AUTORIDAD DE INTERMEDIACIÓN ELECTRÓNICA	Fecha: 20/06/2020
	Versión: 2

POLÍTICA DE SEGURIDAD

info@saeta.pe • www.saeta.pe
General Vidal 921 - Breña • (511) 633 - 7824 / 333 - 2212

Elaborado	Fecha de Elaboración	Versión
José Junior Damian Tirado (Jefe de Aplicaciones y Desarrollo)	01/03/2017	1

Revisado	Fecha de Revisión	Versión
Wilfredo Dávila (Gerente General)	07/03/2017	1
Angela Donayre (Jefe de Infraestructura)	24/04/2018	2
José Junior Damian Tirado (Jefe de Aplicaciones y Desarrollo)	10/05/2019	2
José Junior Damian Tirado (Gerente General / Arquitecto de Soluciones)	08/06/2020	2

Cambios	Fecha de Revisión	Versión	Cambios Realizados
José Junior Damian Tirado	02/03/2017	2	Realización del Documento
José Junior Damian Tirado.	18/04/2018	2	Se agregaron políticas de acceso y contingencia adicionales.
José Junior Damian Tirado	07/05/2019	2	Se agregaron políticas de disponibilidad de nodos y mejora en los servicios de contingencia.
José Junior Damian Tirado	01/06/2020	2	Se agrego el apartado de la planificación del sistema y también de la seguridad Física del mismo.

INTRODUCCIÓN

Soluciones Aplicadas en Tecnología Avanzada SAC (cuyas siglas son SAETA), es una organización con sede en Perú orientada a la cobertura de necesidades de protección documentaria y de marca al servicio de las organizaciones privadas y públicas, mediante la elaboración y comercialización de elementos con tecnología de punta que brindan altos niveles de seguridad contra su duplicación y su falsificación. Actúa también en el campo de la identificación, validación y trazabilidad de personas y documentos digitales. En este sentido, SAETA brinda el servicio de intermediación electrónica conforme a la regulación peruana establecida por la Autoridad Administrativa Competente, el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI).

SAETA, brinda el servicio de intermediación electrónica con la finalidad de garantizar al usuario la legalidad en el manejo de su información, así como también en el manejo de sus documentos digitales. Actualmente el servicio de intermediación electrónica involucra los siguientes servicios:

- Firma Digital a documentos digitales.
- Sello de Tiempo.
- Plataforma de Trazabilidad de Documentos.
- Envío de Correos Electrónicos.
- Transferencia de Archivos digitales de forma segura.
- Custodia de Archivos Digitales.

Para obtener la acreditación de este tipo de modalidad, como es intermediación electrónica es necesario realizar una política de seguridad que vaya acorde a lo estipulado en el Anexo 3. Para efectos de la reglamentación que solicita INDECOPI, existe un comité de Seguridad de la Información que vela por los puntos tratados a continuación. Así como también existe un oficial de seguridad encargado de velar por los controles de seguridad puestos en la plataforma.

Entre las guías de buenas prácticas utilizadas son las siguientes:

- ITIL, ciclo de vida de un servicio.
- ISO 27001 para el uso de herramientas de seguridad que garanticen la validez en seguridad de la información.
- NTP-ISO/IEC 17799:2007

1. OBJETIVOS

- Definir las actividades de planeamiento, preparación y ejecución de tareas destinadas a proteger la Información contra los daños y perjuicios producidos por corte de servicios, fenómenos naturales o humanos.
- Garantizar la continuidad de las operaciones de los principales elementos que componen los Sistemas de Información.
- Establecer actividades que permitan evaluar los resultados y retroalimentación de la política de seguridad de la información.
- Contar con una estrategia planificada compuesta por un conjunto de procedimientos que garanticen la disponibilidad de una solución alterna que permita restituir rápidamente los sistemas de información de la Entidad ante la eventual presencia de siniestros que los paralicen parcial o totalmente.
- Establecer un esquema de seguridad con perfecta claridad y transparencia bajo la responsabilidad de SAETA S.A.C. en la administración del riesgo.

2. ALCANCE

El alcance de este plan se sitúa en los diferentes daños o perjuicios que afectan interna o externamente con los activos de la información más importantes, debido a esto se define el alcance que tendrá este plan:

- El plan solo es aplicable a los procesos que tenga gobierno nuestra organización, cualquier caída fuera de nuestra plataforma, no forma parte de las características del producto.
- El plan atiende una cantidad de procesos que hayan sufrido daño o perjuicio en la información que manejan, pero no garantiza la información externa que no haya sido genera por nuestra organización.

El alcance del plan de contingencia incluye los elementos básicos y esenciales, componentes y recursos informáticos que conforman los sistemas de información que maneja el cliente, que se relacionan a continuación:

- Datos: En general se consideran datos todos aquellos elementos por medio de los cuales es posible la generación de información. Tales elementos pueden ser estructurados (Bases de Datos) o no estructurados (correos electrónicos) y se presentan en forma de imágenes (TIF) u otro archivo o colecciones de bits.
- Aplicaciones: Son los archivos y programas con sus correspondientes manuales de usuario y/o técnicos desarrollados o adquiridos por la entidad.
- Tecnología: Incluye los recursos en la nube como nodos o servidores, servicios de base de datos en general denominados software para el procesamiento de información.

Independientemente de la cobertura y medidas de seguridad que se hallen implantadas, puede ocurrir un desastre, por tanto es necesario que el Plan de Contingencia cuente también con un Plan de Recuperación en caso de desastres, el cual tendrá como objetivo restaurar los servicios de los sistemas de información de forma rápida, eficiente y con el menor costo y pérdidas de tiempo posible.

Como mínimo, los diferentes planes de contingencia que hacen parte del presente documento han sido construidos considerando que el COPNIA tenga soluciones de continuidad en su operación diaria aunque ello implique una posible reducción en su capacidad de proceso.

