Manual de Política de Seguridad de la Información

Tabla de Contenido

1. Información del Documento

1.1. Responsable del Documento

- Jefe Departamento seguridad de la información

1.2. Aprobador del Documento

- Comité de seguridad de la información

1.3. Fecha de aprobación

- 27 de abril de 2023

1.4. Historial de Cambios

Nombre	Fecha	Cambios	Versión
Osbaldo Rojas/Julieta Rincón	Diciembre de 2018	Creación	01
Osbaldo Rojas/Julieta Rincón	Marzo de 2023	Modificación	02

2. Propósito

La política de seguridad de la información de EBSA ha sido establecida con el fin de proteger todos los activos de información y los ciberactivos críticos, incluyendo, pero no limitado a; los documentos, computadores, dispositivos móviles y componentes de la infraestructura de red de TI y TO que son propios, alquilados, o de otra manera mantenidos, controlados y/o usados por el personal de EBSA. Esto incluye, pero no se limita a todas las instalaciones de sistemas de información corporativos, componentes de redes telefónicas y sistemas de apoyo, las redes de comunicaciones y la información almacenada, transmitida y/o procesada por estas instalaciones. Los requisitos de la política se aplican a toda la información de propiedad o administrada por EBSA, sin importar su forma o ubicación.

3. Perspectiva general y alcance

La política de seguridad de la información de EBSA aplica para todos los funcionarios, contratistas, pasantes y practicantes, así como cualquier tercero que interactué, acceda o almacene los activos de información de EBSA. Esta política se aplica a todos los activos y ciberactivos de información sin importar su formato o ubicación.
La política de seguridad de la información esboza el proceso de protección de la confidencialidad, disponibilidad e integridad de la información. EBSA define la información como "datos asociados con significado y propósito" y la protección de la información incorpora los siguientes criterios:

- Confidencialidad

La confidencialidad de la información de los activos y ciberactivos críticos, incluyendo, pero no limitado al capital intelectual, la información confidencial, la información no clasificada pero sensible perteneciente a EBSA, y la información confidencial de socios comerciales.

- Integridad

La información de los activos y ciberactivos críticos debe estar protegida contra el acceso ilícito, la destrucción y/o la modificación para garantizar la integridad de la información.

- Disponibilidad

La información de los activos y ciberactivos críticos debe estar disponible cuando y donde sea necesario para apoyar los procesos de análisis y toma de decisiones que le permiten a EBSA funcionar eficientemente y prestar servicios a sus partes interesadas de manera efectiva. Se espera que los sistemas críticos para la operación del negocio estén disponibles en todo momento durante el horario laboral aplicable según lo establecido en el plan de recuperación de desastres de EBSA.
Los sistemas de gestión de la seguridad de la información eficaces incorporan una gama de políticas, productos de seguridad, tecnologías y procedimientos. EBSA se compromete a garantizar la seguridad de sus empleados y activos, así como la integridad de su reputación frente a posibles amenazas. La salvaguardia de la información confidencial, así como de la información del cliente y la privacidad es de vital importancia para EBSA.
Esta política proporciona la orientación general y los principios fundamentales para asegurar niveles adecuados de seguridad, confidencialidad, integridad y disponibilidad de la información de los activos y ciberactivos críticos de propiedad de EBSA o bajo su custodia. Esta política soporta la protección de la información de EBSA proporcionando de manera segura la información correcta, en el momento adecuado, con los recursos apropiados. Las políticas y procedimientos establecidos en esta política también pueden ser aplicados para otros propósitos y prácticas aplicables a pesar de que esta política se centra en la seguridad.

4. Generalidades

4.1. Visión de Seguridad

Permitir a EBSA crecer con éxito preservando y protegiendo la información que le permite al negocio cumplir con los objetivos establecidos y simplificar la forma en que EBSA opera a través de una fuerte gestión de la seguridad de la información, los controles y la gestión eficaz del riesgo.

4.2. Misión de Seguridad

Garantizar la confidencialidad, integridad y disponibilidad de la información de los activos y ciberactivos críticos en todos los formatos basados en criterios y requisitos específicos y en una tolerancia al riesgo predeterminada.

4.3. Compromiso de Gestión de la Compañía

La alta dirección apoyará activamente la seguridad dentro de la organización a través de la dirección clara, el compromiso, la asignación explícita y el reconocimiento de las responsabilidades de seguridad.

La gerencia general designará a un Oficial de Seguridad de la Información - en inglés "CISO" (Chief Information Security Officer) cuya responsabilidad será la de proporcionar la dirección, asignación y supervisión de las responsabilidades en materia de seguridad.

4.4. Responsabilidad de Seguridad

El gobierno de la seguridad es un marco establecido para garantizar que todos los elementos de seguridad puestos en marcha para proteger nuestro entorno de datos funcionan de manera eficiente, cumple lo que se pretende y lo hace de manera rentable.

Los cuatro pilares para el gobierno de la seguridad de la información son:

- Compromiso del comité de gerencia,
- Visión y estrategia de seguridad,
- Estructura de gestión de la seguridad de la información, y
- Capacitación y concienciación.

4.5. Objetivos y actividades de la gestión de la seguridad de la información:

Los objetivos de la gestión de la seguridad de la información incluyen lo siguiente:

- Definir objetivos claros, roles y responsabilidades en relación con la seguridad de la información.
- Asegurar que se cuente con el personal suficiente para desempeñar las funciones y de esta manera garantizar el éxito del programa de seguridad de la información;
- Demostrar la eficacia de la buena gestión de riesgos de seguridad de la información;
- Avanzar a un nivel de madurez de seguridad superior, según corresponda;
- Proporcionar un marco homogéneo para las decisiones relativas a los riesgos de seguridad de la información;
- Desarrollar políticas y procesos de seguridad de la información;
- Ser proactivo y no reactivo.

Las actividades de gestión de la seguridad de la información incluyen lo siguiente:

- Definir, implementar y mantener una política global de seguridad de la información y unas directrices, estándares y procesos;
- Gestionar el programa de sensibilización;
- Monitorear el progreso y cumplimiento de la política de seguridad de la información, así como de las directrices, estándares, y procesos;
- Definir los indicadores clave de rendimiento de seguridad;
- Monitorear el cumplimiento de las leyes y reglamentos referentes a la seguridad de la información;
- Gestionar el riesgo de seguridad de la información;
- Apoyar y asesorar en la corrección de las recomendaciones de las auditorías de seguridad de la información;
- Monitorear el acceso a los sistemas críticos;
- Informar sobre el progreso en la implementación del programa de seguridad de la información, así como de los principales riesgos y los incidentes de seguridad;
- Autorizar cualquier desviación (excepción) a las directivas de seguridad de acuerdo con el proceso de manejo de excepciones.

4.6. Supervisión

Para asegurar que la seguridad sea supervisada adecuadamente y que todas las áreas del negocio estén incluidas, EBSA establecerá un «Comité de seguridad de la información». Este comité, encabezado por el Gerente general y con la participación del Jefe Departamento de Seguridad de la información, Jefe Oficina de Control de Gestión, Jefe Oficina de Planeación y Regulación, Director Informática y el Gerente de Distribución. La misión de este grupo es:

a. Enlazar y coordinar con las diversas áreas funcionales de EBSA para asegurar que haya una línea clara de comunicación que permita plantear asuntos o inquietudes y transmitir la información de seguridad a todos los empleados de EBSA.
b. Obtener el apoyo y la cooperación de todas las partes interesadas por medios formales e informales.
c. Comunicar el estado y las necesidades de la seguridad de la información a todas las partes interesadas.
d. Servir como canal de comunicación eficaz para cumplir los objetivos y lineamientos de gestión y proveer una base continua para asegurar la alineación del programa de seguridad con los objetivos de la organización.
e. Proporcionar orientación e información a la alta gerencia de la empresa en los siguientes aspectos:

Tendencias en seguridad:

- Gestión y supervisión del marco de seguridad de la información y presentación de la eficacia del programa de seguridad de la información para cumplir con los objetivos de la organización.
- Gestión, supervisión y mantenimiento de la política y de los estándares de seguridad de la información.
- Revisión y aprobación del proceso de todas las excepciones de las políticas y estándares de seguridad de la información.
- Revisión y aprobación de la estrategia de seguridad de la información.
- Aseguramiento de canales de comunicación apropiados sobre riesgos de información en todos los niveles y en especial en la dirección ejecutiva.
- Aseguramiento de la toma de medidas apropiadas en aquellas áreas en donde los riesgos de información han sido identificados y evaluados como riesgos que requieren de la toma de acciones, así como del monitoreo de estas medidas.
- Definición de instrumentos clave para generar un cambio de conducta hacia una cultura que promueva buenas prácticas de seguridad de la información y de cumplimiento de políticas.

- Delegar la autoridad necesaria para garantizar un eficaz funcionamiento de las políticas de seguridad de la información.

5. Terminología

Para facilitar la comprensión del presente documento, se definen los siguientes términos:

- Activo de información: Son aquellos datos o información que tienen valor para la organización.
- Activo crítico: Instalaciones, sistemas o equipos eléctricos que, de ser destruidos, degradados o puestos indisponibles, afecten la confiabilidad (suficiencia y seguridad), operatividad, o que comprometan la seguridad de la operación del SIN.
- Ciberactivo: Dispositivo electrónico programable y elementos de las redes de comunicaciones incluyendo hardware, software, datos e información. Así como aquellos elementos con protocolos de comunicación enrutables, que permitan el acceso al mismo de forma local o remota.
- Red Privada Virtual - en inglés "VPN" (Virtual Private Network): es una conexión de red privada segura construida sobre una red pública, como Internet.
- Contraseña: es una forma de autenticación que utiliza información secreta para controlar el acceso a la cuenta en uso de las credenciales de acceso asignadas.
- Caracteres especiales: Caracteres especiales generales, matemáticos, griegos y símbolos.
- Vulnerabilidad: Ausencia o debilidad de un control. Condición que podría permitir que una amenaza se materialice con mayor frecuencia, mayor impacto o ambas. Una vulnerabilidad puede ser la ausencia o debilidad en los controles administrativos, técnicos y/o físicos. Dicha vulnerabilidad puede ser materializada por una amenaza.
- Amenaza: Factor externo que aprovecha una debilidad en los activos de información y puede impactar en forma negativa en la organización.
- Remediación: Acción que permite minimizar el impacto de las vulnerabilidades en la organización.
- Plan de Remediación: Permite identificar los riesgos asociados a cada vulnerabilidad reportada, así como definir los controles que deben ser implementados para mitigar dichos riesgos.
- Escaneo de vulnerabilidades: Mecanismo que permite identificar los fallos de seguridad de un sistema operativo y de sus servicios. Dicho procedimiento puede ser realizado de forma manual o utilizar herramientas que automatizan el proceso.
- Ingeniería social: Consiste en la recolección de información de una persona utilizando estrategias y acciones que no involucran instrumentos físicos, por ejemplo, mentiras, trampas, sobornos o amenazas.
- Alerta: Hace referencia a una situación de vigilancia o atención. Un estado o una señal de alerta es un aviso para que se extremen las precauciones o se incremente la vigilancia de un determinado activo.
- Evento de seguridad: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad. [ISO/IEC 27000:2009].
- Incidente de seguridad de la información: Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazar la seguridad de la información. [ISO/IEC 27000:2009]
- Log: Registro de los sistemas de información que permite verificar las tareas o actividades realizadas por determinado usuario o sistema.
- Impacto: Consecuencias que produce un incidente de seguridad sobre la organización.

6. Principios y lineamientos

6.1. Principios:

El Programa de seguridad de la información de EBSA opera bajo los siguientes principios:

a. Se garantizará la confidencialidad de la información corporativa y del cliente.
b. La información no clasificada como pública (sin importar su formato) será protegida contra el uso o acceso no autorizado.
c. EBSA cumplirá con las leyes nacionales, departamentales y municipales, con los requisitos reglamentarios, las obligaciones contractuales y con las políticas de EBSA relacionadas con la seguridad de la información.
d. Los procesos empresariales de EBSA serán coherentes con los principios anteriores y, a menos que sean contrarios a la ley, las políticas corporativas o los estándares de configuración de los sistemas de EBSA, deberán seguir las políticas de seguridad de la información de EBSA.
e. Todos los empleados de EBSA deben cumplir con las políticas, procesos, procedimientos y requisitos reglamentarios publicados por EBSA con el fin de proteger los activos y ciberactivos críticos de EBSA.
f. Todos los usuarios son responsables de reportar cualquier vulnerabilidad, incumplimiento o actividad inusual que se haya sospechado, descubierto o detectado.
g. Todos los empleados de EBSA están obligados a apoyar activamente los principios anteriores y se espera que tomen medidas razonables para proteger los activos de información y ciberactivos críticos a su cuidado asegurando:
    - Que funcionan de acuerdo con sus requisitos aplicables.
    - Que están protegidos contra el acceso no autorizado.
    - Que tienen salvaguardias adecuadas y suficientes.
    - Que no hay mal uso de la información
h. El Departamento de seguridad de la información en cooperación con los líderes empresariales y funcionales de EBSA, aplicarán esta política y todas las demás políticas, procedimientos operativos estándar, estándares y protocolos informáticos establecidos para dar cumplimiento y soporte de esta política.
i. Cuando las políticas de seguridad, políticas, procedimientos operativos, estándares del sistema y protocolos no pueden ser cumplidos, una excepción a la política debe ser solicitada y aprobada por el propietario de la información y el Oficial de Seguridad de la Información - en inglés "CISO" (Chief Information Security Officer) y llevado a Comité de seguridad para su evaluación.
j. La implementación de la política de seguridad de la información se revisará de manera independiente de aquellos que se encarguen de su implementación.
k. Cuando sea necesario, la organización de seguridad de la información establecerá y mantendrá contactos apropiados con otras organizaciones, autoridades policiales, organismos reguladores y operadores de redes y telecomunicaciones con respecto a su política de seguridad de la información.

