware que tiene como característica principal que infecta ficheros ejecutables o sectores de arranque de dispositivos de almacenamiento.
- **VLAN:** Una red de área virtual o VLAN (acrónimo de Virtual Local Area Network) es una red lógica independiente dentro de una red física de forma que es posible crear diferentes una VLAN que este conectadas físicamente a diferentes segmentos de una red de área local o LAN.
- **Vulnerabilidad:** Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa

que se denomina exploit). Cuando se descubre el desarrollador del software o hardware lo solucionará publicando una actualización de seguridad del producto.

4. FACTORES DE RIESGOS

Un factor de riesgo es cualquier característica o circunstancia detectable que esté asociada con la probabilidad de estar especialmente manifestada en un tipo de daño. La **CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR – CORPOCESAR**, establece a continuación, los siguientes factores de riesgos de seguridad de la información:

- **Personas:** Empleados, contratistas, terceros, usuarios y visitantes de la organización que intervienen en procesos corporativos de forma directa o indirecta.
- **Procesos:** Conjunto interrelacionado entre sí de actividades y tareas necesarias para llevar a cabo el proceso.
- **Tecnología:** Mecanismos de apalancamiento como software y hardware que se utilizan para la gestión de procesos.
- **Infraestructura:** La interacción de componentes físicos, tecnológicos e intangibles que dan funcionalidad a la operación de servicios de tecnología a los procesos de una organización.
- **Factores Externos:** Elementos, condiciones o situaciones provenientes por agentes externos que generan afectación a procesos internos de una organización.

4. CATÁLOGO DE RIESGOS

A través de los estudios y análisis de riesgos previos en actividades relacionadas con la seguridad de la información, la **CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR – CORPOCESAR**, establece los siguientes riesgos que afectan los Activos de Información bajo criterios de impacto de Integridad, Disponibilidad y Confidencialidad:

No	RIESGOS	CRITERIO IMPACTADO		
		Integridad	Disponibilidad	Confidencialidad
1	Modificación no autorizada de la información	X		
2	Pérdida, destrucción o daño de la información	X	X	X
3	Indisponibilidad de la información		X	
4	Hurto por parte de propios o terceros		X	X
5	Daño o Sabotaje por parte de propios o terceros	X	X	X
6	Uso y divulgación no autorizada de información confidencial			X
7	Inconsistencias en la información	X		
8	Acceso no autorizado a la información			X

De acuerdo con la información suministrada por los colaboradores de la **CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR - CORPOCESAR** y las situaciones detectadas proactivamente en la identificación de Incidentes de Seguridad de la Información que se podrían presentar durante la operación y gestión de la entidad, estos se podrán clasificar en las siguientes categorías:

Categoría o Riesgo	Eventos o Causas	Plan de Acción / Controles
Uso indebido de Información	Uso indebido de la información crítica o sensitiva. Robo (Spoofing), divulgación (SPAM) o fuga no autorizada de información. Borrado, eliminación, modificación o alteración no autorizada de información o datos.	Firmar Compromisos de Confidencialidad. Instalar Software de seguridad en los equipos de cómputo. Establecer políticas para limitar las acciones en los equipos y software. Crear procedimientos para los procesos disciplinarios en materia de incumplimiento de normas que afecten la integridad de la empresa. Adelantar acciones legales para que determine las penalidades.
Acceso no autorizado	Esta categoría comprende todo tipo de ingreso y operación no autorizado a los sistemas. Son parte de esta categoría: • Acceso no autorizado a un activo o tecnologías de la información. • Intentos de acceso no autorizado a un sistema informático. • Modificación, instalación o eliminación no autorizada de software.	Establecer políticas de contraseña de accesos a los recursos tecnológicos. Crear dobles factores de autenticación para acceso a los Sistemas de Información. Crear protocolo de asignación y responsabilidades de los casos escalados por la entidad a sus profesionales. Limitar los privilegios de los perfiles de accesos.
Código malicioso	Esta categoría comprende la introducción de códigos maliciosos en la infraestructura tecnológica de	Activar herramientas de Seguridad Digital para la