3. DEFINICIONES:

- **Acceso:** Es la lectura o grabación de datos que han sido almacenados en un sistema de computación. Cuando se consulta una Base de Datos, los datos son primero accedidos y suministrados a la computadora y luego transmitidos a la pantalla del equipo.
- **Amenaza:** Cualquier evento que pueda interferir con el funcionamiento de un computador o causar la difusión no autorizada de información confiada a un computador. Ejemplo: Fallas del suministro eléctrico, virus, saboteos o descuido del usuario.
- **Ataque:** Término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático o el intento de obtener de modo no autorizado la información confiada a un computador.
- **Base de Datos:** Es un conjunto de datos organizados, entre los cuales existe una correlación y que además están almacenados con criterios independientes de los programas que los utilizan. Entre sus principales características se encuentran brindar seguridad e integridad a los datos, proveer lenguajes de consulta, de captura y edición de los datos en forma interactiva, proveer independencia de los datos.
- **Datos:** Los datos son hechos y/o valores que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos en el presente documento. En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y Bases de Datos, textos (colección de palabras), hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), videos (secuencia de tramas), etc.
- **Golpe (Breach):** Es la violación exitosa de las medidas de seguridad, como el robo de información, la eliminación de archivos de datos valiosos, el robo de equipos, PC, etc.
- **Incidente:** Cuando se produce un ataque o se materializa una amenaza se tiene un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de eliminación de un archivo protegido.
- **Integridad:** Los valores consignados en los datos se han de mantener de tal manera que representen la realidad y su modificación debe ser registrada en bitácoras del sistema que permitan la auditoría de los acontecimientos. Las técnicas de integridad sirven para prevenir el ingreso de valores errados en los datos sea esta situación provocada por el software de la Base de Datos, por fallas de los programas, del sistema, el hardware o, simplemente, por errores humanos.
- **Privacidad:** Se define como el derecho que tiene el COPNIA para determinar, a quién, cuándo y qué información de su propiedad podrá ser difundida o transmitida a terceros.
- **Seguridad:** Se refiere a las medidas que toma el COPNIA con el objeto de preservar la integridad de sus datos o información procurando que no sean modificados, destruidos o divulgados ya sea en forma accidental, no autorizada o intencional. En el caso de los datos e información contenidos en los sistemas de información del COPNIA, la privacidad y seguridad guardan estrecha relación entre sí, aunque la diferencia entre ellas radica en que la primera se refiere a la distribución autorizada de información y la segunda al acceso no autorizado.

- **Sistemas de Información:** Es el término empleado en el ambiente del procesamiento de datos para referirse al almacenamiento de los datos de una organización y ponerlos a disposición de su personal. Pueden ser registros simples como archivos de Word y Excel, o pueden ser complejos como una aplicación de software con base de datos.
- **Cortafuegos (Firewall):** Es un sistema diseñado para bloquear el acceso no autorizado de comunicaciones. Se trata de un dispositivo configurado para permitir, limitar, cifrar y descifrar el tráfico de mensajes entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios. Los cortafuegos se utilizan para evitar que los usuarios.
- **Plan de Contingencia:** Son procedimientos que definen cómo una entidad continuará o recuperará sus funciones críticas en caso de una interrupción no planeada.
- **Riesgo:** Es la vulnerabilidad de un Activo o bien, ante un posible o potencial perjuicio o daño.

4. EVALUACION DE RIESGOS Y ESTRATEGIAS:

Para la clasificación de los activos de las Tecnologías de Información de SOLUCIONES APLICADAS EN TECNOLOGÍA AVANZADA se han considerado:

- Grado de negatividad: Un evento se define con grado de negatividad (Leve, moderada, grave y muy severo).
- Frecuencia del Evento: Puede ser (Nunca, aleatoria, Periódico y continuo)
- Impacto: El impacto de un evento puede ser (Leve, moderado, grave y muy severo).

Para el caso del análisis de riesgo se ha realizado un esquema que aplica a los diferentes riesgos existentes, así como su factor y la posible prevención y mitigación del mismo.

Tipo de riesgo	Factor de riesgo	Prevención y mitigación
Acceso no autorizado: usuario interno o externo malintencionado.	Medio	Cambio de contraseñas, mínimo cada 1 mes (30 días), adicionalmente cada usuario tiene roles que van acorde con la Política de Seguridad. Capacitaciones orientadas a ética y Seguridad de la Información.
Fallas en los Nodos: daño en los archivos, pérdida de los mismos	Medio	Replicación de los Nodos en Nube, en 2 diferentes zonas de disponibilidad, en dos regiones uno en Virginia y el otro en Sao Paulo. Además de un proceso de resguardo diario que pasa a un lugar seguro custodiado por HSM de acceso.
Equivocaciones: daño de los archivos.	Bajo	Capacitación de la herramienta, así como copias de respaldo, lo que garantiza que a pesar del error se manejan herramientas necesarias para restaurar el sistema. Replicación de los Nodos en Nube, en 2 diferentes zonas de disponibilidad, en dos regiones uno en Virginia y el otro en Sao Paulo.
Acción de Virus en los nodos: daño a los nodos e información	Medio	Actualizaciones de parches de seguridad, constantes en los nodos, así como capa de firewalls e IDS actualizados y finalmente copias de respaldo. Las actualizaciones son verificadas previamente, antes de ser desplegadas.
Desastres Naturales: destrucción de nodos y archivos	Bajo	Tenemos replicados en 2 zonas de disponibilidad en diferentes regiones (Sao Paulo y Virginia).
Robo de datos: difusión de datos sin el cubrimiento de su costo y privacidad	Medio	Tenemos mecanismos de autenticación seguros, como cambio de contraseñas cada mes, uso de medidas de seguridad como certificados SSL, para el cifrado de comunicaciones entre los nodos. Copias de respaldo y reguardo de información cifrados.
Fraude: Modificación y/o desvío de la información y fondos de la institución y del cliente	Bajo	El sistema de documentos electrónicos (PLUSSIGNER) se encuentra en una sub-net aislada que solo está autorizada para estos fines, adicionalmente se realizan auditoría,