7. Políticas de apoyo

Las siguientes políticas completan el Marco de políticas corporativas de seguridad de la información y soportan la Política de Seguridad de la Información, que incluye, pero no se limita a estas políticas:

7.1. Política de Uso aceptable

Esta política documenta el uso apropiado de los recursos de información en EBSA. Estas normas están en vigor para proteger tanto a los empleados como a EBSA. El uso inapropiado expone a EBSA a riesgos incluyendo ataques de virus, compromiso de sistemas y servicios de red y asuntos legales.

Este documento también define las expectativas de los sistemas que supervisan y limitan el uso de la web de todos los dispositivos dentro de la red de EBSA. Las expectativas están diseñadas para asegurar que los empleados utilicen internet de manera segura y responsable, y que el uso de la web por parte de los empleados puede ser monitoreada durante un incidente. Esta política también permite definir y distinguir el uso aceptable/apropiado del uso inaceptable/inapropiado.

7.2. Política de Clasificación de la información

Toda la información, independientemente de la forma, formato o ubicación, que se crea o utiliza en apoyo de las actividades comerciales de EBSA, es información corporativa. Como tal, esta información tiene un valor intrínseco a EBSA sin importar dónde o en qué formato reside, y dependiendo de su valor y riesgo para la organización, necesita ser protegida en consecuencia. Es fundamental proporcionar seguridad adecuada sobre toda la información basada en su clasificación.

El propósito de esta política es describir las medidas y responsabilidades necesarias para clasificar y asegurar los recursos de información con el fin de abordar el riesgo de destrucción, modificación, divulgación, acceso, uso o eliminación no autorizada de información.

La información se clasificará en función de sus requisitos de sensibilidad, cumplimiento legal, retención y tipo de acceso requerido por los empleados y otro personal autorizado. La clasificación de la información se basa en su valor y el riesgo que representa para la organización si cae en manos equivocadas o se hace pública.

7.3. Política de control de acceso (incluido acceso remoto y acceso de terceros)

El control del acceso a los recursos de información es esencial para proteger la información de personas no autorizadas. El acceso a los sistemas de información de EBSA se otorga de una manera que se equilibre cuidadosamente las restricciones diseñadas para impedir el acceso no autorizado y la necesidad de proporcionar acceso sin obstáculos a los activos de información y ciberactivos críticos para satisfacer las necesidades del negocio. Los requisitos de control de acceso incluyen medidas de seguridad para proteger los datos personales y otra información corporativa no clasificada como Pública.

Esta política incluye los requisitos para el acceso remoto a los recursos informáticos de EBSA utilizando una Red Privada Virtual - en inglés "VPN" (Virtual Private Network) o una tecnología similar de acceso remoto. Una VPN es una conexión de red privada segura construida sobre una red pública, como Internet. El acceso inapropiado puede exponer a EBSA a riesgos incluyendo ataques de virus, compromiso de sistemas y servicios de red y asuntos legales. Esta política también incluye las reglas para conceder acceso a la red de EBSA o a los centros de datos a los consultores, contratistas, vendedores, socios comerciales, compañías de seguridad y otros proveedores de servicios (terceros). Esta política está diseñada para minimizar el riesgo potencial de exposición no autorizada a las instalaciones y a la información de los activos de información y ciberactivos críticos de EBSA proveniente de los

riesgos asociados con el acceso de terceros. Un tercero es considerado cualquier persona o entidad externa que no está directamente empleada o afiliada a EBSA. Los terceros incluyen, pero no se limitan a invitados, empleados que utilizan sus propios dispositivos, o compañías externas y su personal. Esta política se aplica tanto al acceso físico como remoto a las instalaciones y sistemas de EBSA.

7.4. Política de contraseñas

El propósito de esta política es establecer los criterios para la creación de contraseñas seguras, la protección de esas contraseñas y su frecuencia de cambio. La combinación de un ID de usuario y una contraseña proporciona acceso autenticado a los sistemas y servicios de EBSA.

7.5. Política de cifrado

El cifrado es un método para transformar información clara y significativa en una forma incomprensible. El uso del cifrado garantiza que la información cifrada conserva su confidencialidad, autenticidad e integridad.

El propósito de esta política es proporcionar orientación sobre el uso efectivo del cifrado. Esta aborda el riesgo de usar algoritmos de encriptación inadecuados y el riesgo de usar soluciones de encriptación no autorizadas.

7.6. Política de protección contra malware

El propósito de esta política es proporcionar un completo programa de protección contra el malware para EBSA, describiendo qué sistemas de servidores deben tener aplicaciones antivirus y/o antispyware. Esta política está diseñada para minimizar riesgos potenciales y para asegurar la confidencialidad, integridad y disponibilidad de los datos de EBSA de manera general.

7.7. Política inalámbrica

Las redes de datos inalámbricas son atractivas por la comodidad que ofrecen. La implementación segura de equipos de red inalámbrica es otra cuestión. Esta política describe cómo se despliegan y utilizan las redes inalámbricas, con el objetivo de proteger la red de EBSA. Describe el despliegue aceptable de la infraestructura de red inalámbrica, incluidos los requisitos de conexión física, configuración segura y métodos de acceso. También aborda los mecanismos de aplicación y la autoridad para la provisión.
A diferencia de las redes cableadas tradicionales, el acceso a una red inalámbrica no se limita al espacio físico de la oficina. Debido a que las señales inalámbricas penetran las paredes y los pisos, es necesario emplear las características de seguridad apropiadas para garantizar que sólo aquellas personas que estén autorizadas a acceder a los recursos de la red corporativa puedan hacerlo a través de instalaciones inalámbricas y proteger la información confidencial de EBSA que viaja a través de estas redes.

7.8. Política de registro, monitoreo y auditoría

El registro, monitoreo y auditoría de sistemas le brinda a EBSA la capacidad de identificar y rastrear problemas dentro de los sistemas y de algunas aplicaciones. El propósito de esta política es asegurar que los registros son recolectados y las revisiones de registro son realizadas regularmente por personas que están calificadas para entender las amenazas que enfrentan los sistemas y la manera en que estos riesgos pueden ocurrir.

Los registros de seguridad de la computadora son generados por varias entradas del sistema, incluyendo; software de seguridad, como software antivirus; firewalls; sistemas de detección y prevención de intrusos; sistemas operativos en servidores, estaciones de trabajo; y equipos de red, enrutadores, entre otros.

El uso de registros permite la creación de "pistas de auditoría" mediante la reconstrucción o revisión de elementos de registro generados por sistemas y procesos de aplicación y actividad asociada. Mediante el uso de procedimientos y herramientas adecuadas, se pueden utilizar pistas de auditoría para detectar infracciones de seguridad, problemas de rendimiento del sistema y fallas en las aplicaciones empresariales. Los registros de auditoría suelen contener información sobre eventos de seguridad, como intentos de autenticación, acceso a archivos, cambios en la política de seguridad, cambios en la cuenta (por ejemplo, creación y eliminación de cuentas, asignación de privilegios de cuentas) y uso de privilegios.

7.9. Política de manejo, almacenamiento y eliminación de datos

Los datos son información que es propiedad de EBSA y que apoyan su misión. El acceso a la información se proporciona según sea necesario y ya que no todos requieren acceso a toda la información, algunos sistemas de EBSA contienen información que tiene acceso restringido. Esta información debe estar protegida en consecuencia del acceso no autorizado en todas las fases del ciclo de vida de la información.

El propósito de esta política es asegurar que todo el personal y aquellos empleados contratados por terceros a los que se les haya concedido acceso a la información o a los sistemas de EBSA, utilicen mecanismos físicos y técnicos para asegurar el manejo seguro, transferencia y almacenamiento de datos a través de documentos electrónicos y físicos, impresiones, cintas, discos y otros medios.

7.10. Política de gestión del cambio tecnológico

La gestión del cambio es el proceso por medio del cual se controla la creación e introducción de cambios en el entorno técnico para minimizar las interrupciones del servicio. Esta política identifica los requisitos para implementar los cambios dentro de la infraestructura tecnológica e incluye requisitos específicos para controlar las interrupciones no planificadas de la infraestructura informática de los activos de información y ciberactivos críticos.

7.11. Política de administración de revisiones

Esta política identifica los requisitos para realizar cambios en los sistemas informáticos de producción para mantener, entre otras cosas, una fuerte postura de seguridad. Esta política asegura que las vulnerabilidades conocidas se identifican, priorizan y remedian, en función de su nivel de riesgo.

7.12. Política de desarrollo de software

Para proteger mejor a la organización, la seguridad debe integrarse en las nuevas aplicaciones y sistemas desde su inicio y durante todo el ciclo de vida del desarrollo. Los detalles incluidos en esta política son un conjunto mínimo de requisitos a considerar para desarrollar aplicaciones y bases de datos con el nivel de seguridad adecuado.

Todo software desarrollado por EBSA debe ser configurado de manera segura para proteger la información contenida en el sistema y ponerlo en conformidad con las declaraciones establecidas en la política. El plan de cumplimiento y el cronograma deben ser coordinados con el departamento de Seguridad de la Información.

El propósito de esta política es proporcionar a los desarrolladores de aplicaciones, los administradores de bases de datos y a los gerentes un conjunto de directrices relacionadas con el desarrollo seguro de aplicaciones y bases de datos.

7.13. Política de evaluación de riesgos

Las evaluaciones del riesgo de tecnología de la información forman parte de la política de gestión del riesgo de la información para garantizar la gestión responsable y la seguridad de la información y de los recursos de información. Son realizadas con el fin de evaluar los riesgos de la información, los programas, sistemas, servicios y espacios físicos.

El propósito de la política de evaluación de riesgos es asegurar que la Dirección de informática de EBSA o el tercero responsable de la seguridad realice evaluaciones periódicas del riesgo tecnológico (se recomienda hacerlas trimestralmente) en los sistemas informáticos corporativos con el propósito de determinar áreas de vulnerabilidad e iniciar un esfuerzo correctivo apropiado.

7.14. Política de formación para la concienciación en seguridad

Una seguridad efectiva siempre dependerá de las personas. Como resultado, la seguridad sólo puede ser efectiva si los empleados saben lo que se espera de ellos, cuáles son sus responsabilidades y las repercusiones de violar la seguridad. El propósito de esta política es asegurar que todos los empleados de EBSA reciban capacitación adecuada en sensibilización sobre la seguridad para que ellos puedan ser responsables y hacer a otros responsables del cumplimiento de las políticas de seguridad de la información.

Las actividades de concienciación sobre seguridad están diseñadas para presentar principios de alto nivel de protección de la información a todo el personal de EBSA en una variedad de formatos. El propósito de las presentaciones de sensibilización es simplemente centrar la atención en la seguridad con el objetivo de mejorar el conocimiento del personal con respecto a la protección de los activos de información y ciberactivos críticos de EBSA. Los empleados que toman la capacitación de sensibilización tienen una mejor comprensión de sus responsabilidades, un mayor nivel de responsabilidad para adherirse a las políticas, y pueden reconocer las preocupaciones de seguridad tecnológica y responder en consecuencia.

8. Control de documentos y políticas de gestión

Esta política y todos los documentos de apoyo al marco de políticas se revisarán y actualizarán según sea apropiado, anualmente o con más frecuencia, si los cambios importantes en las reglas de negocios, procesos tecnológicos, objetivos organizacionales, ley local u objetivos de seguridad de la información ameritan cambios para asegurar su continuidad, conveniencia, suficiencia y efectividad. La revisión de esta política también tendrá en cuenta los resultados de las revisiones por la dirección u otras actividades de auditoría/cumplimiento.
La siguiente información será presentada en la revisión por la dirección:
Los cambios que podrían afectar el enfoque de la organización para la gestión empresarial de la seguridad de la información,

El cumplimiento de la política de seguridad de la información y el desempeño del proceso,

Los comentarios de las partes interesadas y de las autoridades pertinentes,

Las tendencias relacionadas con amenazas, vulnerabilidades e incidentes,

El estado de las acciones preventivas y correctivas,

Los resultados de los exámenes de gestión anteriores, y

Los resultados de revisiones independientes o auditorías internas.

En respuesta a la información presentada, la gerencia propondrá acciones relacionadas con:

- La mejora del enfoque de la organización para la gestión de la seguridad de la información y sus procesos.
- La mejora de los objetivos de control y asignación de recursos y/o responsabilidades.

Las recomendaciones resultantes de una auditoría se tendrán en cuenta en la planificación estratégica y en la mejora continua de la seguridad de la información.

Las modificaciones significativas y las revisiones de esta política y de todos los documentos de apoyo del marco de políticas, así como cualquier solicitud importante de desviación de esta política, se presentarán al Comité de Gestión de la Seguridad.