Categoría o Riesgo	Eventos o Causas	Plan de Acción / Controles
	la compañía. Son parte de esta categoría: • Virus informáticos. • Troyanos. • Gusanos informáticos. • Spyware. • Adware.	protección de los activos de TI. Bloquear puertos de los equipos de cómputo donde se procesa la información de los casos que son atendidos para los profesionales de la entidad. Activar políticas en el Firewall.
Denegación del servicio	Esta categoría incluye los eventos que ocasionan la pérdida de un servicio en particular. Son parte de esta categoría: • Tiempos de respuesta muy altos sin razones aparentes en servicios críticos. • Servicios internos críticos inaccesibles, sin razón. • Servicios externos críticos inaccesibles, sin razón.	Garantizar la disponibilidad de los Sistemas de Información que se utilicen para la gestión misional y administrativa de la entidad. Monitorear la gestión de la capacidad para atender los posibles desmejoramientos de la infraestructura.
Mal uso de un activo o tecnologías de la información	Esta categoría agrupa los eventos que atentan contra los recursos tecnológicos por su mal uso. Hacen parte de esta categoría: • Abuso, mal uso y violación de los servicios y recursos informáticos internos o externos que requieren autenticación, sea red o cuentas de usuario. • Violación, comportamientos no tolerables en la Administración de servidores. • Intrusión física a centros de datos restringidos. • Uso de Sniffers, Keylogers, Password Crackers.	Crear consciencia en los colaboradores a través de la educación sobre los riesgos o incidentes en materia de Seguridad de la Información. Monitorear el estado de los activos. Establecer controles de accesos a la información digital como a la física. Adoptar políticas de buen uso de los recursos tecnológicos.

Categoría o Riesgo	Eventos o Causas	Plan de Acción / Controles
	• Detección no informada y explotación de una anomalía o vulnerabilidad técnica de software. • Activo comprometido.	Crear controles para evitar la vulnerabilidad de los activos físicos de TI.
Violación a políticas y normatividad	Violación a las normatividad de Derechos de Autor y Propiedad Intelectual. Tratamiento indebido de datos personales. Incumplimiento a leyes colombianas. Violación de las normas, políticas y procedimientos de Seguridad Informática. Fraude informático.	Capacitar en materia de tratamiento de datos personales. Socializar las políticas y procedimientos en materia de Seguridad de la Información. Crear procedimientos para los procesos disciplinarios en materia de incumplimiento de normas que afecten la integridad de la empresa. Adelantar acciones legales para que determine las penalidades.
Pérdida de información	Daño en los dispositivos de almacenamiento de la información. Traspapelar documentación. Derrame de líquidos o químicos sobre documentos. Pérdida de acceso a los equipos que contienen la información.	Crear un protocolo para definir las acciones que deben realizar los gestores al momento de producir un activo de información para los casos gestionados. Fomentar que, en la cultura organizacional, se mantenga el escritorio limpio. Dar cumplimiento al programa de copias de seguridad de la información.

A continuación, se detallan los riesgos asociados a Seguridad de la Información con sus planes de tratamiento para mitigar:

RIESGO 1: MODIFICACIÓN NO AUTORIZADA DE LA INFORMACIÓN

Dentro del análisis realizado al riesgo, se determinaron los siguientes activos afectados con sus vulnerabilidades, amenazas y el respectivo Plan de Tratamiento:

ACTIVO(S) AFECTADOS	VULNERABILIDADES	AMENAZAS
Bases de Datos	Falta de políticas que rigen el uso aceptable de los activos de información. Asignación errada de los derechos de acceso Ausencia de mecanismos de identificación y autentificación. Ausencia de mecanismos de monitoreo. Ausencia de procedimientos para el manejo de información tipificada. Ausencia de control de los activos que se encuentran fuera de las instalaciones. Mantenimiento insuficiente. Exposición de datos de respaldo. Vulnerabilidades conocidas. Gestión deficiente de credenciales de acceso Información legible y en texto plano	Incumplimiento en el mantenimiento. Ataque informático. Abuso de derechos. Falsificación de derechos. Sabotaje de la información. Suplantación de identidad. Escucha encubierta. Procesamiento ilegal de datos. Ausencia de asignación adecuada de responsabilidades en seguridad de la información. Corrupción de los datos. Exceso de confianza. Acceso no autorizado a los centros de cómputo.

PLAN DE TRATAMIENTO

Establecer directrices sobre el buen uso de la información en las bases de datos.

1. El acceso y diferentes acciones en las bases de datos debería contemplar configuraciones tipo RBAC, que controlen Roles y Privilegios para cada uno de los usuarios y administradores. (Servidores AAA)
2. Las bases de datos deberán generar y mantener una trazabilidad sobre todas las acciones realizadas sobre las mismas.
3. Deberá clasificarse la información que pueda existir dentro de las bases de datos, teniendo en cuenta su criticidad.
4. Detallar adecuadamente los procedimientos que se realizan en las bases de datos.
5. Realizar pruebas de vulnerabilidad o pentesting periódicas al (los) motores de bases de datos y aplicar los diferentes parches de seguridad, teniendo en cuenta las posibles consecuencias en la funcionalidad de los aplicativos.
6. Cifrar adecuadamente la información respaldada en soluciones NAS o en cintas, existen soluciones de almacenamiento con estas características.
7. Evitar emplear aplicaciones/códigos/componentes, que tengan vulnerabilidades conocidas en fuentes como (CVE, NVD) entre otras fuentes.
8. Definir una política de contraseñas seguras, que rijan todos los accesos a las bases de datos, si se considera necesario, se deberá implementar 2 o más factores de autenticación.
9. Definir planes de mantenimiento/depuración/actualización/afinamiento de las bases de datos de manera periódica.
10. Todas las bases de datos deberán ser tenidas en cuenta para la generación de las políticas y planes de respaldos de información.
11. Las bases de datos deberán estar debidamente cifradas y protegidas contra escritura no autorizada, empleando los algoritmos/herramientas necesarias.
12. Tener en cuenta el TOP 10 de vulnerabilidades de OWASP, para proteger las bases de datos.