		control y registros en las diferentes transacciones. Capacitaciones y medidas de seguridad de información interna manejada por el cliente. Control de recepción de archivos o información a través de la generación de hash para futuras verificaciones y auditorías antes de ingresar a nuestra plataforma. Control de envío de paquetes a través de TTL (Tiempo de vida del paquete), si no se respeta este tiempo de vida el paquete no es aceptado por los nodos siguientes. Los tiempos de vida se estandarizan en base a la carga que tendrá la aplicación.
Imposibilidad de acceso a los recursos informáticos, sean estos por cambios involuntarios o intencionales, tales como cambios de claves de acceso, eliminación o borrado físico/lógico de información clave, proceso de información no deseado.	Medio	Tenemos mecanismos de autenticación seguros, como cambio de contraseñas cada mes. La complejidad de las contraseñas es de 12 caracteres como mínimo, que incluye Mayúsculas, Minúsculas, caracteres especiales y números. Bloqueo de cuenta en 3 intentos de 5 min. Si vuelve a ocurrir será notificado al cliente como a la empresa. Replicación de archivos y base de datos en 2 zonas de disponibilidad conectadas, que en el borrado y/o modificación del nodo de replicación (caja negra) sea con autorización del cliente y su participación en conjunto con el representante de la empresa.
Ruptura de las claves de acceso a los sistema computacionales	Bajo	Uso de protocolos auditados por la comunidad.
Ataques de Denegación de Servicio.	Medio	El servicio WAF detecta este tipo de ataques y notifica a través del servicio CloudWatch se comunica la denegación de las peticiones solicitados por nodos fraudulentos.

El área de Aplicaciones y desarrollo, está conformada por profesionales con conocimientos de sistemas de información quienes prestan asesoría técnica sobre el presente procedimiento y supervisan su correcto desarrollo en caso de requiera. Adicionalmente se deben contar con contratos de mantenimiento vigentes para las diferentes plataformas informáticas, con profesionales especializados que prestarán soporte técnico de acuerdo a los niveles de servicio exigidos.

Debido a que la tecnología es muy volátil, es posible que algunos sistemas de información dejen de operar por encontrase obsoletos o al ser reemplazados por unos más modernos. De acuerdo con lo anterior, los programas que dejen de operar por ser reemplazados por otros o por ser obsoletos, deben permanecer instalados durante los tres (3) meses siguientes en forma simultánea para emplearlos en caso de contingencia y una vez concluido este período el funcionario responsable debe realizar una copia de seguridad completa de la información BD y enviarla al área de sistemas para su verificación y custodia en diferentes oficinas de la entidad.

5. POLÍTICA DE CONTROL DE ACCESO:

OBJETIVO

- Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.
- Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.
- Controlar la seguridad en la conexión entre la red de la Plataforma y otras redes públicas o privadas.
- Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.
- Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y accesos.
- Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.

ALCANCE

- La Política definida en este documento se aplica a todas las formas de acceso de aquellos a quienes se les haya otorgado permisos sobre las aplicaciones, bases de datos o servicios de información que utilice la plataforma, cualquiera sea la función que desempeñe.
- Asimismo se aplica al personal técnico que define, instala, administra y mantiene los permisos de acceso y las conexiones de red, y a los que administran su seguridad.

POLITICA DE CONTROL DE ACCESOS

Para los accesos y su control del mismo se ha dispuesto las siguientes normas dentro de la política de seguridad

- Debe establecerse reglas sobre la premisa “Todo debe estar prohibido a menos que se permita expresamente” y no sobre la premisa inversa de “Todo está permitido a menos que se prohíba expresamente”.
- Todos los usuarios con acceso a un sistema de información o a una red informática, dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña.
- Ningún usuario recibirá un identificador de acceso a la Red de Comunicaciones, Recursos Informáticos o Aplicaciones hasta que no acepte formalmente la Política de Seguridad vigente y tenga una autorización de su superior.
- Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones, conforme a los criterios establecidos por el responsable de la información. Para este fin existe un panel de administración que brinda estos accesos.
- La longitud mínima de las contraseñas será igual o superior a ocho caracteres, y estarán constituidas por combinación de caracteres alfabéticos, numéricos y especiales.
- El cambio obligatorio de contraseñas será cada 45 días calendario, después de su inicio de sesión, continuando sucesivamente.
- Se realizará un control con los cambios en los permisos de usuario que son iniciados automáticamente por el sistema de información y aquellos que son iniciados por el administrador.

- Los identificadores para usuarios temporales se configurarán para un corto período de tiempo. Una vez expirado dicho período, se desactivarán de los sistemas.
- Bloqueo de cuenta en 3 intentos de 5 min. Si vuelve a ocurrir será notificado al cliente como a la empresa.
- Todas las plataformas cuentan con un código Captcha que se encarga de evitar cualquier intromisión de un robot o algún actor intruso.
- Se mantendrá un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no deben ser otorgados hasta que se haya completado el proceso formal de autorización.
- Se debe cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización, se desvincularon de la plataforma o sufrieron la pérdida/robo de sus credenciales de acceso.
- Se debe entregar a los usuarios un detalle escrito de sus derechos de acceso.