9. Excepciones

No todas las políticas se ajustan a todas las situaciones, ya que un tamaño no se ajusta a todos. Cuando las aplicaciones, procedimientos u otras actividades no cumplan con los requisitos de una política o procedimiento de seguridad, se debe realizar una adaptación por medio de una excepción a la política.

En tales casos, es necesario que la Dirección o jefatura correspondiente complete un proceso formal de excepción por escrito, como se describe a continuación, antes de proceder con cualquier acción. A través de la aprobación ejecutiva de la excepción, la unidad de negocio se responsabiliza de todos los riesgos relacionados con la excepción.

A. Cuando los sistemas o procedimientos se vean afectados negativamente debido a la aplicación de políticas de seguridad, se puede solicitar una excepción a la sección apropiada de dicha política utilizando el formulario de Excepción de Política de Seguridad.

B. Como parte del proceso de excepción, el solicitante deberá proporcionar:

   i. Una explicación detallada de por qué se requiere la excepción, incluyendo:
      a. Impactos.
      b. Otros factores.
   ii. El esfuerzo realizado para cumplir con los requisitos de política.
   iii. Los controles compensatorios que se están utilizando para gestionar el riesgo.
   iv. El riesgo residual.

C. Una excepción a la política es una cuestión comercial, así como una cuestión tecnológica. El jefe de área o director que solicita la excepción deberá aceptar el riesgo como parte del proceso de aprobación. La Dirección de Informática también deberá aprobarla, así como cualquier otra área afectada.

D. Se llevará a Comité de seguridad para evaluar su aprobación.

E. Se concederán excepciones por un período máximo de un año. Si se requiere una excepción por un período más largo, debe renovarse.

10. Cumplimiento

El incumplimiento de cualquiera de las disposiciones de la presente política podrá generar el inicio de un procedimiento disciplinario de acuerdo con la normatividad laboral colombiana, el Reglamento interno de trabajo y la Convención colectiva de trabajo de la EBSA (para quienes les es aplicable).

El resultado de la investigación disciplinaría podrá generar acciones de carácter sancionatorio y/o inclusivo la terminación del contrato por justa causa. En los casos en los que corresponda, se reportará a las autoridades competentes para que se adelanten las investigaciones a que haya lugar.

Apéndice A

Uso aceptable de la política de tecnología de la información

1. Información general

La Política de uso aceptable de EBSA está diseñada para apoyar y proteger a sus empleados, socios, clientes y a la organización de acciones ilegales o dañinas por parte de individuos, ya sea a sabiendas o sin saberlo. Los equipos informáticos, dispositivos móviles, software, sistemas operativos, medios de almacenamiento, las cuentas de red que proporcionan el correo electrónico, la mensajería instantánea, fax, el correo de voz y la navegación web son de propiedad de EBSA, excepto en la medida en que ciertos dispositivos sean de propiedad personal. Estos sistemas deben ser utilizados con fines comerciales para servir a los intereses de la organización y de sus clientes en las operaciones normales.

La seguridad efectiva es un esfuerzo de equipo que involucra la participación y el apoyo de todos los empleados de EBSA y de otros que se encargan del manejo de la información y/o de los sistemas de información. Es responsabilidad de cada usuario conocer y comprender esta política y llevar a cabo sus actividades en consecuencia.

2. Propósito

El propósito de esta política es describir el uso aceptable de los equipos informáticos de EBSA. Estas reglas están diseñadas para proteger al empleado y a EBSA. El uso inapropiado expone a EBSA a riesgos incluyendo ataques de virus, compromiso de sistemas y servicios de red y asuntos legales.

3. Política

3.1. Propiedad y uso general

Salvo que se disponga lo contrario de manera expresa en esta política, el uso de los activos de información o ciberactivos críticos de EBSA está restringido para propósitos relacionados con la realización de negocios o prestación del servicio.

Los empleados son responsables de ejercer un buen juicio con respecto al uso personal razonable. EBSA permite un uso personal limitado para las comunicaciones con la familia; el aprendizaje independiente y el servicio público, siempre y cuando no interfiera con la productividad del personal y con cualquier actividad empresarial; comprometa la seguridad o la reputación de EBSA o cargue a EBSA con incrementos de costos notorios.

Los empleados de EBSA no deben involucrarse en ninguna actividad que sea ilegal bajo la ley local o internacional mientras utilizan recursos de propiedad de EBSA o recursos bajo licencia.
EBSA se reserva el derecho de monitorear cualquier uso de Internet, red y correo electrónico, y acceder y revelar cualquier información almacenada en los sistemas de EBSA o transmitida usando las redes de EBSA, con o sin el conocimiento del usuario. EBSA puede ejercer dicho derecho periódicamente para garantizar la seguridad del sistema, supervisar el cumplimiento de las políticas corporativas, cumplir con un propósito comercial válido, evaluar el impacto de internet y el uso del correo electrónico en el rendimiento del empleado y la eficiencia del negocio o cumplir con cualquier orden o requisito de un tribunal, agencia administrativa u otro organismo gubernamental.

No debe haber expectativa de privacidad relacionada con las comunicaciones y la información que se accede o se distribuye utilizando los recursos de internet y correo electrónico de EBSA o se almacena en un disco duro local o en la red. Toda la información creada, accedida, almacenada o comunicada a través de un computador de EBSA o de la red, incluso información de carácter personal es propiedad de EBSA.

Los administradores de los sistemas u otras personas con responsabilidades de monitoreo no pueden examinar el correo electrónico o la información almacenada de una persona sin la aprobación apropiada. Hacer caso omiso es considerado como una violación de la Política de Seguridad de la Información.

3.2. Seguridad y confidencialidad de la información

3.2.1. Mantenga las contraseñas seguras y no comparta información de cuentas. Los propietarios de cuentas son responsables de la seguridad de estas y de sus contraseñas. Se considera que toda la actividad de la cuenta ha sido iniciada por el propietario de esta y este es responsable de esa actividad. Los incumplimientos deben ser reportados inmediatamente al departamento de seguridad de la información.

3.2.2. Todas los computadores portátiles y estaciones de trabajo deben estar protegidas con un protector de pantalla protegido por contraseña con configuración de activación automática establecida en 15 minutos.

3.2.3. Todos los datos o archivos transferidos a la infraestructura tecnológica de EBSA deberán estar libres de virus.

3.2.4. Aunque por su naturaleza, el correo electrónico y la mensajería instantánea parecen ser menos formales que otras comunicaciones escritas, se les aplican las mismas leyes. Por lo tanto, es importante que los usuarios sean conscientes de los riesgos legales por el uso del correo electrónico, y de que ellos y EBSA pueden ser considerados responsables si:

- Usted envía o reenvía mensajes de correo electrónico o mensajes instantáneos con contenido calumnioso, difamatorio, ofensivo, racista u obsceno;
    - Usted envía ilegalmente información confidencial; y/o
- A propósito, envía un archivo adjunto que contiene un virus u otra tecnología destructiva.

3.2.5. Si recibe un correo electrónico de un remitente desconocido, no debe abrir ningún archivo adjunto, ya que puede contener malware, virus, gusanos u otro malware.

3.2.6. Al acceder a internet mediante una conexión que no sea de EBSA, los usuarios deben ser conscientes de que los Access point públicos pueden no ser tan seguros como parecen, ya que han sido utilizados por criminales para capturar información personal y corporativa. La solución de acceso remoto aprobada por EBSA debe utilizarse para conectarse a cualquier información de EBSA.

3.2.9. Las firmas automáticas que contienen la información personal de contacto y la información de EBSA están estandarizados para seguir los estándares de la marca EBSA. Todos los correos electrónicos a destinatarios externos deben ser etiquetados con una advertencia estándar de correo electrónico para (a) garantizar el cumplimiento legal, (b) administrar y mitigar los diversos riesgos asociados con el uso del correo electrónico y (c) contar con buenas prácticas de gobierno corporativo.

3.2.10. El uso de medios extraíbles, incluyendo, pero no limitado a USB, unidades externas, CD/DVD ROM, etc., está permitido sólo en dispositivos aprobados por EBSA. Los puertos USB se configurarán para reconocer los dispositivos compatibles, de lo contrario, sólo proporcionarán alimentación.

3.2.10.1. Las políticas y procedimientos relacionados con lo anterior están en desarrollo y hasta que las mismas sean completadas, usted debe hacer todo lo posible para garantizar su cumplimiento.

3.2.11. El uso de correo electrónico basado en la web, p. Gmail, Hotmail, Shaw, etc. está prohibido para fines comerciales.

3.3. Uso de la tecnología

Las siguientes actividades, en general, están prohibidas. La siguiente lista no es exhaustiva, pero intenta proporcionar un marco para las actividades que están dentro de la categoría de uso inaceptable. Los usuarios no deberán:

- Instalar cualquier tipo de software. Todo software requerido para propósitos de negocios será instalado por la Dirección de Informática. Todos los programas informáticos deben seguir los acuerdos de derechos de autor o licencias de software de EBSA.
- Utilizar software no estándar en los recursos informáticos de EBSA sin la aprobación departamento de seguridad de la información o la Dirección de Informática.
- Hacer copias no autorizadas de recursos con derechos de autor o propiedad de EBSA o licencia de software, datos, etc.
- Operar los negocios de EBSA usando cuentas personales de correo electrónico o compartir información corporativa con cuentas personales de correo electrónico.
- Hacer ofertas fraudulentas de productos, artículos o servicios que provienen de una cuenta de EBSA.
- Participar en cualquier tipo de actividad utilizando activos o recursos electrónicos de EBSA para ganancia personal, actividad ilegal u otro propósito en violación de las políticas de la compañía, los procedimientos o en contra de los mejores intereses de EBSA.
- Enviar mensajes que contengan lenguaje, imágenes, etc. que contengan materiales ofensivos, despectivos o abusivos, incluyendo aquellos que sean sexualmente explícitos o profanos.
- Utilizar los sistemas de EBSA para uso personal que le pudiera causar congestión, retraso o interrupción del servicio a cualquier recurso tecnológico. Por ejemplo, tarjetas de felicitación, vídeo, sonido u otros archivos adjuntos de gran tamaño pueden degradar el rendimiento de toda la red, al igual que algunos usos de la tecnología "push", como la transmisión de audio/vídeo desde internet.
- Intentar acceder a los datos, documentos, correspondencia por correo electrónico y programas contenidos en los sistemas de EBSA para los cuales no se tiene autorización.
- Compartir información de cuentas, contraseñas, Números de Identificación Personal "Personal Identification Numbers (PIN)", códigos de seguridad, o información similar o dispositivos utilizados para fines de identificación y autorización.
- Intentar monitorear cualquier transmisión de datos u otras comunicaciones por cualquier medio.
- Intentar realizar pruebas de seguridad o evaluaciones de cualquier tipo, excepto cuando se requiera de manera explícita para realizar una función relacionada con su trabajo.
- Acceder a información que no se requiere para el desempeño del trabajo, o iniciar sesión utilizando una cuenta a la que el empleado no está expresamente autorizado a acceder.
- Evitar la autenticación de usuario o la información de seguridad de cualquier computador, red o cuenta.
- Conectar dispositivos que eludan los controles de seguridad de Internet y/o de la red de EBSA.
- Utilizar recursos para beneficio personal, actividad política, publicidad no solicitada, recaudación no autorizada de fondos o para la solicitud de la realización de cualquier actividad que esté prohibida por la ley.
- Permitir que los usuarios no autorizados accedan a cualquier sistema informático de EBSA.
- Enviar mensajes de correo electrónico no solicitados, incluyendo el envío de "correo no deseado" u otro material publicitario a personas que no soliciten específicamente dicho material (correo electrónico spam).
- Alterar o falsificar información de identificación tal como la información del encabezado del correo electrónico.

- Crear o enviar "cadenas de cartas" u otros esquemas de "pirámide" de cualquier tipo.
- Cuando participen en blogs personales o en redes sociales, los empleados no deben atribuir declaraciones, opiniones o creencias personales a EBSA. Si un empleado está expresando sus creencias y/u opiniones en blogs, el empleado no puede, expresa o implícitamente, representarse como empleado o representante de EBSA. Los empleados asumen todos y cada uno de los riesgos asociados con los blogs.
- Hacer público o revelar información corporativa, secretos comerciales, etc. que está restringida debido a su clasificación.
- Introducir programas maliciosos en la red o en el servidor (por ejemplo, virus, gusanos, códigos de troyanos, etc.)
- Dañar la imagen de EBSA.

3.4. Comunicaciones por mensajería instantánea

- El uso de mensajería instantánea está disponible dentro del ambiente interno de EBSA y debe usarse para propósitos administrativos y causales. Sólo se puede utilizar el correo electrónico aprobado por la compañía para fines comerciales esenciales.
- Durante las sesiones de mensajería instantánea, los usuarios deben ser conscientes de la sensibilidad de la información de EBSA que se intercambia y deben cumplir con la Política de clasificación de la información de EBSA durante dichas sesiones.

3.5. Buzones y correos electrónicos compartidos

Los Directores o Gerentes que soliciten una cuenta de correo electrónico compartida serán responsables de toda la actividad en esa cuenta. Con el propósito de designar a un grupo que debe leer y responder a los mensajes de correo electrónico que se envían a una dirección en particular, deben observarse los siguientes niveles de control preferidos.