ACTIVO(S) AFECTADOS	VULNERABILIDADES	AMENAZAS
Información en tránsito (correos electrónicos, Drive, página web, carpetas compartidas, dispositivos de almacenamiento)	Falta de políticas que rigen el uso aceptable de los activos de información. Ausencia de pruebas de envío o recepción de mensajes. Líneas de comunicación sin protección. Tráfico sensible sin protección. Ausencia de mecanismos de monitoreo. Ausencia de identificación y autenticación de emisor y receptor. Conexiones de red publicas sin protección. Gestión inadecuada de la red (Tolerancia a fallos en el enrutamiento).	Escucha encubierta. Espionaje remoto. Incumplimiento en el mantenimiento. Ataque informático. Suplantación de identidad.

PLAN DE TRATAMIENTO

Teniendo en cuenta las conexiones de red que se definan y que así lo requieran, se deberán implementar las siguientes medidas:

Para las conexiones entre entidades es importante tener en cuenta las siguientes recomendaciones:
1. Los canales de información que tengan como medio de transmisión internet, deberán emplear el uso de tecnologías como VPN, para garantizar la integridad y la confidencialidad de la información que está siendo transmitida.
2. Monitorear los canales y las conexiones, para verificar posibles pérdidas en el canal que puedan afectar los datos transmitidos.
3. Para las conexiones de enrolamiento (que utilizarán internet), un tipo de acceso distinto a la solución de servicios digitales básicos, se recomienda el uso de VPN tipo Client-to-Site, que permita que puedan unirse a la red donde está implementada la solución y poder realizar los enrolamientos o registros de nuevos usuarios.
4. Los accesos a las plataformas deberán tener diferentes factores de autenticación si así se consideran, teniendo una política de contraseñas previamente definida en los sistemas de información.
5. Aplicación de defensa en profundidad, es decir, un perímetro de acceso a los sistemas a través de sistemas como firewalls stateful y de capa de aplicación, Intrusion Prevention Systems y Proxy, definición de VLANs (Segmentación de Red), restricciones a través de ACL (Access Control List) cuando sea conveniente y implementación de honeypots.
6. Al compartir información a través de Drive, se deben establecer permisos solamente de descarga y a correos puntuales (Conocidos).

NOTA: Para cifrado a nivel de red, se recomendaría el uso del protocolo IPSEC con ESP (Encapsulating Security Protection), que busca el cifrado del canal o tunel VPN y de la información que viaje a través de este).

Debe emplearse para cifrado de VPN a nivel web, el protocolo TLS, SSL está obsoleto y tiene graves vulnerabilidades conocidas.

ACTIVO(S) AFECTADOS	VULNERABILIDADES	AMENAZAS
front End Usuarios, Front End Operador Front End Entidad	Asignación errada de los derechos de acceso. Ausencia de mecanismos de identificación y autentificación. Ausencia de mecanismos de monitoreo. Ausencia de manuales de uso. Mantenimiento insuficiente. Ausencia o insuficiencia de pruebas. Ausencia de terminación de sesión. Vulnerabilidades conocidas. Gestión deficiente de credenciales de acceso.	Incumplimiento en el mantenimiento. Ataque informático. Abuso de derechos. Falsificación de derechos. Sabotaje de la información. Suplantación de identidad

PLAN DE TRATAMIENTO

1. Ejecutar pruebas de pentesting en los diferentes front-ends definidos, con el objetivo de evitar los siguientes tipos de ataques (Considerando que serán páginas web:
   - *Web Parameter Tampering.
   - *XSS (Cross Site Scripting)
   - *SQL Injections
   - *Defacement
2. Implementar el protocolo TLS en su versión más estable en combinación con HTTPS y el certificado correspondiente (con la CA que mejor se considere).
3. Implementar mecanismos de autenticación de diferentes factores para reducir los riesgos de suplantación de identidad.
4. Implementar elementos de seguridad perimetral como firewalls y/o balanceadores para evitar ataques DDoS a las plataformas front-end.
5. Implementación Web Application Firewall.
6. Desarrollar el código de las aplicaciones web teniendo en cuenta las recomendaciones dadas en OWASP.