6. SEGURIDAD DEL PERSONAL:

OBJETIVO:

- Reducir los riesgos de error humano, comisión de ilícitos, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.
- Explicitar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado.
- Garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para respaldar la Política de Seguridad de la organización en el transcurso de sus tareas normales.
- Establecer Compromisos de Confidencialidad con todo el personal y usuarios externos de las instalaciones de procesamiento de información.
- Establecer las herramientas y mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia.

ALCANCE:

Esta Política se aplica a todo el personal de la organización, cualquiera sea su situación de revista, y al personal externo que efectúe tareas dentro del ámbito de la organización.

POLÍTICA DE SEGURIDAD DEL PERSONAL:

- Las funciones y responsabilidades en materia de seguridad serán incorporadas en la descripción de las responsabilidades de los puestos de trabajo.
- Se llevarán a cabo controles de verificación del personal en el momento en que se solicita el puesto.
- Como parte de sus términos y condiciones iniciales de empleo, los empleados, cualquiera sea su situación de revista, firmarán un Compromiso de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información del Organismo. La copia firmada del Compromiso deberá ser retenida en forma segura por el Área de Recursos Humanos u otra competente.
- Los términos y condiciones de empleo establecerán la responsabilidad del empleado en materia de seguridad de la información.
- Todos los empleados de la plataforma y, cuando sea pertinente, los usuarios externos y los terceros que desempeñen funciones en el organismo, recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos de la organización. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general, como por ejemplo su estación de trabajo.
- Los incidentes relativos a la seguridad serán comunicados a través de canales gerenciales apropiados tan pronto como sea posible.
- Todos los empleados y contratistas deben conocer el procedimiento de comunicación de incidentes de seguridad, y deben informar de los mismos tan pronto hayan tomado conocimiento de su ocurrencia.

- Los usuarios de servicios de información, al momento de tomar conocimiento directo o indirectamente acerca de una debilidad de seguridad, son responsables de registrar y comunicar las mismas al Responsable de Seguridad Informática.
- Se establecerán procedimientos para la comunicación de anomalías de software, los cuales deberán contemplar:
  - Registrar los síntomas del problema y los mensajes que aparecen en pantalla.
  - Establecer las medidas de aplicación inmediata ante la presencia de una anomalía.
  - Alertar inmediatamente al Responsable de Seguridad Informática o del Activo de que se trate.

7. SEGURIDAD FÍSICA

Este tipo de herramientas o plataformas en la NUBE no tienen seguridad física del componente, como parte de la seguridad lógica cada nodo en AWS (SaaS, software as a Service) maneja una llave ".ppk" con la cual puedes acceder a las instancias creadas. (TRANSFERIR RESPONSABILIDAD AL PROVEEDOR).

Nuestro proveedor de servicio de nube cuenta con la ISO/IEC 27001:2013 es una norma o estándar de administración de la seguridad que establece prácticas recomendadas en materia de administración de la seguridad, así como controles de seguridad exhaustivos, conforme a las prácticas recomendadas de la norma ISO/IEC 27002. La base de esta certificación es el desarrollo y la implementación de un estricto programa de seguridad, que incluye el desarrollo e implementación de un sistema de administración de seguridad de la información (ISMS) que define cómo AWS administra la seguridad constantemente de forma exhaustiva e integral. Este estándar de seguridad internacional, ampliamente conocido, especifica que AWS realiza lo siguiente:

- Evaluamos sistemáticamente los riesgos de seguridad física y virtual de la información, teniendo en cuenta el impacto de las amenazas y vulnerabilidades.
- Diseñamos e implementamos un conjunto completo de controles de seguridad físico y virtual de la información y otros mecanismos de gestión de riesgos para afrontar los riesgos de seguridad a los que están expuestos el cliente y la arquitectura.
- Disponemos de un proceso general de administración para garantizar que los controles de seguridad físico y virtual de la información satisfagan nuestras necesidades de manera continua.

AWS cuenta con la certificación de conformidad con las normas ISO/IEC 27001:2013, 27017:2015 y 27018:2014. Estas certificaciones las llevan a cabo auditores externos independientes. El cumplimiento de estos estándares y códigos de conducta reconocidos a escala internacional demuestra nuestro compromiso con la seguridad de la información en todas las esferas de la organización y que el programa de seguridad de AWS está en consonancia con las principales prácticas recomendadas del sector. Esto incluye protección de acceso físico, protección contra desastres naturales, detección y protección contra incendios, contingencia en cortes de energías y comunicaciones, colapso de la estructura, aniego, protección contra robo, ruptura, recuperación en caso de desastres, conforme a los resultados del análisis de riesgos. Se deben implementar controles que impidan el retiro no autorizado de equipos, información, medios de almacenamiento, software relativo a los servicios críticos.

Así como maneja mecanismos de compliance tales como:

- Privacidad de la información: https://aws.amazon.com/es/compliance/data-privacy/
- Programas de Conformidad de AWS: https://aws.amazon.com/es/compliance/programs/

Algunas de sus medidas de seguridad física se especifican en el siguiente apartado:

https://d0.awsstatic.com/whitepapers/Security/ES_Whitepapers/AWS_Security_Whitepaper.pdf

Nosotros también contamos con sistemas de seguridad física en las cuales se conectan nuestras instalaciones, para ello se cuenta con las siguientes medidas de seguridad:

- Contamos con cámaras de vigilancia, tanto en el ingreso y en el proceso donde se encuentran los equipos de cómputo, los cuales permiten identificar personas no autorizadas.
- Contamos con un sistema de identificación biométrica para el acceso a nuestro lugar de trabajo donde se operan con las credenciales

8. SEGURIDAD DE COMUNICACIONES Y REDES

Las conexiones no seguras a los servicios de red pueden afectar a todo la organización, por lo tanto, se controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos.

El Responsable del Área de Recursos en la Nube tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal del titular de una Unidad Organizativa que lo solicite para personal de su incumbencia.