3.5.1.1. Los propietarios de cuentas de correo electrónico compartidas deben estar indicados en los comentarios de la libreta de direcciones del buzón correspondiente.

3.5.1.2. El propietario de la cuenta de correo electrónico compartida debe ser un Director o un Gerente que tenga la responsabilidad general de la cuenta y de su uso

3.5.1.3. Limitar el número de miembros que utilizan la cuenta compartida en donde tanto las opciones de envío como de recepción son requeridas. El propietario debe delegar acceso de lectura sólo al buzón a menos que sea parte de la responsabilidad de un usuario enviar correos electrónicos de la cuenta en nombre de un grupo o equipo.

3.6. Adquisición de equipos informáticos

3.6.1. Los computadores, fotocopiadoras, impresoras, escáneres y otros equipos asociados han sido estandarizados en EBSA ya que están conectados a la red de EBSA. Los equipos que no son comprados de acuerdo con este requisito no serán soportados en o por la red de EBSA.

3.7. Licencias y distribución de software

3.7.1. Las licencias de software para computadores (por ejemplo, Microsoft Office, etc.) son propiedad de EBSA y están protegidas por la ley internacional de derechos de autor. Cualquier duplicación de software fuera de las limitaciones del acuerdo de licencia de un editor es una violación de la ley internacional de copyright y constituye una violación de la licencia. Como tal:

3.7.1.1. Los usuarios no pueden hacer copias de software, revenderlo, transferirlo a otro computador o red, o entregarlo a otra persona para su uso;

3.7.1.2. El software no puede ser entregado a terceros (incluyendo familiares y amigos) o ser transferido o hacerse disponible electrónicamente a través de un contrato de uso compartido, de una red u otro sistema que proporciona acceso a múltiples usuarios a menos que se haya obtenido una licencia adecuada (como una licencia de red), obtenida por EBSA;

3.7.1.3. Se prohíbe estrictamente la copia, la distribución, el montaje inverso, la compilación inversa, la traducción o la modificación de programas informáticos por parte de los empleados de EBSA, ya sea en el computador personal o en la red de EBSA;

3.7.1.4. Si necesita usar un software de EBSA en su casa, primero debe consultar con la dirección de informática para asegurarse de que la licencia para ese software permite el uso doméstico;

3.7.1.5. No se instalará ningún software o hardware no autorizado en ningún recurso tecnológico de EBSA a menos que sea aprobado por la dirección de informática de EBSA. Cualquier software o hardware no aprobado puede ser removido por el personal de la dirección de informática de EBSA sin previo aviso o advertencia; y

3.7.1.6. La adquisición o desarrollo de nuevos sistemas será revisada y aprobada por la dirección de informática de EBSA antes de la compra o despliegue.

4. Responsabilidades

Persona / Grupo	**Responsabilidad dentro del alcance de esta política**
Comité de Gerencia	Llamar el equipo de respuesta a incidentes de seguridad informática y los protocolos de recuperación de desastres. Revisar la información de riesgos y aprobar iniciativas de mitigación estratégicas y operacionales.
Directores, Jefes de Departamento	Proporcionar el compromiso empresarial y la comunicación necesarios para apoyar las iniciativas de gestión del riesgo tecnológico. Aceptar riesgos calificados para la organización de EBSA
Director de Informática(TI)	Garantizar la alineación tecnológica con los negocios de EBSA. Patrocinar el programa de gestión del riesgo tecnológico y aprobar la estrategia de gestión del riesgo tecnológico. Aprobar todas las políticas relacionadas con la información de EBSA.
Oficial de Seguridad de la Información	Mantenimiento general, interpretación y comunicación de la política de Uso Aceptable. Aprobar o rechazar solicitudes de exención/desviación de la política. Desarrollar y ejecutar la estrategia de seguridad de la información.

Empleados de EBSA	Identificar y reportar los riesgos y son responsables de la protección de los activos que se utilizan para facilitar la actividad comercial del negocio. Todos los empleados de la empresa, contratistas o empleados temporales a los que se les ha otorgado el derecho de usar el acceso a Internet de la organización deben dar fe de este acuerdo confirmando su comprensión y aceptación de esta política: • En el momento de la contratación • Anualmente desde ese momento.
Comité de seguridad de la información	Proporcionar la estructura y dirección para las iniciativas de gestión del riesgo tecnológico. Monitorear y medir el desempeño del programa de riesgo tecnológico y evaluar el vencimiento del riesgo anualmente.
	Realizar auditorías y revisiones puntuales para asegurar que los usuarios cumplan con los controles descritos en el Marco de Gestión de Riesgos. Actualizar y revalidar la política de seguridad de la información. Definir la tolerancia al riesgo de EBSA. Proporcionar asesoría, orientación y competencia en la gestión de eventos de seguridad. Facilitar el proceso de exención.
Control de Gestión	Revisar de manera independiente la Estrategia de gestión del riesgo tecnológico.

Apéndice B

Política de clasificación de la información

1. Información general

Toda la información, independientemente de la forma, formato o ubicación, que se crea o utiliza en apoyo de las actividades comerciales de EBSA, es información corporativa. Como tal, esta información tiene un valor intrínseco a EBSA no importa dónde o en qué formato reside, y, dependiendo de su valor y riesgo para la organización, necesita ser protegida en consecuencia. Es fundamental proporcionar seguridad adecuada sobre toda la información basada en su clasificación.

La información puede ser casi cualquier cosa. Puede ser almacenada electrónicamente en un documento o en una base de datos, enviada por correo electrónico, enviada por fax, escaneada, impresa, transmitida, enviada electrónicamente, enviada físicamente en medios electrónicos o puede estar en papel, exhibida en una página web, en vídeo e incluso almacenada como comunicación verbal, como es el caso de los mensajes de voz.

La clasificación de la información se basa en su valor y en el riesgo que representa para la organización si cae en manos equivocadas o se hace pública. Generalmente, el propietario de la información determina el nivel de clasificación aplicado a su información. Para asegurar que la información esté debidamente protegida, el propietario de la información trabajará con el centro de servicios de tecnológicos para identificar cómo se utilizará, procesará y distribuirá esta información.

La información debe ser mantenida de manera segura, precisa y confiable y estar disponible para uso autorizado. Las medidas de seguridad de la información se aplicarán acorde al valor, la sensibilidad y el riesgo de la información. Para garantizar la clasificación y el manejo adecuado de los activos de información, debe mantenerse un inventario de toda la tecnología e información clasificada como confidencial. El inventario debe identificar el propietario y la ubicación de la información.

2. Propósito

El propósito de esta política es describir las medidas y responsabilidades necesarias para clasificar y asegurar los activos de información y ciberactivos con el fin de hacer frente al riesgo de destrucción, modificación, divulgación, acceso, uso y eliminación de información.

La información se clasificará en función de sus requisitos de sensibilidad, cumplimiento legal, retención y tipo de acceso requerido por los empleados y por otro personal autorizado. Las políticas y procedimientos relacionados con lo anterior están en desarrollo y hasta que se complete el mismo, usted debe hacer todo lo posible por cumplir con esta política.

Según se define en la Política de seguridad de la información, los activos de información incluyen, pero no se limitan a; el papel, los computadores, dispositivos móviles, redes y activos de información y ciberactivos críticos de propiedad, arrendados o de otra manera mantenidos, controlados y/o utilizados por EBSA.

3. Política

Para ayudar en el manejo apropiado de la información, se debe usar una jerarquía de clasificación de la sensibilidad en EBSA. Esta jerarquía proporciona una forma abreviada de referirse a la sensibilidad de la información y puede usarse para simplificar las decisiones de seguridad de la información y minimizar los costos en este aspecto. Los propietarios de la información deben agregar un nivel de clasificación a toda la información que se recopila, procesa, almacena y usa.

El tratamiento de los datos personales está descrito en el documento *Manual de procedimientos en materia de protección de datos de carácter personal MA-01.*

4. Clasificaciones

Para implementar la seguridad al nivel apropiado, la información en EBSA se clasifica en una de las siguientes tres categorías de clasificación: (A) Confidencial, (B) Interna y (C) Pública.

Clasificación	Descripción	Ejemplos
Privada o Confidencial	• Es la clasificación disponible más alta. La información con esta clasificación incluye información recopilada y utilizada por EBSA en el manejo de su negocio, para emplear a personas, registrar y cumplir con pedidos, y administrar todos los aspectos de las finanzas corporativas. • El acceso a esta información es muy limitado dentro de la organización. Es vital mantener los niveles más altos de integridad, confidencialidad y disponibilidad. • La divulgación no autorizada, la pérdida de la confiabilidad de la información y/o de la disponibilidad de información confidencial causaría daños que afectarían negativamente a EBSA o podrían causar otros daños serios.	• Ingresos consolidados, ganancias u otros resultados financieros no públicos para EBSA. • Diseño de productos o servicios no anunciados. • Fechas de anuncio de nuevos productos o servicios. • Previsiones financieras. • Información del empleado que no es específica del trabajo, Ejemplo. Historial médico o historial de crédito. • Investigaciones e informes de seguridad. • Información Personal de Salud e Información de Identificación Personal, tanto de clientes como de empleados. • Planificación financiera o análisis de información. • Ingresos, costos, utilidades u otros resultados financieros de la unidad de negocios.

		• Información que define los procesos especiales en el diseño del producto. • Número de identificación emitido por el gobierno, es decir, número de seguro social. • Información de salario.

Interna o semiprivada	• Esta es la clasificación por defecto que se aplicará a cualquier información en la que no se haya indicado ninguna clasificación. • Interna es la categoría más grande de clasificación. Aunque parte de la información puede parecer de naturaleza no sensible, tiene un valor inherente o propietario para EBSA. • La información interna de EBSA no es para divulgación pública a menos de que se haya firmado un acuerdo de no divulgación o se haya recibido la aprobación de la gerencia. • La divulgación no autorizada, la pérdida de fiabilidad y/o de disponibilidad de la información interna podrían causar daños menores o ayudar a la ingeniería social / inversa, la recolección de información y/o el perfil de objetivos.	• Información de las instalaciones. • Dibujos arquitectónicos de instalaciones. • Información de empleados no privada. • Información del proveedor. • Organigramas. • Diagramas de red. • Políticas, Normas y Procedimientos.

Pública	• Pública es una clasificación para la información que ha sido autorizada para ser liberada y consumida por el público.	• Comunicados de prensa. de la empresa. • Boletines empresariales • Contenido del sitio web. • Información de marketing. • Propuestas públicas.

5. Clasificación por defecto

La clasificación predeterminada es interna o semiprivada. Cualquier documento que no haya sido etiquetado caerá dentro de esta clasificación. Al seguir los lineamientos de EBSA respecto al principio de privilegios mínimos, tener acceso a cierta información en las categorías confidencial o interna no proporciona al usuario acceso a toda la información de la categoría. No importa la clasificación, el acceso a la información se proporciona sólo para cumplir con los requerimientos de trabajo.

6. Roles y responsabilidades

Pueden establecerse las siguientes funciones y responsabilidades para apoyar el cumplimiento de la clasificación de la información:

Rol	Responsabilidad
Propietario de la Información	Tener responsabilidad empresarial directa a nivel operativo para la gestión de la información que crean o administran. Una de las responsabilidades de propiedad incluye el establecimiento de la clasificación de los datos, así como asegurar la existencia de acceso suficiente a los datos y a cuestiones de control.
Custodio de Información - Electrónica	La Dirección de Informática es el custodio de la información. El custodio es responsable de proveer una infraestructura segura en apoyo de la información, incluyendo, pero no limitado a proporcionar seguridad física, procesos de respaldo y recuperación, otorgar privilegios de acceso a los usuarios del sistema según lo autoricen los propietarios de la información o sus delegados, implementar y administrar los controles sobre la información.
Custodio de información - No Electrónica	El propietario de la información debe identificar al custodio asegurando que los controles apropiados están en su lugar para proteger la información.
Usuario	Cualquier persona que haga uso de la información.

7. Opciones de control

Cada activo de información clasificada estará sujeto a varias opciones de control que sean relevantes para la sensibilidad de la información. Los propietarios deben decidir a quién se le permitirá acceder a la información, y los usos que se le darán a la información. Adicionalmente, el Custodio de Información debe tomar medidas para asegurar que se utilizan controles apropiados en el almacenamiento, manipulación, distribución y uso regular de la información.

8. Cambios en la clasificación

Con el tiempo, el significado o el valor de la información puede cambiar. Cuando hay un cambio sustancial en el valor de la información, su clasificación debe ser revisada. Cuando el valor ha disminuido, los requisitos de seguridad también pueden haber disminuido y la clasificación debe cambiarse para reflejar eso. Lo mismo se aplica a la información que se vuelve más sensible.

Apéndice C

Política de control de acceso

Esta política incluye los siguientes tres componentes: Control de acceso, Acceso remoto y Acceso de terceros.

Control de Acceso

1. Información general

El control del acceso a los recursos de información es esencial para proteger la información de personas no autorizadas. El acceso a la información y a los sistemas de EBSA se otorga de una manera que equilibra cuidadosamente las restricciones diseñadas para impedir el acceso no autorizado y la necesidad de proporcionar acceso sin obstáculos a los activos informativos para satisfacer las necesidades del negocio. Los requisitos de control de acceso incluyen medidas de seguridad para proteger los datos personales y otra información corporativa no clasificada como Pública.