RIESGO 2: PÉRDIDA, DESTRUCCIÓN O DAÑO DE LA INFORMACIÓN

Dentro del análisis realizado al riesgo, se determinaron los siguientes activos afectados con sus vulnerabilidades, amenazas y el respectivo Plan de Tratamiento:

ACTIVO(S) AFECTADOS	VULNERABILIDADES	AMENAZAS
Información en tránsito (correos electrónicos, Drive, página web, carpetas compartidas, dispositivos de almacenamiento)	Procedimientos o políticas ausentes o definidas deficientemente. Servicio de energía eléctrica inestable. Inexistencia de protección contra inundaciones. Infraestructuras físicas inadecuadas o en mal estado, no resistente a desastres naturales. Protección física insuficiente o incorrecta. Insuficiente acondicionamiento de aire (altas temperaturas). Falta de capacidades y competencias. Falta de conciencia seguridad de la información. Medios de comunicación y equipos obsoletos o en mal estado. Exposición a humedad, contaminación, electromagnetismo. Inexistencia de contingencia. Programación o configuración insegura. Vulnerabilidad de las plataformas y protocolos de la Base de Datos. Ataques por intrusos o inyección SQL. Exposición de los Datos Backups. Missing Function Level Access. Ausencia de políticas y recursos de backup/respaldo. Falta o débil control de acceso físico y lógico.	Terremoto. Incendio. Robo de Información. Terrorismo. Falla en equipo de telecomunicaciones. Ataque informático.

PLAN DE TRATAMIENTO

1. Verificar canales de contingencia entre los operadores, para evitar perdida de solicitudes de transacciones o transmisión de información entre los mismos.
2. Elaborar un plan de continuidad de negocio, con roles, responsabilidades, recursos tecnológicos y personal necesario para asegurar la continuidad del servicio en los escenarios más críticos.
3. Disponer de dos datacenters con las siguientes condiciones mínimas:
   *Datacenter principal, que mínimo cumpla las condiciones/configuraciones TIER3.
   *Datacenter alterno (ubicado geográficamente en otro sitio) y que permita a su vez mitigar las amenazas de tipo natural y de terrorismo. que mínimo cumpla con configuraciones TIER2.
4. Todos los procedimientos de contingencia deberán estar debidamente documentados, para garantizar una respuesta adecuada ante posibles incidentes y a su vez la mayor disponibilidad posible de los servicios y de la información.
5. Mantener mantenimiento y monitoreo constante en los sistemas de refrigeración y de control de humedad.
6. Control de acceso físico a datacenters, con registros (preferiblemente bajo sistemas de información)
7. Capacitar al personal de seguridad física, en temas de seguridad de la información.
8. Implementar sistemas DLP (Data Leak Prevention), a nivel de redes, para evitar fugas de información sensible.

ACTIVO(S) AFECTADOS	VULNERABILIDADES	AMENAZAS
Información en reposo	Procedimientos o políticas ausentes o definidas deficientemente. Servicio de energía eléctrica inestable. Inexistencia de protección contra inundaciones. Infraestructuras físicas inadecuadas o en mal estado, no resistente a desastres naturales. Protección física insuficiente o incorrecta. Insuficiente acondicionamiento de aire (altas temperaturas). Falta de capacidades y competencias. Falta de conciencia seguridad de la información.	Terremoto. Incendio. Falla en el suministro de energía. Robo de Información. Terrorismo. Falla en equipos de respaldo. Falla en equipos de telecomunicaciones. Ataque informático.

	Medios de comunicación y equipos obsoletos o en mal estado. Exposición a humedad, contaminación, electromagnetismo. Inexistencia de contingencia. Programación o configuración insegura. Vulnerabilidad de las plataformas y protocolos de la Base de Datos. Ataques por intrusos o inyección SQL. Exposición de los Datos Backups. Missing Function Level Access. Ausencia de políticas y recursos de backup/respaldo. Falta o débil control de acceso físico y lógico.	Error humano.

PLAN DE TRATAMIENTO

1. Elaborar un plan de continuidad de negocio, con roles, responsabilidades, recursos tecnológicos y personal necesario para asegurar la continuidad del servicio en los escenarios más críticos.
2. Disponer de dos datacenters con las siguientes condiciones mínimas:

*Datacenter principal, que mínimo cumpla las condiciones/configuraciones por lo menos TIER3.