Este control es particularmente importante para las conexiones de red a aplicaciones que procesen información clasificada o aplicaciones críticas, o a usuarios que utilicen el acceso desde sitios de alto riesgo, por ejemplo áreas públicas o externas que están fuera de la administración y del control de seguridad de la organización.

POLITICA:

- Establecer los procedimientos para la administración del equipamiento remoto, incluyendo los equipos en las áreas usuarias, la que será llevada a cabo por el responsable establecido en el punto “Asignación de Responsabilidades en Materia de Seguridad de la Información”.
- Establecer controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados. Implementar controles especiales para mantener la disponibilidad de los servicios de red y computadoras conectadas.
- Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información.
- Utilización de certificados SSL junto a funciones criptográficas para asegurar la transferencia de archivos.
- Cada instancia creada en AWS maneja sus listas de control de Acceso, las cuales son restringidas en base a los permisos que debe tener esa aplicación.
- Cada subred, también restringirá en AWS por los denominados Security Groups, que tienen como función realizar restricciones a nivel de puerto (UDP, TCP) e IP, así como servicio que manejen.
- Cada Zona de disponibilidad contará con un firewall que tendrá asociado IPS que permita o restringa el acceso en base a los permisos otorgados.
- Cada Región utilizará un servicio de VPN que restringe el acceso a ciertas IP tanto a nivel de red como a nivel de la capa de transporte.

9. MANTENIMIENTO DE EQUIPOS Y SU DESECHO

(RESPONSABILIDAD DEL PROVEEDOR) En este apartado el mantenimiento de equipos, así como los nodos de integración lo maneja Amazon a través de su plataforma, lo que se tiene en cuenta son las notificaciones que se envían por correo electrónico, indicando reinicio o cambio de nodo por fallas o mantenimiento, para este fin se siguen los siguientes pasos en su desarrollo:

- La notificación es recibida por correo electrónico al responsable del soporte de los nodos en AWS.
- Una vez recibido se procede a seguir los pasos previstos en el correo y se destina una fecha y hora de ejecución de dicha notificación.
- Se realiza la acción en la hora y fecha indicada, si es necesario con el soporte de AWS.
- Una vez realizada se llena un informe de cambio o mantenimiento de nodos.

10. CONTROL DE CAMBIOS Y CONFIGURACIÓN

OBJETIVO:
Proporcionar el Procedimiento de control de versiones y gestión de cambios de software, con el objetivo de tener un inventario de los mismos y mantener una trazabilidad de cambios y mejoras.

ALCANCE:
El alcance de este procedimiento es relacionado con productos y proyectos que han sido puestos en producción en alguna empresa o para alguna funcionalidad dentro de la organización. No debe incluirse en este procedimiento lo siguiente:

- Código Fuente que no haya probado previamente.
- Código Fuente que provenga de un externo.

REFERENCIA:

Para la elaboración de este documento, se consideró las disposiciones y normativas que se detallan a continuación:

- Norma ISO 9001:2015.
- Norma ISO/IEC 27001:2013
- Guía de Buenas Prácticas ITIL – AXELOS.
- Metodología ágil SCRUM.
- Mejores Prácticas de SVN.

POLITICA DE CONTROL DE CAMBIOS Y CONFIGURACIÓN

N°	ACTIVIDAD	RESPONSABLE	DOCUMENTO
1	Registrar la versión en base al formato FOR.AAPL.004, en el cual contiene dos secciones: • Datos del Proyecto: Donde se incluye la fecha de creación, nombre del proyecto, fecha de registro, código del proyecto, lenguaje de programación, sistemas operativos, base de datos, descripción del proyecto(en caso sea	Responsable del Área de Aplicaciones	Formato de Hoja de Control de Versiones o Cambios

	cambio, describir el cambio, en caso sea nuevo detallar lo que realizará el proyecto) y el objetivo del proyecto. • Versiones del Proyecto: Que contiene el número de la versión, con el código de la versión, así como las características adicionales y alguna observación o comentario. Este documento debe ser aprobado y firmado por el encargado del área.		
2	Ingresar el código fuente en el software de repositorios de código fuente y todos los archivos involucrados a este proyecto. Finalmente se envía un correo donde se colocará el link donde está el repositorio para que se guarde el proyecto nuevo o la nueva versión para el cambio efectuado.	Responsable del Área de Aplicaciones	Formato de Hoja de Control de Versiones o Cambios

11. PLAN DE RESPALDO

Para asegurar que se consideran todas las posibles eventualidades, se relacionan las actividades que se deben realizar con el objeto de prever, mitigar o eliminar los riesgos conocidos para el SOLUCIONES APLICADAS EN TECNOLOGÍA AVANZADA:

Nº	Actividad	Elementos	Resultado
1	Copias de seguridad de la información y documentos residentes en servicios de repositorios de archivos	Documentos en formato PDF, imágenes, archivos de texto.	Una copia de seguridad en la nube en línea opcional, una, Copia de seguridad diaria obligatoria de todos los documentos. **Responsable:** Líder de Soporte de la Plataforma
2	Copias de Seguridad de los sistemas de información y Bases de Datos del Módulo Documentos Digitales	Aplicación Web de la Aplicación. Base de datos de administración y gestión de Documentos Digitales. Plataforma de Firma Digital. Plataforma de Servicios Web.	Copia de seguridad semanal de los sistema de información activos de la Entidad. **Responsable:** Líder de Soporte de la Plataforma
3	Contar mínimo con un kit de instalación para restaurar los archivos del sistema operativo y aplicaciones de un computador o servidor en caso de falla.	Sistemas Operativos. Aplicaciones Web.	Contar con mínimo un medio de instalación por cada miembro de la oficina de Soporte de la Plataforma. **Responsable:** Líder de Soporte de la Plataforma
4	Mantener descentralizados los sistemas de información	Sitio WEB, Base de Datos, aplicaciones fuera de línea en seccionales.	Aplicaciones instaladas en diferentes localizaciones físicas, computadores o servidores. **Responsable:** Líder de Soporte de la Plataforma
5	Actualizar las claves o contraseña de acceso	Base de Datos, y sistemas de información del Módulo	Mínimo cada tres meses o cuando se requiera por el