2. Propósito

El propósito de esta política es proporcionar los requisitos de control de acceso a los sistemas de información de EBSA con el fin de proteger:

- La confidencialidad
- Integridad
- Y disponibilidad de la información.

3. Política

Todas las personas que utilizan los recursos de tecnología de información de EBSA deben estar autorizadas para acceder a los sistemas y recursos apropiados. El acceso es controlado y monitoreado de acuerdo con la política de EBSA.

A. Los elementos que intervienen en el control y supervisión del acceso incluyen la identificación, autorización y autenticación.

i. Identificación - A todos los usuarios se les asigna una identificación única o ID para el acceso a los sistemas y aplicaciones de EBSA. Los ID de usuario no se deben compartir. Los usuarios son responsables de mantener la seguridad de sus identificaciones y de toda la actividad que se realice bajo esas identificaciones.

ii. Autorización - Sólo los empleados que tienen razones válidas para acceder a los sistemas de EBSA y a la información se les conceden privilegios de acceso adecuados a sus necesidades de negocio.

iii. Autenticación - La autenticación garantiza una identidad. Cada ID requiere una técnica, usualmente una contraseña, para validar la identidad. A medida que las necesidades o requerimientos del negocio requieran el uso de autenticaciones alternativas adicionales, se podrían emplear alternativas tales como las de dos factores (un token o un certificado con una contraseña o PIN). Los ejemplos de dónde puede ser apropiado aplicarlas incluyen, pero no se limitan a, claves de aplicaciones financieras, acceso remoto, acceso de terceros, etc.

iv. Excepciones - Bajo ciertas condiciones, las personas que representan a los proveedores que soportan hardware o software, consultores o auditores pueden tener acceso al sistema. Tales conexiones también deben cumplir con los controles apropiados de identificación, autenticación y duración. Todos los terceros que accedan a cualquiera de los sistemas de EBSA deben diligenciar y firmar el documento de acuerdo de acceso apropiado.

B. El acceso a la información, sistemas o aplicaciones debe seguir un procedimiento documentado de registro de usuarios para conceder el acceso. Ningún usuario puede solicitar y aprobar su propia solicitud de acceso, incluso si dicha autoridad de aprobación fue delegada por una autoridad superior. Los altos ejecutivos deben tener solicitudes aprobadas por el Oficial de Seguridad de la Información - en inglés "CISO" (Chief Information Security Officer).
C. El acceso a la información de los activos de información y ciberactivos críticos debe proporcionarse sobre la base de la necesidad y debe seguir los principios de acceso de privilegios mínimos y de segregación de funciones con el fin de restringir el acceso no autorizado a la información.
D. El nivel de acceso otorgado a un usuario para el acceso a la información y sistemas debe soportar, pero no exceder, lo que sea necesario para desempeñar sus responsabilidades y funciones. La asignación de los derechos de acceso debe basarse en la clasificación y función de un individuo, o en las responsabilidades laborales.
E. Los privilegios elevados de acceso de emergencia sólo pueden concederse en una situación crítica, para completar una tarea o función específica relacionada con tal situación. Tales privilegios elevados de acceso son temporales y sólo están disponibles durante el tiempo necesario para resolver la situación crítica. Estos privilegios deben registrarse junto con todas las tareas realizadas.
F. Como condición para proporcionar una cuenta en cualquier sistema, se informará a los usuarios que dicho acceso o cualquier actividad realizada por medio de la cuenta asignada puede ser registrada, supervisada o auditada, sobre la base de restricciones legales y reglamentarias, y que el usuario será responsable de manera exclusiva de todas las actividades realizadas con dicha cuenta.
G. El acceso se realiza de acuerdo con el proceso de aprobación de acceso a la cuenta. Se prohíbe a los empleados compartir cuentas de aplicaciones/sistemas con identificación exclusiva. Cuando se requiera que los empleados de EBSA reciban identificaciones no únicas, dicho acceso estará limitado por la función y la responsabilidad del trabajo. El proceso de aprobación de acceso debe ser iniciado por el jefe directo del empleado y los privilegios otorgados deben permanecer en vigor hasta que el empleado cambie de trabajo o abandone EBSA. Si ocurre cualquiera de los dos eventos, Recursos Humanos debe notificar inmediatamente a la Dirección de informática.
H. Cuando un empleado abandona EBSA, todos los privilegios del sistema cesan inmediatamente, y el acceso a la información de EBSA también debe cesar de inmediato. El acceso a los recursos se revisará periódicamente a través de la información del sistema y de la certificación. Si el evento ocurre, Talento Humano debe notificar inmediatamente a la Dirección de Informática.

   La Dirección del Talento Humano utilizando el medio que la dirección de informática disponga, reportará la inactivación temporal de las cuentas de usuario de los diferentes sistemas en los siguientes casos: licencias, vacaciones, sanciones, permisos remunerados y no remunerados mayores a tres días. Se exceptúa el acceso a Directorio activo y correo electrónico, los cuales no serán bloqueados para Gerentes y Asesores de la compañía por necesidad del negocio; sin embargo, deberá ser solicitado por la Dirección de Talento Humano a la Dirección de informática a través del sistema de manejo de incidencias para dejar registro de la necesidad y de la autorización.

I. En caso de vacaciones o ausencias mayores a ocho días el funcionario que tenga a su cargo un equipo de cómputo deberá coordinar la entrega en custodia al Jefe inmediato o a la Dirección de informática para evitar pérdida o robo del equipo y/o información durante su ausencia.
J. Para cambios de responsabilidad o reubicación de equipos de cómputo dentro de la organización, se requiere la autorización expresa de la Dirección de informática. El Almacén General no podrá asignar, realizar reasignaciones o dar equipos de baja sin dicha autorización.
K. En caso de retiro definitivo del funcionario, se debe entregar el equipo de cómputo a la Dirección de informática quien expedirá el paz y salvo correspondiente.

L. Siempre que sea posible, cada sistema de información de EBSA mostrará un mensaje de notificación de aprobación de uso del sistema, antes de conceder el acceso.
M. Los empleados remotos que accedan a la red de EBSA a través de una Red Privada Virtual- en inglés VPN (Virtual Private Network) deben ser autenticados y autorizados para emplear recursos basados en los requerimientos del negocio. No se permitirá ningún acceso externo que no esté controlado por un dispositivo de red o sistema en red.
N. En caso de acceso no autorizado a un sistema, la Dirección de informática desactivará inmediatamente cualquier cuenta o permiso que considere necesario y adoptará otras medidas que sean apropiadas para proteger la información y la infraestructura técnica.
O. Todo personal externo (contratistas, consultores, trabajadores temporales, empresas de outsourcing, etc.) debe someterse a un proceso de aprobación y autorización de acceso. Los privilegios otorgados a contratistas deben ser revocados inmediatamente cuando el proyecto haya finalizado, o cuando los empleados temporales dejen de trabajar con EBSA. La gerencia correspondiente realizará la verificación de los usuarios y privilegios asignados de las aplicaciones con alcance SOX cada tres meses.
P. El acceso a instalaciones físicas que albergan servidores, equipos telefónicos, ciberactivos críticos u otra infraestructura tecnológica debe restringirse mediante el uso de mecanismos adecuados de control de acceso electrónico. El acceso a estas áreas también seguirá el principio de mínimo privilegio y se concederá según sea necesario. Cuando las personas, como los visitantes, que normalmente no tienen acceso, requieren ingresar a estas áreas, deben estar acompañados por una persona autorizada para acceder a la zona.

    Las políticas y procedimientos relacionados con lo anterior están en desarrollo y hasta que no sean completadas, usted debe hacer todo lo posible por cumplirlas.

4. Comentarios de los usuarios

Los derechos de acceso a sistemas y aplicaciones deben ser revisados al menos una vez al año por la gerencia a través de un proceso formal documentado. Esta revisión también debe incluir los accesos dentro de las aplicaciones.

La revisión debe asegurar que todas las cuentas de usuario que no se han utilizado durante 90 días se han inhabilitado, y que ninguna cuenta haya estado inactiva por más de 180 días, ya que estas deberían haber sido eliminadas.

Acceso remoto

1. Información general

El acceso inapropiado puede exponer a los activos de información y ciberactivos críticos de EBSA a riesgos como ataques de virus, compromiso de sistemas y servicios de red y asuntos legales. Esta política describe los lineamientos establecidos para proteger la reputación de EBSA y está diseñada para minimizar la exposición potencial de EBSA a daños que pueden resultar del uso no autorizado de los recursos tecnológicos. Los daños pueden incluir la pérdida de datos sensibles o confidenciales de la compañía, la propiedad intelectual, el daño a la imagen pública o el daño a los sistemas internos críticos de EBSA.

Los recursos de información son activos estratégicos, y deben ser tratados y manejados como recursos valiosos. EBSA proporciona diversos recursos tecnológicos a sus usuarios, los cuales incluyen contratistas, trabajadores de medio tiempo y temporales, aprendices, estudiantes en práctica, proveedores de servicios y aquellos empleados por terceros para realizar trabajos en sitios tercerizados, o que han tenido acceso a los sistemas o a la información de EBSA para el desempeño de las funciones relacionadas con el trabajo. Estos sistemas deben ser utilizados con

fines comerciales para servir a los intereses de la organización, y de nuestros miembros y clientes en el curso normal de operaciones.

2. Propósito

El propósito de esta política es establecer los requisitos para el acceso remoto a los recursos informáticos de EBSA utilizando una Red Privada Virtual (VPN) o una tecnología similar de acceso remoto. Una VPN es una conexión de red privada segura construida sobre una red pública, tal como el Internet.

3. Política

A. General

i. El personal autorizado por EBSA puede utilizar los beneficios de las Redes Privadas Virtuales (VPNs) o una tecnología similar de acceso remoto.

B. SSL VPN

Este acceso es necesario para los empleados encargados de la gestión, mantenimiento o apoyo de los sistemas de producción, para los empleados que requieren este acceso para realizar sus funciones y para aquellos que tienen acceso a la información clasificada como interna.

C. Conexión con tecnología que no es de EBSA

i. El acceso a la red corporativa será permitido únicamente cuando se ha ingresado el equipo al dominio correspondiente tanto de la rede de TI como la de TO.

ii. Se prohíbe a terceros acceder remotamente al entorno de las aplicaciones mediante el uso de tecnología no corporativa, excepto cuando se acuerde contractualmente.

D. Condiciones de uso

i. Es responsabilidad de todo el personal de EBSA con privilegios de acceso remoto asegurarse de que no se les permita el acceso a redes internas de EBSA y contenido asociado, a personas no autorizadas.

ii. Todos los individuos y equipos que utilicen la tecnología de acceso remoto de EBSA, son una extensión de hecho de la red de EBSA y, como tal, están sujetos a todas las políticas y lineamientos de EBSA. Además de lo anterior, todo acceso de proveedores debe cumplir con los requisitos establecidos en la Política de Seguridad de la Información.

a. Las cuentas utilizadas por los proveedores para el acceso remoto, el mantenimiento o el soporte sólo deben habilitarse durante el período necesario y sólo con los niveles de acceso adecuados.

b. La Dirección de Informática de EBSA registrará y monitoreará el acceso remoto de los proveedores con regularidad.

c. Los usuarios de Redes Privadas Virtuales (VPN)) o una tecnología similar de acceso remoto sólo se conectarán o tendrán acceso a máquinas y recursos que tengan permisos y derechos de uso.

d. Las puertas de enlace a Redes Privadas Virtuales (VPN)) o una tecnología similar de acceso remoto que residen en la infraestructura de EBSA serán creadas, configuradas y administradas por la Dirección de Informática de EBSA.

e. El software y los certificados de Redes Privadas Virtuales (VPN) para usuarios individuales serán distribuidos de forma segura por el equipo de asistencia tecnológica.

La conexión a Redes Privadas Virtuales (VPN) de acceso remoto o una tecnología similar de acceso remoto se establecerá mediante un cifrado fuerte.

f. Los usuarios de Redes Privadas Virtuales (VPN) serán desconectados automáticamente de la red de EBSA después de quince minutos de inactividad. El usuario debe iniciar sesión de nuevo para volver a conectarse a la red. pings u otros procesos de red artificiales no se deben utilizar para mantener la conexión abierta.

g. El acceso desde un sitio remoto a una red de EBSA que contiene datos clasificados como confidenciales (según la Política de Clasificación de Información) puede requerir procedimientos adicionales de identificación y autenticación.

h. El acceso remoto se considera un privilegio y puede ser revocado en cualquier momento sin causa por el director de informática o el CISO.

Acceso de terceros

1. Información general

Un tercero incluye cualquier persona o entidad externa que no esté directamente empleada o afiliada por EBSA. Los terceros incluyen, pero no se limitan a, invitados, empresas externas y su personal, consultores, contratistas, vendedores, socios de negocios, compañías de seguridad, otros proveedores de servicios, etc. (colectivamente, "terceros").

El acceso de terceros a los sistemas de EBSA puede desempeñar un papel importante para el soporte, la administración de hardware y software y el desarrollo de sistemas. Establecer límites a lo que se puede acceder, modificar y copiar por un tercero reduce el riesgo al que EBSA se vería expuesto en caso de presentarse un incidente causado por un tercero.

La ley de protección de datos aplicable puede imponer restricciones y/o requisitos al acceso de terceros en los casos en que el tercero pueda acceder a los datos personales almacenados en las ubicaciones o sistemas de EBSA.