*Datacenter alterno (ubicado geográficamente en otro sitio) y que permita a su vez mitigar las amenazas de tipo natural y de terrorismo. que mínimo cumpla con configuraciones TIER2.

3. realizar mantenimientos periódicos a los sistemas eléctricos, con el diseño de su respectiva contingencia.
4. Mantener mantenimiento y monitoreo constante en los sistemas de refrigeración y de control de humedad.
5. Garantizar protecciones y sistemas contra fuego y explosiones.
6. Puertas y cámaras de seguridad en los centros de cómputo donde se encuentren los componentes que conforman la solución tecnológica.
7.Control de acceso físico a datacenters, con registros (preferiblemente bajo sistemas de información)
8. Capacitar al personal de seguridad física, en temas de seguridad de la información.
9. Establecer ambientes adecuados de desarrollo, pruebas y producción para los sistemas de información.
10. Definir políticas de respaldo de información.

RIESGO 3: INDISPONIBILIDAD DE LA INFORMACIÓN

Dentro del análisis realizado al riesgo, se determinaron los siguientes activos afectados con sus vulnerabilidades, amenazas y el respectivo Plan de Tratamiento:

ACTIVO(S) AFECTADOS	VULNERABILIDADES	AMENAZAS
Información, hardware, software, red	Using Components with Known Vulnerabilities. Missing Function Level Access. Security Misconfiguration. Insecure Direct Object References. Cross-Site Scriting (XSS). Injection. Vulnerabilidad de las plataformas y protocolos de la Base de Datos. Software desactualizado / programación insegura. Configuración o instalación incorrectas (puertos abiertos innecesarios, protocolos innecesarios). Firmware desactualizado. Hardware obsoleto. Exposición a electromagnetismo o temperaturas no toleradas por el HW. Servicio de energía eléctrica inestable. No segmentación de la red. Medios físicos de comunicación obsoletos o en mal estado. Falta de administración y monitoreo de vulnerabilidades. Personal Insuficiente / definición incorrecta de roles. Procedimientos o políticas ausentes o definidas deficientemente. Insuficiente acondicionamiento de aire (altas temperaturas).	Terremoto. Inundaciones. Derrumbe. Sabotaje. Terrorismo. Falla suministro de energía. Falla de telecomunicaciones. Falla en hardware. Falla en software. Ataque informático. Incumplimiento en Mantenimiento.

PLAN DE TRATAMIENTO

1. Definir una política de continuidad de negocio y los respectivos planes derivados para los servicios más críticos.
2. Deberán documentarse todos los procedimientos definidos para la recuperación de los servicios y para el desarrollo de las actividades más críticas para el servicio.
3. Si así lo define el análisis respectivo, deberá implementarse un datacenter alterno, para restaurar los servicios en caso de alguna amenaza de tipo natural (terremoto, inundaciones), un incendio, terrorismo entre otros que pueda afectar físicamente los servicios alojados en el sitio original.
4. Mantener mantenimiento y monitoreo constante en los sistemas de refrigeración y de control de humedad.
5. Entrenar adecuadamente al personal que administra o gestiona la solución, adicionalmente, implementar metodologías de transversalidad, para que la mayoría de los ingenieros conozcan varios temas y puedan suplir bajar de personal de manera temporal.
6. Realizar controles de cambios para verificar consecuencias en actualizaciones o configuraciones nuevas, empleando los respectivos ambientes de desarrollo, pruebas y producción.
7. Implementación de sistemas de seguridad perimetral (IPS, Firewall) y balanceadores, que eviten saturaciones y/o ataques de DDoS.
8. Garantizar pruebas periódicas en contingencia de energía eléctrica, con el uso de UPS, plantas alternas etc....
9. Garantizar la seguridad física donde se encuentren ubicados los sistemas de información, así mismo asegurar las conexiones eléctricas para evitar sabotajes como desconexión de los servidores o de los dispositivos de red.
10. Definir tiempos específicos de respuesta y recuperación para los incidentes (ANS), adicionales a los que planamente hablen sobre disponibilidad del servicio.
11. Implementación de aplicaciones de seguridad (Antimalware, antiphishing, antispyware, etc.)
12. Disponer de dos datacenters con las siguientes condiciones mínimas:

    *Datacenter principal, que mínimo cumpla las condiciones/configuraciones por lo menos TIER3.

    *Datacenter alterno (ubicado geográficamente en otro sitio) y que permita a su vez mitigar las amenazas de tipo natural y de terrorismo. que mínimo cumpla con configuraciones TIER2.