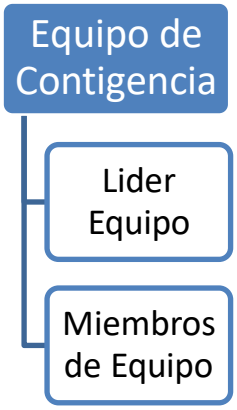
	a las aplicaciones y bases de datos del Módulo de Documentos Digitales.	de Documentos Digitales.	usuario o por reemplazos del cargo. **Responsable:** Líder de Soporte de la Plataforma
6	Disponibilidad de redundancia de recursos para evitar la interrupción de la prestación del servicio en los sistemas de información de la Entidad.	Nodos de Aplicación y Base de Datos	Evitar la suspensión del servicio a los usuarios teniendo una alternativa adicional, que es una zona de disponibilidad adicional que se encuentra en otra Región y así garantizar la alta disponibilidad.

Los registros que se generen con la aplicación de este documento se deben conservar y archivar**.**

12. PLAN DE RECUPERACION Y RESPALDO DE LA INFORMACION:

El costo de la Recuperación en caso de desastres severos, como los de un terremoto que destruya completamente los nodos que la organización tenga en AWS, estará directamente relacionado con el valor de la replicación y puesta en marcha de la plataforma en otra zona de disponibilidad. Este plan de restablecimiento estratégico del servicio de documentos digitales será abordado en la parte de Actividades Posteriores al desastre.

El paso inicial en el desarrollo del plan contra desastres, es la identificación de las personas que serán las responsables de la ejecución del Plan de contingencia. Por tanto se definen los siguientes responsables:



Líder de equipo: Será responsable de liderar las acciones correctivas definidas anteriormente a fin de minimizar los riesgos establecidos.
Miembros del equipo: Será responsable de realizar las acciones correctivas a fin de minimizar los riesgos.

Un Plan de Recuperación de Desastres se clasifica en tres etapas:

- Actividades Previas al Desastre.
- Actividades Durante el Desastre.
- Actividades Después del Desastre.

12.1. ACTIVIDADES PREVIAS AL DESASTRE

Se considera las actividades de actividades de resguardo de la información, en busca de un proceso de recuperación con el menor costo posible para la Entidad. Se establece los procedimientos relativos a:

- Nodos e Información
- Obtención y almacenamiento de los Respaldos de Información (BACKUPS).

a. Activos de Información

Los activos de información que se cuentan en este proceso son definidos en el siguiente cuadro, definidos por una Criticidad dependiendo la sensibilidad de la información manejada:

Activo	Criticidad
Base de Datos	Alto
Nodo de Aplicación	Medio

Nodo de Firma	Medio
Nodo de Servicios Web	Medio

b. Obtención y almacenamiento de Copias de Seguridad (Backups)

Se debe contar con procedimientos para la obtención de las copias de seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los sistemas en la organización. Las copias de seguridad son las siguientes:

- Backups del Nodo: Todas las versiones de sistema operativo instalados en la Red. (Periodicidad – Cada día).
- Backups de los datos: Todos los registros necesarios (Periodicidad – Cada día, replicados en línea cada vez que haya modificación de configuración).

12.2. ACTIVIDADES DURANTE EL DESASTRE (PLAN DE EMERGENCIAS)

Presentada la contingencia o desastre se debe ejecutar las siguientes actividades planificadas previamente:

Plan de Emergencias

La presente etapa incluye las actividades a realizar durante el desastre o siniestros, se debe tener en cuenta la probabilidad de su ocurrencia durante: el día, noche o madrugada. Este plan debe incluir la participación y actividades a realizar por todas y cada una de las personas que se pueden encontrar presentes como soporte o en el área misma, descritas a continuación.

Buscar Respaldo en la otra zona de disponibilidad

Es de tener en cuenta que solo se debe realizar acciones de resguardo de nodos en los casos en que no se pone en riesgo la operatividad de la organización. Normalmente durante en la acción del siniestro es necesario. Para ello:

- Se debe tener en cuenta la disponibilidad de la AZ (Avaliability Zone).
- Realizar la migración completa de los nodos de manera sincronizada, siguiendo la secuencia de los siguientes, a través del panel de administración de procesos en Amazon:

Activo	**Orden de Instalación**
Base de Datos	Primer
Nodo de Firma	Segundo
Nodo de Aplicación	Tercero
Nodo de Servicios Web	Cuarto

- Instruir al personal dedicado al proceso de respaldo de la empresa respecto a la forma de migrar, con el manual de instalación y prevención de continuidad de negocio, esto se realiza acorde a los Planes de Contingencia (Seguridad y Continuidad del Negocio) organizadas por la empresa.

Formación de Equipos

Se debe establecer los equipos de trabajo, con funciones claramente definidas que deberán realizar en caso de desastre. En caso de que el siniestro lo permita (al estar en un inicio o estar en un área cercana, etc.), se debe formar 02 equipos de personas que actúen directamente durante el siniestro, un equipo para combatir el siniestro y evaluar los riesgos potenciales, así como el daño causado (Brigadas de Seguridad) y el otro para salvamento de los nodos y la información (Equipo de contingencia en TI), teniendo en cuenta la clasificación de prioridades.