2. Propósito

El propósito de esta política es establecer las reglas para otorgar el acceso a terceros a la red o a los centros de datos de EBSA. Esta política está diseñada para minimizar el riesgo potencial de exposición no autorizada a las instalaciones de EBSA y a la información de los riesgos asociados al acceso de terceros.

3. Política

A. Acuerdos de tercerización

i. Todo el acceso de terceros a la información de EBSA, a los sistemas de información y a los activos de información y ciberactivos críticos debe ser autorizado y tener una necesidad comercial legítima. Antes de autorizar y conceder el acceso, se deben acordar los términos y condiciones del acceso los terceros como parte de un contrato o de un acuerdo formal de EBSA. Todo acceso autorizado de terceros debe ser limitado, monitoreado y controlado de manera apropiada.

ii. Todo acceso de terceros debe cumplir con las políticas de seguridad de la información de EBSA, con los lineamientos y con los recursos de control de seguridad relacionados. Ejemplo, Procedimientos operativos estándar, prácticas, directrices, etc., según lo definido en el respectivo acuerdo.

iii. La seguridad de los activos de información, ciberactivos críticos y sitios de EBSA no debe ser reducida o comprometida por la introducción de productos, servicios, actividades y/o acuerdos de tercerización.

iv. En caso de que terceros tengan acceso a información no clasificada como pública se puede requerir el uso un acuerdo adicional de no divulgación.

B. Desarrollos de Terceros

Los terceros que diseñan o personalizan un software específicamente para EBSA, deben someterse a actividades adicionales de debida diligencia para asegurar la protección de la organización.

Apéndice D

Política de contraseñas

1. Información general

La autenticación de contraseñas garantiza que los usuarios están autorizados a acceder a los sistemas y tienen los derechos y permisos adecuados para hacerlo. Una contraseña segura se define como una contraseña que es razonablemente difícil de adivinar en un corto período de tiempo, ya sea a través de la adivinación humana o del uso de software especializado. Los usuarios deben asegurarse de que las contraseñas se construyen, utilizan y protegen de manera segura de acuerdo con esta política.

2. Propósito

El propósito de esta política es establecer los criterios para la creación de contraseñas seguras, la protección de esas contraseñas y su frecuencia de cambio. Los ID de usuario y las contraseñas son la primera línea de defensa en la protección de un entorno técnico. La combinación de un ID de usuario y una contraseña proporciona acceso autenticado a los sistemas y servicios de EBSA.

3. Política

A. Las contraseñas deben ser controladas a través de un proceso formal de administración. Se deben implementar los siguientes controles para mantener la seguridad de las contraseñas:
   i. Se debe prohibir mostrar las contraseñas cuando estas son ingresadas. ii. Las contraseñas deben cambiarse siempre que se sospeche que el sistema o la contraseña están comprometidos.
   iii. Las contraseñas de usuario no deben ser compartidas.
   iv. Los usuarios deben evitar mantener un registro de las contraseñas, por ejemplo, en papel, en un archivo de software o en un dispositivo portátil.
   v. La identidad del usuario debe ser verificada utilizando métodos documentados antes de realizar restablecimientos de contraseñas.

B. Reglas de las contraseñas de cuentas de usuario
   i. Cuando se utiliza un solo factor de autenticación (por ejemplo, una contraseña) para asegurar el acceso a datos o sistemas, los usuarios deben seleccionar contraseñas de calidad de al menos ocho (8) caracteres las cuales son:

      a. Fáciles de recordar.

      b. No son iguales al ID de usuario.

      c. No se basan en cambios incrementales. Ejemplo. Contraseña, Contraseña1, Contraseña, etc.

      d. No se basan en nada que alguien pueda adivinar u obtener fácilmente usando información relacionada con esa persona, como nombres y apellidos. No se deben usar palabras como: Ebsa, Inicio, Prueba, Informatica, meses del año, últimos 5 años y sus combinaciones: ejemplo: Mayo2023, Ebsa2023.

      e. Utilizan una combinación de tres de las siguientes cuatro:

         - Letra mayúscula.
         - Letra minúscula.

- Números.
- Caracteres especiales.

C. Cuentas privilegiadas

i. Las cuentas privilegiadas incluyen cualquier tipo de cuentas para:

a. Sistemas operativos;

b. Cuentas de dispositivos de red;

c. Administración de aplicaciones;

d. Administración de dominios.

ii. Las contraseñas de estas cuentas deben seguir los requisitos de contraseña estándar.

iii. Se deben cambiar las contraseñas de los dispositivos de red al menos una vez al año.

iv. Cuando las cuentas privilegiadas son compartidas, sus contraseñas deben cambiarse como se documentó anteriormente, así como cuando alguien con conocimientos ya no necesita este nivel de acceso, como en caso de transferencia interna, salida de la organización o similar.

Excepción: Para cuentas de servicio que deben mantener una contraseña permanente debido a que son utilizadas para configuración de servicios en las aplicaciones no se activará el parámetro de caducidad de contraseña, para lo cual el director de informática semestralmente monitorea que las cuentas de administración de bases de datos, sistemas operativos y firewall tengan un responsable asignado y generará un reporte en el cual se documenten los hallazgos.

D. Responsabilidades del usuario

i. Los usuarios son responsables de TODA la actividad que se produce con su ID de usuario.
   a. Si se cree que una contraseña es conocida por otros, esta debe ser cambiada.
   b. Si un usuario cree que su cuenta ha sido comprometida y está siendo utilizada por otros, el usuario debe notificar a la Dirección de Informática inmediatamente.
   c. Las contraseñas deben mantenerse confidenciales y no deben ser reveladas a ninguna otra persona por ningún motivo.
   d. Los usuarios no deben mantener un registro de sus contraseñas (por ejemplo, papel, registro electrónico o registro contenido en un dispositivo portátil, etc.) a menos que el método de almacenamiento haya sido aprobado por La Dirección de Informática.

E. Reglas de las contraseñas de usuario - Sistema de aplicación

i. Los servicios, sistemas y plataformas deben:

   a. Exigir a los usuarios que cambien las contraseñas al menos una vez cada 60 días.
   b. Requerir cambios de contraseña para cuentas privilegiadas al menos cada 60 días a excepción de las cuentas de servicio mencionadas anteriormente.
   c. Impedir que los usuarios reutilicen o reciclen las últimas cinco (5) contraseñas.
   d. Hacer cumplir las reglas de las contraseñas (consulte "Reglas de las contraseñas de cuentas de usuario" más arriba).
   e. Forzar a los usuarios a cambiar la contraseña en el primer inicio de sesión tanto para los nuevos usuarios como para los usuarios que requieran restablecimiento de contraseña.

f. Bloquear un ID de usuario después de no más de tres (3) intentos fallidos repetidos.
g. Solicitar a la Dirección de Informática restablecer la contraseña de una cuenta bloqueada.
h. Asegurar que las contraseñas no se incluyan en ningún proceso de inicio de sesión automático (por ejemplo, almacenado en una macro o una tecla funcional).
i. No mostrar las contraseñas en la pantalla de inicio.
j. Cambiar los valores predeterminados suministrados por el proveedor antes de instalar un sistema en la red incluyendo contraseñas. Ejemplo, el protocolo de gestión de red simple SNMP (protocolo de administración de red) y la eliminación de cuentas innecesarias.
k. Asegurar las contraseñas de acuerdo con la política de cifrado de datos. Para el almacenamiento de las contraseñas en reposo, se debe implementar cifrado o hash usando algoritmos aprobados.

Apéndice E

Política de cifrado de datos

1. Información general

La encriptación es un método para transformar información clara y significativa en una forma cifrada e ininteligible. El uso del cifrado garantiza que la información cifrada conserve su confidencialidad, autenticidad e integridad.

2. Propósito

El propósito de esta política es proporcionar orientación sobre el uso efectivo del cifrado. Abordar el riesgo de usar algoritmos de encriptación inadecuados y el riesgo de usar soluciones de encriptación no autorizadas.

3. Política

A. General

i. Los controles de cifrado deben considerarse para proteger la información clasificada como confidencial de la visualización no autorizada o manipulación indebida.
ii. Los algoritmos de cifrado y el sistema de encriptación utilizado deben ser bien aceptados en la industria durante un período de tiempo prolongado.
iii. Los algoritmos de cifrado se obtendrán de tecnologías de seguridad reconocidas y establecidas.
iv. El tipo, la intensidad y la calidad del algoritmo de cifrado deben basarse en el nivel de protección necesario para que la información se cifre.
v. Las claves de cifrado estarán protegidas contra la modificación, destrucción y divulgación no autorizada durante el ciclo de vida de la clave (generación, distribución, archivado, actualización, revocación y destrucción):
    a. Sólo el personal autorizado de la Dirección de Informática tendrá acceso a las claves de cifrado. El acceso a las claves de cifrado se basará en criterios de "necesidad de conocimiento".
    b. Las actividades de gestión de claves de cifrado se registrarán.
    c. Las claves de cifrado, incluidas las claves privadas asociadas con los empleados, no se almacenarán en texto claro (por ejemplo, en archivos de texto, archivos de Microsoft Word, etc.) y sólo cuando sea necesario para permitir la funcionalidad del sistema.
    d. Todo el uso de la tecnología de cifrado debe ser manejado de manera tal que permita que el personal de informática de EBSA apropiado tenga acceso rápido a todos los datos, para propósitos de investigación y continuidad del negocio.
    e. Esta política se implementará una vez que se identifique una solución de cifrado.

B. Transmisión de datos

i. Cuando se transmite información clasificada como confidencial, la información debe encriptarse en todo momento, interna o externamente.

C. Almacenamiento de datos

i. Toda la información clasificada como confidencial debe ser cifrada.
ii. Las credenciales de autenticación de contraseña deben estar cifradas cuando se almacenan de forma recurrente o se transmiten a través de la red. Las credenciales no se deben mostrar en texto claro.

D. Uso del cifrado

i. Todas las técnicas de encriptación utilizadas no deben ser más débiles que las exigidas por los requisitos legales y reglamentarios.

ii. Los viajeros pueden entrar libremente a un país con un dispositivo cifrado bajo una "exención de uso personal" siempre y cuando el viajero no cree, mejore, comparta, venda o de otra manera distribuya la tecnología de cifrado mientras su visita, basado en el "Acuerdo de Wassenaar".

iii. En algunos países, es ilegal utilizar cifrados, o el tipo de cifrado permitido puede estar fuertemente regulado.

iv. Estados Unidos Prohíbe la exportación de tecnología de cifrado, incluyendo unidades cifradas a los siguientes países:

   a. Cuba,
   b. Irán,
   c. Corea del Norte,
   d. Sudán y Siria.

Apéndice F

Política de protección contra malware

1. Información general

El malware es visto como un software hostil y a menudo como un software invasivo o como el código del programa que puede afectar seriamente la confidencialidad, integridad y disponibilidad de los activos de información y ciberactivos críticos de EBSA. Es una amenaza seria que sigue creciendo cada vez más, requiriendo recursos significativos de todas las partes para contar con un programa de malware eficaz.

2. Propósito

El propósito de esta política es proporcionar un programa de malware integral para EBSA, además de definir qué sistemas de servidores deben tener aplicaciones antivirus y/o antispyware, y además de esto contar con una política de malware bien diseñada que se esfuerce por garantizar de manera general la confidencialidad, Integridad y disponibilidad de la red de EBSA.

3. Política

Los siguientes pasos deben ser cumplidos por cualquier personal u otros que se conecten a la red de EBSA:

A. Responsabilidades de la Dirección de Informática

i. Implementar y mantener un software antivirus y/o antimalware creíble y de buena reputación.
ii. Configurar el software para realizar escaneo continuo y/o programado.
iii. Configurar todos los computadores de modo que los usuarios no puedan alterar o evitar la solución antivirus/malware.
iv. Mantener las definiciones de virus/malware actuales instaladas en todos los dispositivos de propiedad o arrendados por EBSA.
v. Habilitar un firewall, el que se suministra con el sistema operativo y/o una aplicación de firewall comercial, en todos los puestos de trabajo y servidores (según corresponda), salvo cuando no sea práctico.
vi. El software antivirus/antimalware debe generar registros, y estos registros deben conservarse durante un periodo mínimo de tres meses disponibles para análisis inmediatamente.
vii. Los equipos infectados deben eliminarse inmediatamente de la red. El equipo no debe ser conectado de nuevo a la red, hasta que sea confirmado como limpio por un recurso tecnológico adecuado. Los usuarios nunca deben intentar destruir o eliminar un virus, o cualquier evidencia de ese virus, sin la dirección del recurso tecnológico apropiado.
viii. Todos los datos introducidos y utilizados en la red, a través de dispositivos móviles o de almacenamiento portátil (dispositivos USB, CD, etc.) deben analizarse con un mecanismo de detección de virus/malware aprobado antes de ser utilizados, almacenados o instalados en cualquier sistema de EBSA.
ix. Cualquier entorno autónomo debe cumplir con esta Política a menos que el Oficial de Seguridad de la Información - en inglés "CISO" (Chief Information Security Officer) lo apruebe de otra manera.
x. En el caso de que un virus o malware sea detectado e informado, el grupo de soporte de informática realizará un análisis del incidente y determinará el impacto en el entorno informático de EBSA de acuerdo con el Instructivo para la gestión de incidentes de TI y TO.

xi. Analizar todos los archivos adjuntos de correo electrónico antes de abrirlos. El correo electrónico es un método para distribuir programas maliciosos mediante archivos adjuntos.