RIESGO 4: HURTO POR PARTE DE PROPIOS O TERCEROS

Dentro del análisis realizado al riesgo, se determinaron los siguientes activos afectados con sus vulnerabilidades, amenazas y el respectivo Plan de Tratamiento:

ACTIVO(S) AFECTADOS	VULNERABILIDADES	AMENAZAS
Hardware e Información	Ausencia de controles de seguridad física. Falta de políticas que rigen el uso aceptable de los activos de información. Procedimientos ausentes o definidas deficientemente. Falta de capacitación en el uso de los aplicativos. Falta de sensibilización en seguridad de la información. Empleado insatisfecho. Equipos de cómputo desatendidos.	Hurto de equipos. Hurto de documentos y/o medios. Escucha encubierta. Recuperación de medios reciclados o desechados. Sabotaje.

PLAN DE TRATAMIENTO

1. Implementación de soluciones DLP (Data Leak Prevention), tanto a nivel de información en reposo (almacenada), en tránsito o en uso.
2. En el caso de información física sensible, deberá disponerse de un área de archivo con la custodia correspondiente (Puertas, Cámaras de seguridad y Controles de Acceso Físico)
3. Garantizar la seguridad física donde se encuentren ubicados los sistemas de información, así mismo asegurar las conexiones eléctricas para evitar sabotajes como desconexión de los servidores o de los dispositivos de red.
4. Tener plenamente preparados planes de continuidad de negocio en caso de robo de algún componente específico, teniendo en cuenta los tiempos de respuesta definidos.
5. Políticas para disposición de información de medios físicos.
6. Sensibilización a todo el personal en temas de ingeniería social, para evitar posibles robos de información a través de estos métodos.
7. Implementación de herramientas como antivirus o IPS a nivel de Host, que protejan a los servidores y/o sistemas de información de amenazas como ransomware y otro tipo de malware.

RIESGO 5: DAÑO O SABOTAJE POR PARTE DE PROPIOS O TERCEROS

Dentro del análisis realizado al riesgo, se determinaron los siguientes activos afectados con sus vulnerabilidades, amenazas y el respectivo Plan de Tratamiento:

ACTIVO(S) AFECTADOS	VULNERABILIDADES	AMENAZAS
Hardware e Información	Falta o débil control de acceso físico y lógico. Procedimientos o políticas ausentes o definidas deficientemente. Ausencia de Cultura de Seguridad de la Información. Personal Insuficiente / Falta de capacidades y competencias. Uso de contraseñas débiles / credenciales de acceso robadas. Protocolos de red sin cifrar (transferencias de datos sensibles o críticos en texto plano). Puertos abiertos innecesarios / No segmentación de la red. Ausencia de filtros ACL entre segmentos de red. Falta de administración y monitoreo de vulnerabilidades. Software desactualizado / programación insegura, hardware obsoleto. Abusos de privilegios / elevación de privilegios no autorizada. Vulnerabilidad de las plataformas y exposición de los Datos Backups. Inyección Código. Unvalidated Redirects and Forwards. Using Components with Known Vulnerabilities. Cross-Site Request Forgery (CSRF). Missing Function Level Access. Sensitive Data Exposure / Security Misconfiguration. Insecure Direct Object References.	Espionaje remoto. Escucha encubierta. Hurto de equipo, medios o documentos. Hackeado de equipos y cuentas de correos electrónicos. Recuperación de medios reciclados o desechados. Interceptación de señales de interferencia comprometida. Abuso de derechos. FootPrinting, Packet Sniffeing (Ataques de reconocimiento) Recolectar información de la red, de los sistemas y de la organización). Ataques de acceso (Port Redirection). Ataques de acceso (Man in the middle) … Robo de información, secuestro de sesión, análisis de tráfico, DoS, Alterar la información. Ataques de acceso (Trust Exploitation). Acceso no autorizado a los centros de cómputo.

	Cross-Site Scriting (XSS). Broken Authentication and Session Management.	

PLAN DE TRATAMIENTO

1. Establecer políticas de uso de equipos al exterior de la organización.
2. Diseñar procedimiento de borrado a bajo nivel en el caso de devolver equipos a terceros, ya sea por daño o por aplicación de garantía.
3. Autenticación, Antisniffer, criptografía (SSH, SSL, IPSec), IDS a nivel de red y a nivel de host. 4. Logs
5. IDS a nivel de host
6. IPSec tunnel
7. Sistemas ubicados en el área externa de un firewall no deben ser autorizados por sistemas ubicados en la zona interna del firewall.