BRIGADA DE SEGURIDAD
1 Responsable de Brigada de Seguridad
Brigada de Siniestro
1 Supervisor de Brigada y 1 Miembro
Brigada de Riesgos
1 Supervisor de Brigada y 1 Miembro
BRIGADA DE CONTINGENCIA EN TI
1 Líder de Equipo
2 Miembro de Contingencia

Entrenamiento

Se debe establecer un programa de prácticas periódicas con la participación de todo el personal involucrado en la lucha contra los diferentes tipos de siniestro, de acuerdo a los roles que se hayan asignado en los planes de seguridad del personal o equipos. Es importante lograr que el personal tome conciencia de que los siniestros pueden realmente ocurrir; y tomen con seriedad y responsabilidad estos entrenamientos; para estos efectos es conveniente que participen todo el personal.

12.3. ACTIVIDADES DESPUÉS DEL DESASTRE

Estas actividades se deben realizar inmediatamente después de ocurrido el siniestro:

12.3.1. Evaluación de daños

El objetivo es evaluar la magnitud del daño producido, es decir, que sistemas se están afectando, que nodos han quedado inoperativos, cuales se pueden recuperar y en cuanto tiempo. Se debe atender a los equipos e información relacionados a la Región, por la importancia estratégica. La recuperación y puesta en marcha de los servidores que alojan dichos sistemas, es prioritario.

12.3.2. Priorizar Actividades

La evaluación de los daños reales nos dará una lista de las actividades que debemos realizar, preponderando las actividades estratégicas y urgentes de nuestra institución. Las actividades comprenden la recuperación y puesta en marcha de los nodos ponderados y los Sistemas de Información, etc.

12.3.3. Ejecución de actividades

La ejecución de actividades implica la colaboración de todo el personal involucrado, creando Equipos de Trabajo, asignando actividades. Cada uno de estos equipos deberá contar con un líder que deberá reportar el avance de los trabajos de

recuperación y en caso de producirse un problema, reportarlo de inmediato al Comité de SGSI, brindando posibles soluciones.

Los trabajos de recuperación se iniciaran con la restauración del servicio usando los recursos de la empresa, teniendo en cuenta que en la evaluación de daños se contempló y gestionó la adquisición de los nodos o información dañados. La segunda etapa es volver a contar con los recursos en las cantidades y lugares propios del Sistema de Información, debiendo ser esta última etapa lo suficientemente rápida y eficiente para no perjudicar la operatividad de la institución y el buen servicio de nuestro sistema e Imagen Institucional.

12.3.4. Evaluación de Resultados

Una vez concluidas las labores de Recuperación de los sistemas y equipos que fueron afectados por el siniestro, debemos de evaluar objetivamente, todas las actividades realizadas, con que eficacia se hicieron, que tiempo tomaron, que circunstancias modificaron (aceleraron o entorpecieron) las actividades, como se comportaron los equipos de trabajo, etc. De la evaluación de resultados y del siniestro, deberían de obtenerse dos tipos de recomendaciones, una la retroalimentación del Plan de Contingencias, y otra una lista de recomendaciones para minimizar los riesgos y pérdida que ocasionaron el siniestro.

12.3.5. Retroalimentación de Actividades

Con la evaluación de resultados, podemos mejorar las actividades que tuvieron algún tipo de dificultad y reforzar los elementos que funcionaron adecuadamente.

13. AUDITORIAS Y DETECCIÓN DE INTRUSIONES

El Responsable de Seguridad Informática, realizará revisiones periódicas de todas las áreas dela Organización a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad. Entre las áreas a revisar se incluyen las siguientes:

- Sistemas de información.
- Proveedores de sistemas.
- Propietarios de información.
- Usuarios.

Los Propietarios de la Información brindarán apoyo a la revisión periódica del cumplimiento de la política, normas, procedimientos y otros requisitos de seguridad aplicables.

CONTROLES DE AUDITORÍA DE SISTEMAS

Cuando se realicen actividades de auditoría que involucren verificaciones de los sistemas en producción, se tomarán recaudos en la planificación de los requerimientos y tareas, y se acordará con las áreas involucradas a efectos de minimizar el riesgo de interrupciones en las operaciones.

Se contemplarán los siguientes puntos:

a. Acordar con el Área que corresponda los requerimientos de auditoría.
b. Controlar el alcance de las verificaciones. Esta función será realizada por el responsable de auditoría.
c. Limitar las verificaciones a un acceso de sólo lectura del software y datos de producción. Caso contrario, se tomarán los resguardos necesarios a efectos de aislar y contrarrestar los efectos de las modificaciones realizadas, una vez finalizada la auditoría. Por ejemplo:
    - Eliminar archivos transitorios.
    - Eliminar entidades ficticias y datos incorporados en archivos maestros.
    - Revertir transacciones.
    - Revocar privilegios otorgados
d. Identificar claramente los recursos de tecnologías de información (TI) para llevar a cabo las verificaciones, los cuales serán puestos a disposición de los auditores. A tal efecto, la Unidad de Auditoría o en su defecto quien sea propuesto por el Comité de Seguridad de la Información completará el siguiente formulario, el cual deberá ser puesto en conocimiento de las áreas involucradas:

Recursos de TI a Utilizar en la Verificación	
Aplicaciones	……
Servicio de Custodia de Documentos	……
Capa de Servicios	……
Base de Datos	……
Componente de Firma	……
Medios Magnéticos	……
Conexiones a Red	……

e. Identificar y acordar los requerimientos de procesamiento especial o adicional.
f. Monitorear y registrar todos los accesos, a fin de generar una pista de referencia. Los datos a resguardar deben incluir como mínimo:
    - Fecha y hora.
    - Puesto de trabajo.
    - Usuario.
    - Tipo de acceso.
    - Identificación de los datos accedidos.

- Estado previo y posterior.

g. Documentar todos los procedimientos de auditoría, requerimientos y responsabilidades.