B. Responsabilidades del usuario:

i. Las soluciones antivirus implementadas en sistemas no deben desactivarse en ningún momento.

ii. Los contratistas, terceros o individuos cuyo equipo no sea propiedad de EBSA deben tener instalada una solución aprobada de antivirus/antimalware antes de conectarla a un activo de información o ciberactivo crítico de EBSA.

iii. Nunca abra ningún archivo adjunto del correo electrónico desde una fuente desconocida, sospechosa o poco confiable.

iv. Desconfiar de los mensajes de correo electrónico que contengan enlaces a sitios web desconocidos. Es posible que el enlace sea un ejecutable malicioso disfrazado (.exe) o que el sitio web descargue malware en su computador. No haga clic en un enlace que le haya sido enviado si no estaba esperando recibir un enlace específico.

v. Los usuarios no deben escribir, generar, copiar, recopilar, propagar, ejecutar o intentar introducir ningún código de computador diseñado para auto replicarse, dañar u obstaculizar el desempeño o el acceso a cualquier computador, red o información de EBSA.

vi. Si un usuario recibe lo que se cree que es malware, o sospecha que un equipo está infectado con malware, debe ser reportado a la Dirección de informática inmediatamente.

vii. Los usuarios nunca deben intentar destruir o eliminar malware, ni ninguna evidencia de la infección, tal proceso debe ser liderado por la Dirección de informática

C. La alta gerencia de EBSA es responsable de mantener y asegurar que la Política de Malware se adhiera a las condiciones anteriores con el propósito de cumplir con los requerimientos de seguridad organizacional establecidos y aprobados por la administración.

4. Definiciones

Término	**Definición**
Malware	Software creado y/o utilizado con el propósito de dañar diversos sistemas, tales como el código del computador, los archivos, aplicaciones y otras plataformas y servicios de tecnología de la información relevantes.
Antivirus	Software utilizado con fines de prevención, detección y eliminación de software malicioso (es decir, malware).
Virus de Computador	Se trata de un programa que tiene la capacidad de replicarse y propagarse de un computador a otro. Los virus comunes incluyen, pero no se limitan a lo siguiente: virus de arranque, virus de macro, virus de secuencias de comandos Web, etc.
Gusano	Este es un programa que puede ser autónomo, independiente y con la capacidad de replicarse y propagarse a otros computadores, infiltrando programas y destruyendo datos.
Bomba lógica	Se trata de un código que se inserta intencionalmente en un sistema de software y que inicia una función malintencionada cuando se cumplen condiciones específicas.

Adware	Este programa facilita la entrega de contenido publicitario y de materiales relacionados con un usuario a través de su navegador mientras que está navegando en Internet, o a través de algún otro tipo de interfaz. Nota: se considera malware cuando es "no autorizado" ya que hay usos legítimos de adware.
Ransomware	Tipo de malware que puede ser instalado de forma encubierta en un computador sin conocimiento o intención del usuario, restringe el acceso al sistema informático infectado de alguna manera y exige que el usuario pague un rescate a los operadores de software malicioso para eliminar la restricción.
Spyware	Recopila información vital de un sistema informático con respecto a los datos de dicho sistema y las actividades del usuario asociado. Nota: Se considera malware cuando es "no autorizado" ya que hay usos legítimos de spyware.
Troyanos	Es una pieza dañina de malware que facilita el acceso no autorizado a un sistema informático a través de tácticas y estrategias de ingeniería social.
Rootkits	Permiten el acceso no autorizado a un sistema informático y se encuentra oculto. Los rootkits pueden ocultar alteraciones de archivos, datos, etc. y son una forma grave de malware.
Keyloggers	Se trata de una captura no autorizada de las pulsaciones de teclas de un usuario en un sistema informático. Nota: Se considera malware cuando es "no autorizado", ya que hay usos legítimos del software de keylogging.

Apéndice G

Política de redes inalámbricas

1. Información general

Las redes de datos inalámbricas son atractivas por la comodidad que ofrecen. La implementación segura de equipos de red inalámbrica puede ser, sin embargo, un reto. A diferencia de las redes cableadas tradicionales, el acceso a una red inalámbrica no se limita al espacio físico de la oficina. Debido a que las señales inalámbricas penetran las paredes y los pisos, es necesario emplear las características de seguridad apropiadas para garantizar que sólo aquellas personas que estén autorizadas a acceder a los recursos de la red corporativa puedan hacerlo a través de instalaciones inalámbricas y proteger la información confidencial de EBSA que viaja a través de estas redes.

Se debe deben tomar precauciones antes de la implementación de los dispositivos inalámbricos, ya que hay varios riesgos asociados con estos dispositivos. Los siguientes son los riesgos conocidos que se han identificado están relacionados con los dispositivos inalámbricos:

- Personal no autorizado y/o empleados no autorizados, u otros, pueden acceder a redes inalámbricas tomando provecho de vulnerabilidades en las conexiones externas.
- La información no clasificada como Pública que se transmite entre dos dispositivos inalámbricos puede ser interceptada y mal utilizada.

Es posible que se despliegue equipo no autorizado (por ejemplo, dispositivos inalámbricos de clientes y puntos de acceso) para obtener acceso a los sistemas e información de EBSA.

2. Propósito

Esta política describe cómo se implementan y utilizan las redes inalámbricas, con el objetivo de proteger la red de EBSA. Describe el despliegue aceptable de la infraestructura de red inalámbrica, incluidos los requisitos de conexión física, configuración segura y métodos de acceso. También aborda los mecanismos de aplicación y la autoridad para la provisión.

3. Política

A. <u>General</u>

i. La infraestructura de red inalámbrica debe ser provista y desplegada sólo según las instrucciones del personal de la Dirección informática de EBSA.
ii. Se debe mantener y documentar un inventario de todos los Access point inalámbricos y de otros dispositivos inalámbricos.
iii. Los administradores de red deben estar al tanto de las últimas amenazas que afectan a los dispositivos inalámbricos.
iv. Todos los dispositivos inalámbricos que se administran de forma remota deben utilizar un protocolo de red seguro y cifrado (por ejemplo, HTTPS, SSH2 y SNMPv3).

v. Cada administrador debe tener credenciales de acceso únicas para la administración de sistemas y solo debe utilizar sistemas de control de acceso centrales de autenticación, autorización y responsabilidad al acceder a sesiones administrativas en dispositivos inalámbricos.

vi. Todos los relojes de los sistemas de red inalámbrica deben sincronizarse con los protocolos de tiempo de Red - en inglés "Network Protocol Time (NTP)" de los servidores centrales.

vii. Los equipos de sistemas de redes inalámbricas deben colocarse en áreas seguras donde se controle el acceso físico, las fuentes de alimentación, la temperatura y la humedad.

B. Requisitos de la política

i. Todos los Access point inalámbricos deben ser aprobados por la Dirección de Informática de EBSA.
ii. Los Access point se deben conectar a una red que este aislada de cualquier otra red (interna y DMZ), tal como una red independiente en un firewall gestionado por la empresa.
iii. Las conexiones a los recursos corporativos a través de redes inalámbricas deben hacerse utilizando protocolos de seguridad específicos.
iv. Los Access point no autorizados se definen como cualquier punto de acceso que no sea provisto por La Dirección de Informática de EBSA. Está estrictamente prohibido para cualquier persona conectar un punto de acceso no autorizado a la red de datos de EBSA o configurar su computador para actuar como un punto de acceso.

C. Configuración del dispositivo de red inalámbrica

i. El identificador de grupo de servicios - en inglés "Service Set Identifier (SSID)" y las contraseñas de acceso para administración deben cambiarse a un valor diferente al valor predeterminado de fábrica.
ii. Los Access point deben configurarse utilizando todos los mecanismos de seguridad disponibles, incluido el uso de cifrado fuerte para la autenticación.
iii. Los Access point se deben configurar para desactivar la difusión SSID.
iv. La intensidad de la señal de los Access point inalámbricos debe ser medida y reducida (donde sea posible) para cubrir solamente las áreas deseadas.
v. La autenticación de usuario para la interfaz de gestión de puntos de acceso inalámbricos debe estar habilitada.
vi. Todos los servicios no deseados y los puertos no utilizados de los Access point y de otros dispositivos inalámbricos deben estar deshabilitados.
vii. Para los Access point y otros dispositivos inalámbricos se deben seguir los procesos de configuración/control de cambios y de gestión de parches para garantizar que el equipo tenga las versiones/lanzamientos de software más recientes.
viii. El sistema operativo del sistema inalámbrico que se utiliza debe ser actual y debe estar soportado por el fabricante. El sistema operativo que se utiliza debe ser de un fabricante oficial y/o probado por un laboratorio de liberación, y no una versión beta.
ix. Los dispositivos inalámbricos deben configurarse para que conserven su configuración actual y la configuración de seguridad durante un reinicio programado o no programado o un fallo de alimentación.
x. Las configuraciones de dispositivos inalámbricos y los archivos de contraseñas deben estar respaldados y protegidos contra el acceso y divulgación no autorizados.
xi. Todos los sistemas de redes inalámbricas deben mostrar un mensaje de advertencia legal previo al proceso de inicio de sesión de ser posible.

D. Gestión de llaves inalámbricas

i. Las funciones de seguridad de los dispositivos inalámbricos deben estar activadas, incluida la autenticación sobre el canal encriptado y la característica de privacidad de WPA2 o superior.
ii. Las claves de cifrado deben cambiarse de la configuración predeterminada de fábrica.

iii. Las claves de cifrado deben seguir los requisitos descritos en la Política de cifrado.

Apéndice H

Política de registro, monitoreo y auditoría

1. Información general

El registro, monitoreo y auditoría de sistemas proporciona a EBSA la capacidad de identificar y rastrear problemas dentro de los sistemas y de algunas aplicaciones.

Un registro del sistema se compone de una lista de actividades que han tenido lugar dentro del sistema que se está registrando. Dentro del registro, cada línea se conoce como una entrada. Las entradas contienen información relacionada con un evento específico que se ha producido dentro de un sistema. Existen varios tipos de registros que se generan en el entorno informático, incluida la actividad del sistema, el tráfico de red, etc. Para los efectos de esta política, se tratarán los registros que son específicos o que contienen información de seguridad. El registro se está implementando en todos los sistemas nuevos.

Los registros de seguridad del computador son generados por varias entradas del sistema, incluyendo software de seguridad, como software antivirus, firewall, sistemas de prevención y detección de intrusos, sistemas operativos en servidores, puestos de trabajo y equipos de red como enrutadores, entre otros. En algunos casos, las aplicaciones pueden crear registros que contienen información de seguridad.

El uso de registros permite la creación de "pistas de auditoría" mediante la reconstrucción o revisión de elementos de registro generados por sistemas, procesos de aplicación y actividad asociada. Mediante el uso de procedimientos y herramientas adecuadas, se pueden utilizar pistas de auditoría para detectar infracciones de seguridad, problemas de rendimiento del sistema y fallas en las aplicaciones empresariales. Los registros de auditoría suelen contener información sobre eventos de seguridad, como intentos de autenticación, acceso a archivos, cambios en la política de seguridad, cambios en la cuenta (por ejemplo, creación y eliminación de cuentas, asignación de privilegios de cuentas) y uso de privilegios.

2. Propósito

El propósito de esta política es asegurar que los registros son recolectados y las revisiones de registros son realizadas regularmente por personas que están calificadas para entender las amenazas que enfrentan los sistemas y la manera en que estos riesgos pueden ocurrir. EBSA requiere de un medio para reconstruir y/o revisar actividades relacionadas con operaciones, procedimientos o eventos que ocurren en sus sistemas. La entrada inicial a menudo se recopila en un registro, el cual registra los eventos que ocurren dentro de los sistemas y las redes de una organización.

3. Política

A. El registro debe estar habilitado para todos los servidores, componentes de red, antimalware y cualquier otro sistema de seguridad. El registro debe configurarse para capturar la actividad de seguridad y acceso de usuarios o como se defina en los procedimientos y normas que soportan esta política. Los registros deben ser recogidos o registrados en un host físicamente separado. El acceso a este host debe ser estrictamente controlado. Los registros pueden contener información sensible y, como tal, deben estar debidamente clasificados y protegidos.

B. Para asegurar que todos los registros estén sincronizados, se debe implementar un servidor de Protocolo de Tiempo de Red (NTP) o una tecnología similar y mantenerse actualizada para configurar el tiempo en todos los dispositivos. El acceso a las funciones de fecha y hora debe restringirse únicamente al personal con una necesidad de negocio para acceder a los datos de tiempo. Cualquier cambio en la configuración de tiempo en sistemas críticos debe ser registrado, monitoreado y revisado.

C. Todos los computadores y entornos de EBSA pueden ser registrados para todos los propósitos legales incluyendo:
   i. Asegurar que el uso está autorizado.
   ii. Gestión de sistemas.
   iii. Protección contra el acceso no autorizado.
   iv. Verificación de procedimientos de seguridad.
   v. Seguridad del sistema y seguridad operacional.
   vi. Cumplimiento de las políticas de EBSA.
   vii. Detección y prevención de delitos.