RIESGO 6: USO Y DIVULGACIÓN NO AUTORIZADA DE INFORMACIÓN CONFIDENCIAL

Dentro del análisis realizado al riesgo, se determinaron los siguientes activos afectados con sus vulnerabilidades, amenazas y el respectivo Plan de Tratamiento:

ACTIVO(S) AFECTADOS	VULNERABILIDADES	AMENAZAS
Información Física, Digital	Ausencia de controles de seguridad física. Falta de políticas que rigen el uso aceptable de los activos de información. Procedimientos ausentes o definidas deficientemente. Falta de capacitación en el uso de los aplicativos. Falta de sensibilización en seguridad de la información. Empleado insatisfecho. Equipos de cómputo desatendidos. Asignación errada de los derechos de acceso.	Error Humano. Sabotaje. Acceso no autorizado a instalaciones. Conflictos laborales. Tratamiento inadecuado de la información. Fuga de información.

PLAN DE TRATAMIENTO

1. Acuerdos de confidencialidad entre los operadores y el Ministerio de Tecnologías de la Información y las Comunicaciones, donde se garantice que la información manipulada por parte de los operadores tiene el único fin de proveer los servicios de carpeta ciudadana al ciudadano y absolutamente nada más, es decir, que esta información no podrá ser utilizada para fines publicitarios ni comerciales, adicionalmente deberán definirse multas y/o sanciones correspondientes si el proveedor del servicio incumple con la protección de los datos que tiene en su poder.
2. Verificación minuciosa sobre el personal contratado (Pasado judicial y pruebas de seguridad), dependiendo del tipo de privilegios que pueda tener en cuanto al acceso a los datos o la información.
3. Firma de acuerdos de confidencialidad para cada uno de los empleados que tengan o no acceso a la información y las instalaciones (incluyendo al personal de mantenimiento y aseo)
4. En los acuerdos o documentos definidos para la confidencialidad, deberá enfatizarse las consecuencias legales y disciplinarias correspondientes en caso de faltar a los compromisos que en este se enuncien.

5. Políticas que regulen el ingreso de dispositivos de almacenamiento extraíbles como discos duros, memorias USB etc., las cuales no deberían emplearse por parte del operador.
6. Limitar el uso de herramientas personales (correo electrónico, soluciones en la nube etc....) Ajenas a las asignadas por el operador, incluyendo los computadores, NO debe haber acceso a la administración de las plataformas desde máquinas particulares o personales.
7. Preparar al personal de técnicas como la ingeniería social para evitar fugas de información por este método.
8. La información sensible o privada que esté alojada en las distintas bases de datos y en las soluciones de respaldo deberán estar debidamente cifradas y protegidas por aplicaciones de seguridad, si existe un robo de la información, no necesariamente implica que la información este legible.
9. Implementación de soluciones DLP (Data Leak Prevention), tanto a nivel de información en reposo (almacenada), en tránsito o en uso.
10. Garantizar la seguridad física donde se encuentren ubicados los sistemas de información, así mismo asegurar las conexiones eléctricas para evitar sabotajes como desconexión de los servidores o de los dispositivos de red.

RIESGO 7: INCONSISTENCIAS EN LA INFORMACIÓN

Dentro del análisis realizado al riesgo, se determinaron los siguientes activos afectados con sus vulnerabilidades, amenazas y el respectivo Plan de Tratamiento:

ACTIVO(S) AFECTADOS	VULNERABILIDADES	AMENAZAS
Información, Sistemas de Enrolamiento	Falta o débil control de acceso físico y lógico. Procedimientos o políticas ausentes o definidas deficientemente. Insuficiente acondicionamiento de aire (altas temperaturas). Servicio de energía eléctrica inestable. Protocolos de red sin cifrar (transferencias de datos sensibles o críticos en texto plano). Falta de administración y monitoreo de vulnerabilidades. Medios físicos de comunicación y equipos obsoletos o en mal estado. Exposición a electromagnetismo y temperaturas no toleradas por el HW. Falta de mantenimiento. Programación insegura. Vulnerabilidad de la plataforma. Broken Authentication and Session Management. Using Components with Known Vulnerabilities. Cross-Site Request Forgery (CSRF).	Error Humano. Sabotaje. Conflictos Laborales.

PLAN DE TRATAMIENTO

1. En los posibles puntos de enrolamiento se recomienda verificar que el personal tenga los procedimientos de enrolamientos bien documentados y definidos.
2. Verificar antecedentes de empleados contratados para tal fin.
3. En caso de despido o de bajas de personal, efectuar las bajas en los sistemas de información a la mayor brevedad (esto implica el desarrollo de procedimientos de creación y gestión de usuarios según cada rol).
4. Verificar adecuadamente que los usuarios registren información verídica (incluyendo la biométrica), todo esto en el marco del procedimiento de enrolamiento que deberá generarse.
5. Capacitación adecuada en los diferentes procesos, para evitar el mal uso de las aplicaciones o la carga de información errada en las mismas.
6. Establecimiento de ambientes adecuados de desarrollo, pruebas y producción para los sistemas de información.