14. MEDIOS DE ALMACENAMIENTO

Los medios de almacenamiento se rigen en base a los tipos de repositorio que se manejan actualmente, los cuales son:

- Por servidor de archivos o medios magnéticos.
- Por el servicio S3 de Amazon.

El Responsable del Área Aplicaciones y Desarrollo, con la asistencia del Responsable de Seguridad Informática, implementará procedimientos para la administración de medios informáticos removibles, como cintas, discos, casetes e informes impresos.

Se deberán considerar las siguientes acciones para la implementación de los procedimientos:

a) Eliminar de forma segura los contenidos, si ya no son requeridos, de cualquier medio reutilizable que ha de ser retirado o reutilizado por la organización.
b) Requerir autorización para retirar cualquier medio de la organización y realizar un control de todos los retiros a fin de mantener un registro de auditoría.
c) Almacenar todos los medios en un ambiente seguro y protegido, de acuerdo con las especificaciones de los fabricantes o proveedores.

ELIMINACIÓN DE MEDIOS DE INFORMACIÓN

El Responsable del Área Aplicaciones y Desarrollo, junto con el Responsable de Seguridad Informática definirá procedimientos para la eliminación segura de los medios de información respetando la normativa vigente. Los procedimientos deberán considerar que los siguientes elementos requerirán almacenamiento y eliminación segura:

a) Documentos electrónicos.
b) Voces u otras grabaciones.
c) Discos o casetes removibles.
d) Nodos o Servidores.
e) Medios de almacenamiento óptico (todos los formatos incluyendo todos los medios de distribución de software del fabricante o proveedor).
f) Listados de programas.
g) Datos de prueba.
h) Documentación del sistema.

Asimismo, se debe considerar que podría ser más eficiente disponer que todos los medios sean recolectados y eliminados de manera segura, antes que intentar separar los ítems sensibles.

PROCEDIMIENTOS DE MANEJO DE LA INFORMACIÓN

En los procedimientos se contemplarán las siguientes acciones:

a) Incluir en la protección a documentos, sistemas informáticos, redes, computación móvil, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general, multimedia, servicios e instalaciones postales, uso de máquinas de fax y cualquier otro ítem potencialmente sensible.
b) Restringir el acceso solo al personal debidamente autorizado
c) Mantener un registro formal de los receptores autorizados de datos
d) Garantizar que los datos de entrada son completos, que el procesamiento se lleva a cabo correctamente y que se valida las salidas.

e) Proteger los datos en espera ("colas").
f) Conservar los medios de almacenamiento en un ambiente que concuerde con las especificaciones de los fabricantes o proveedores.

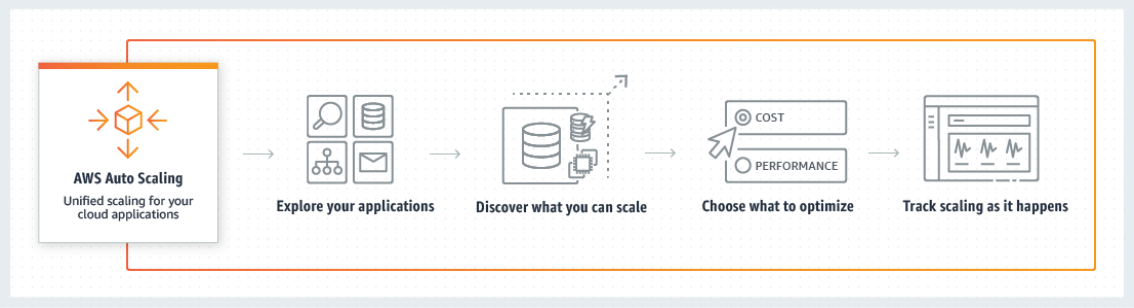
SEGURIDAD DE LA DOCUMENTACIÓN DEL SISTEMA

La documentación del sistema puede contener información sensible, por lo que se considerarán los siguientes recaudos para su protección:

a) Almacenar la documentación del sistema en forma segura.
b) Restringir el acceso a la documentación del sistema al personal estrictamente necesario. Dicho acceso será autorizado por el Propietario de la Información relativa al sistema.

15. PLANIFICACIÓN DEL SISTEMA:

Para realizar el monitoreo y la planificación de la capacidad de nuestras futuras demandas realizamos un proceso de evaluación a través de nuestra herramienta AWS CloudWatch que realiza la gestión del monitoreo y seguimiento de los procesos y también tenemos un servicio denominado AWS Auto Scaling que realiza el escalado de aplicaciones con la intención de mejorar el nivel de desempeño. AWS Auto Scaling monitoriza nuestras aplicaciones y ajusta automáticamente la capacidad para mantener un desempeño predecible y estable al menor costo posible, lo cual resulta sencillo configurar el escalado de aplicaciones para distintos recursos en varios servicios en cuestión de poco tiempo.



Este servicio nos trae los siguientes beneficios:

- Nos permite definir niveles de uso específicos para varios recursos en una única interfaz intuitiva. Puede ver rápidamente el uso promedio de todos los recursos de escala ajustable sin tener que ir a otras consolas.
- Nos permite crear planes de escalado que automatizan la manera en la que diferentes recursos responden ante los cambios que se producen en la demanda.
- Nos permite conservar niveles óptimos de disponibilidad y desempeño de las aplicaciones, inclusive cuando las cargas de trabajo sean periódicas, impredecibles o se modifiquen continuamente. Para esto se monitoriza continuamente las aplicaciones para garantizar que estén funcionando de acuerdo con los niveles de desempeño definidos. Cuando se producen picos en la demanda, AWS Auto Scaling aumenta automáticamente la capacidad de los recursos limitados para poder conservar el alto nivel de calidad del servicio.