RIESGO 8: ACCESO NO AUTORIZADO A LA INFORMACIÓN

Dentro del análisis realizado al riesgo, se determinaron los siguientes activos afectados con sus vulnerabilidades, amenazas y el respectivo Plan de Tratamiento:

ACTIVO(S) AFECTADOS	VULNERABILIDADES	AMENAZAS
Información Física, Digital, Sistema de Información (Bases de Datos), Front-Ends	Inyección de código. Sensitive Data Exposure. Using Components with Known Vulnerabilities. Unvalidated Redirects and Forwards. Falta o débil control de acceso físico y lógico. Vulnerabilidad de las plataformas y protocolos de la Base de Datos. Abusos de privilegios / elevación de privilegios no autorizada. Vulnerabilidad de las plataformas y exposición de los Datos Backups. Ausencia de filtros ACL entre segmentos de red. No segmentación de la red, puertos abiertos innecesarios y protocolos innecesarios. Robo de credenciales de acceso / uso de contraseñas débiles. Procedimientos o políticas ausentes o definidas deficientemente. Ausencia de Cultura de Seguridad de la Información. Ausencia o deficiencia en roles de acceso a sistemas de información. Falta o débil control de acceso físico y lógico. Fallas en el reclutamiento y definición incorrecta de roles. Falta de conciencia seguridad de la información, capacidades y competencias.	Ingeniería Social. Escucha Encubierta. Espionaje Remoto. Ataque informático. Incumplimiento en Mantenimientos. Suplantación de Identidad.

PLAN DE TRATAMIENTO

1. Definición de esquemas AAA para la autenticación, autorización y registro de las transacciones realizadas en los sistemas de información.
2. Definir las políticas de uso aceptable de los recursos tecnológicos asignados, entre ellos las cuentas de usuario de las plataformas de administración.
3. Campañas de sensibilización a la ciudadanía, para que hagan un uso adecuado de las credenciales otorgadas a la solución de servicios digitales básicos.
4. Generación de campañas para la ciudadanía, reforzando los temas principalmente de ingeniería social y phishing, para el robo de datos de acceso.
5. Definir factores adicionales de autenticación que incrementen los niveles de seguridad, teniendo en cuenta los principios:
*Algo que el usuario sabe. (Ej. Contraseña, PIN)
*Algo que el usuario posee. (Ej. Token, Apps, Tarjetas)
*Algo que el usuario es. (Ej. Biometría)
*Algo que el usuario sabe hacer. (Ej. Firma)
6. Deberán ejecutarse pruebas de pentesting en los diferentes front-ends y sistemas de información, con el objetivo de evitar los siguientes tipos de ataques (Considerando que serán páginas web:
*Web Parameter Tampering.
*XSS (Cross Site Scripting).
*SQL Injections.
7. Garantizar la seguridad física donde se encuentren ubicados los sistemas de información, así mismo asegurar las conexiones eléctricas para evitar sabotajes como desconexión de los servidores o de los dispositivos de red.
8. En el caso de información física sensible, deberá disponerse de un área de archivo con la custodia correspondiente (Puertas, Cámaras de seguridad y Controles de Acceso Físico)
9. Implementación de herramientas como antivirus o IPS a nivel de Host, que protejan a los servidores y/o sistemas de información de amenazas de malware que incluyen backdoors, para acceder a los sistemas sin autorización.

5. REVISIÓN DE LOS RIESGOS

Los riesgos aquí definidos se deberán revisar de manera periódica con el fin de establecer planes de acción dada la materialización de estos o la identificación de

nuevos riesgos de seguridad de la información a partir de los nuevos servicios de tecnologías, esto con el fin de asegurar su vigencia y aplicabilidad dentro de la **CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR – CORPOCESAR.**

6. CONTROL DE CAMBIOS

RESPONSABLE	VERSIÓN	FECHA	CAMBIOS
MAURICIO GARCÉS ORDÓÑEZ	1.0	01/12/2022	Creación del documento.
MAURICIO GARCÉS ORDÓÑEZ	2.0	25/01/2024	Ajuste de forma del documento y alineación de acciones basadas en nuevas tecnologías.
MAURICIO GARCÉS ORDÓÑEZ	3.0	22/01/2025	Se agregan las categorías y los eventos para identificar los Incidentes en materia de Seguridad de la Información durante la gestión misional y administrativa de la entidad.

ELABORÓ	REVISÓ	APROBÓ
MAURICIO GARCÉS ORDÓÑEZ Profesional Especializado	MARÍA CRISTINA ROBAYO ABELLO Subdirectora General Área de Planeación	MARÍA CRISTINA ROBAYO ABELLO Subdirectora General Área de Planeación