D. La información capturada a través del registro puede ser examinada, registrada, copiada y usada para propósitos autorizados. El uso de computadores, redes o sistemas de EBSA constituye el consentimiento del personal para el registro de dichos sistemas.

E. Como parte del registro, el desarrollo de pistas de auditoría debe incluir la recolección y retención de los registros de actividades que se encuentran en curso sobre o con todos los sistemas de EBSA incluyendo:

   i. Los cambios de contraseña.
   ii. Todas las acciones realizadas por cualquier cuenta con privilegios raíz o administrativos.
   iii. Creaciones, cambios y/o eliminaciones de archivos.
   iv. Revisión periódica de las actividades de los programadores de aplicaciones.
   v. Creación y eliminación de objetos a nivel de sistema.
   vi. Intentos fallidos de inicio de sesión.

F. Excepto cuando no sea suministrado por el dispositivo, las siguientes variables deben incluirse en el registro del evento de pista de auditoría:
   i. El tipo de evento.
   ii. El programa o comando utilizado para iniciar el evento.
   iii. Identidad del usuario.
   iv. Dirección IP.
   v. Nombre del host.
   vi. Comando del programa.
   vii. Identidad terminal.
   viii. Fecha / hora.
   ix. Lugar de origen/ubicación de destino u objeto.
   x. ID de usuario / ID del proceso.
   xi. Acción realizada.
   xii. Éxito o fracaso de las acciones.

G. Los registros se deben mantenerse seguros y el acceso a los registros de auditoría debe restringirse solo a aquellos con una necesidad empresarial aprobada. Los registros de auditoría deben estar asegurados para que no puedan ser alterados. El acceso a éstos debe asegurarse de la siguiente manera:
   i. Sólo los individuos que tienen una necesidad relacionada con el trabajo pueden ver archivos de auditoría.
   ii. Los archivos actuales de auditoría deben estar protegidos contra modificaciones no autorizadas a través de mecanismos de control de acceso, segregación física y/o segregación de red.

iii. Los archivos de seguimiento de auditoría actuales se deben respaldar rápidamente en un servidor de registro centralizado o en un medio de comunicación que sea difícil de modificar.

iv. Los registros de las tecnologías externas (por ejemplo, inalámbricas, firewalls, DNS, correo) se deben descargar o copiar en un servidor o medio de registro interno centralizado que sea seguro.

Apéndice I

Política de manejo, almacenamiento y eliminación de datos

1. Información general

Los datos son información que es propiedad de EBSA y que apoyan su misión. El acceso a la información se proporciona según sea necesario y ya que no todos requieren acceso a toda la información, algunos sistemas de EBSA contienen información que tiene acceso restringido. Esta información debe estar protegida en consecuencia del acceso no autorizado en todas las fases del ciclo de vida de la información. Generalmente, cuanto mayor sea el riesgo para EBSA si la información se hiciera pública esto implicaría un mayor esfuerzo para asegurar su seguridad. La falta de protección de la información puede conducir a fraude, mal uso, abuso y otros resultados negativos que en última instancia pueden dañar tanto el negocio como las relaciones comerciales y las relaciones con los clientes de EBSA.

Un registro de negocios es cualquier documento relacionado con cualquier aspecto de la actividad empresarial. Los expedientes del negocio incluyen minutas de reuniones, memorandos, detalles del empleo y actividad o información de usos del negocio. Los registros de negocios pueden ser electrónicos, físicos o ambos.

La información comercial y los registros de negocios, como cualquier recurso, tienen valor tangible e intangible. Por lo tanto, es fundamental que formen parte de un programa integral de gestión del ciclo de vida de los datos que garantice que todos los registros se administren de forma adecuada y segura, sean reemplazables (en el caso de registros vitales), eliminados, conservados y/o archivados.

La retención y la capacidad de inspeccionar rápidamente los registros comerciales se ha convertido en una necesidad para detectar actividades sospechosas, amenazas internas y otras violaciones de la seguridad. Un programa de retención de registros es una tabla que describe lo siguiente:

A. El tiempo que se conservará cada documento o registro (los requisitos de retención se pueden encontrar en la Política de Retención de Documentos) como: Un registro activo (en línea o basado en papel), Un registro fácilmente accesible (fuera de línea), Un registro archivado (almacenamiento a largo plazo)
B. El motivo (legal, fiscal, histórico) para su retención, y C. La disposición final (archivo o destrucción) del registro.

Con base en el tipo y la sensibilidad de los datos, se requerirán diferentes plazos de retención, incluyendo el archivo de esa información y las directrices para su destrucción cuando llegue al final de su vida útil. En la mayoría de los casos, los requisitos comerciales son las directrices utilizadas. Sin embargo, cierta retención de información depende de los requisitos contractuales, legales / legislativos y reglamentarios.

2. Propósito

El propósito de esta política es asegurar que todos los empleados de EBSA y aquellos empleados por otros a los que se les haya concedido acceso a información o sistemas de EBSA, utilicen mecanismos físicos y técnicos para garantizar un manejo, transferencia y almacenamiento seguro de los datos a través de documentos electrónicos y físicos, impresiones, cintas, discos y otros medios. La protección no termina con el uso del computador. Los empleados también deben considerar la información que se puede guardar en los medios de comunicación y equipo previsto para su eliminación.

3. Política

A. <u>Creación</u>

El personal de EBSA crea registros como parte del curso normal de la administración de negocios. La información confidencial definida en la Política de Clasificación de la Información se considera como crítica debido al riesgo severo que representa para EBSA si los registros se manejan mal o la información se accede

o se divulga inapropiadamente. Es esencial que los registros de negocios sean creados y mantenidos adecuadamente a lo largo de todo su ciclo de vida.

B. Acceso

   i. La información confidencial requiere de un control estricto, un acceso y divulgación muy limitados, y puede estar sujeta a restricciones legales. En algunos casos, la información está restringida debido a su agrupación en un único documento, independientemente de si contiene elementos de datos confidenciales.

   ii. Solo el personal de EBSA que tenga autorización del propietario de la información puede tener acceso a información confidencial.

C. Almacenamiento

   i. El almacenamiento diario de datos debe asegurar que los datos actuales estén disponibles para el personal autorizado y que los archivos puedan ser creados y sean accesibles en caso de necesidad.

   ii. Los servidores que almacenan información deben ser escaneados regularmente en busca de vulnerabilidades del sistema, revisiones y respaldos.

   iii. Los medios de almacenamiento utilizados para archivar la información deben ser adecuados a la durabilidad esperada. A medida que los dispositivos y medios de almacenamiento lleguen al final de su ciclo de vida, la información tendrá que adaptarse a la tecnología actual.

   iv. Los sistemas (hardware y software) diseñados para almacenar y transferir información clasificada como Interna requieren protecciones de seguridad mejoradas y deben ser monitoreados de cerca.

   v. Toda la información clasificada como confidencial no debe almacenarse en medios de almacenamiento extraíbles.

D. Transporte

Se requieren los siguientes controles cuando se transporta información clasificada como confidencial:

a. Al enviar información clasificada como Confidencial, no importa el formulario, la información debe ser asegurada en un embalaje resistente a manipulación indebida.

b. Al llevar información clasificada como Confidencial, o dispositivos que contengan dicha información, asegúrese de que está físicamente asegurada en todo momento.

c. Cuando la información clasificada como Confidencial está siendo transferida por un mensajero u otro empleado externo, debe ser enviada usando un método de entrega que puede ser rastreado.

d. No elimine la información clasificada como confidencial de una ubicación segura sin la aprobación previa del propietario de la información.

E. Eliminación

   i. Todos los usuarios de sistemas de información deben gestionar la eliminación/destrucción de los archivos de datos que poseen de una manera que se proteja la confidencialidad, integridad y disponibilidad de dichos archivos.

   ii. Debe existir un proceso trimestral para identificar y borrar de forma segura todos los datos almacenados que excedan los requisitos de retención definidos.

iii. Toda la información clasificada como Interna debe ser irrecuperable antes o durante la eliminación de equipos o medios. Todos estos datos deben ser borrados irrevocablemente antes de la reutilización del equipo o de los medios de comunicación, aunque la reutilización sea dentro de la misma organización.

iv. Cortar, triturar o pulpar toda la información clasificada como interna en medios extraíbles o en papel. Esto incluye todos los productos de trabajo transitorios, como copias no utilizadas, borradores, notas, etc.

v. Cuando se esté utilizando un servicio de destrucción subcontratado, se debe solicitar un certificado de destrucción.

F. Copia de seguridad y restauración de datos

i. Deben hacerse copias de seguridad de los datos de producción regularmente para garantizar la disponibilidad de datos en caso de que se produzca un fallo en el entorno o la información se corrompa.

ii. Es necesario restaurar uno o más archivos de forma periódica para asegurar que la información sea recuperable.

iii. Los medios que contienen información respaldada deben ser almacenados en una ubicación segura que no esté dentro de las mismas instalaciones de los sistemas de producción que alojan la información en línea.

iv. Durante el transporte, los medios de respaldo deben estar asegurados en un contenedor resistente a la manipulación que no se identifique el contenido.

4. Consideraciones legales y de retención de registros

Cada período de retención de registros se basará en los requisitos legislativos nacionales, departamentales y municipales aplicables, el derecho común y las prácticas del sector, si las hubiere. En ningún caso se destruirán los registros antes de que se cumpla el período de retención interno, el cual se basa en los requisitos legales. Se pueden encontrar más detalles en la Política de retención de documentos.

5. Retención de Registros / Programa de Disposición (RRDS)

El RRDS establece las reglas de negocio para cada agrupación o serie de registros funcionales junto con el propietario oficial del registro, el período de tiempo para retener los registros, el propósito de retención incluyendo citas legales y la destrucción apropiada. La disposición de los registros es fundamental para el buen gobierno y el control de costos. El programa define la disposición para cada serie de registros. Se pueden encontrar más detalles en la Política de retención de documentos.

Apéndice J

Política de gestión del cambio tecnológico

1. Información general

Esta política discute la necesidad de que EBSA tenga una Gestión del cambio implementada para supervisar y controlar adecuadamente todos los cambios realizados en el entorno tecnológico de EBSA. Es esencial tener un adecuado proceso de gestión del cambio en su lugar, para asegurar que los riesgos potenciales asociados con el cambio del entorno tecnológico se identifiquen y mitiguen adecuadamente.

2. Propósito

El propósito de esta política es establecer una dirección de gestión y unos objetivos de alto nivel para la gestión y el control del cambio. La intención de esta política es asegurar que la implementación de la gestión del cambio y los procedimientos de control estén en su lugar para mitigar los riesgos y minimizar el impacto negativo en el servicio y para los clientes.

3. Alcance

A. Todos los cambios realizados en los entornos de producción, recuperación de desastres y preproducción están cubiertos por la Gestión de cambios.

B. Cualquier cambio o posible cambio que afecte a lo siguiente está cubierto:

a. Hardware

i. Instalación, modificación, desinstalación o reubicación de todo el equipo tecnológico utilizado para prestar servicios al cliente, incluido el hardware que proporciona servicios de red (appliance, routers, bridges, gateways, hubs, etc.).

b. Software

i. Modificaciones a sistemas operativos, métodos de acceso, productos del programa, utilidades, incluyendo software que proporciona conectividad en un entorno de red entre nodos (NT, UNIX, TCP / IP, software de monitoreo NetView, etc.).

ii. Los cambios de aplicación se están promoviendo a la producción, así como la integración de nuevos sistemas de aplicación y la eliminación de elementos obsoletos.

c. Red

i. Modificaciones a la red y conectividad relacionadas con las actividades (cableado, conectores, adaptadores de red, definición de tabla/configuración, etc.).

d. Base de datos

i. Cambios en bases de datos o archivos (implementaciones, cambios de modelos de datos, modificación de scripts, copias de seguridad/recuperaciones, extractos/cargas de datos, actualizaciones de datos y mantenimiento).

C. La administración del cambio es aplicable a todos los equipos tecnológicos de EBSA involucrados en la administración del entorno tecnológico, incluyendo proveedores y terceros.

4. Política

A. El proceso de gestión del cambio será formalmente definido y documentado. Deberá establecerse un proceso para gestionar los cambios en todos los recursos tecnológicos especificados anteriormente. Este proceso documentado incluirá responsabilidades y procedimientos de gestión, y se publicará en un lugar accesible para todas las partes afectadas.
B. Todas las solicitudes de cambio ya sean aprobadas o rechazadas se registrarán en un sistema de gestión de incidencias centralizado. La aprobación de todas las solicitudes de cambio y los resultados de las mismas se documentarán en el sistema de gestión de incidencias.
C. Se mantendrá en todo momento una pista de auditoría documentada que contenga toda la información pertinente. Esta debe incluir la documentación de la solicitud, autorización y resultado del cambio. Ningún individuo debe ser capaz de efectuar cambios en los sistemas de información de producción sin la aprobación del personal autorizado.
D. Se llevará a cabo una evaluación del riesgo para todos los cambios.
E. Cuando sea aplicable, los cambios en la producción serán probados en un ambiente aislado, controlado y representativo antes de su implementación para evaluar su impacto en las operaciones y en la seguridad, minimizar el efecto negativo sobre el medio y verificar que solo se hagan los cambios previstos y aprobados.
F. Todos los cambios deberán ser aprobados antes de su implementación. La aprobación de los cambios se hará sobre la base de criterios formales de aceptación. La autorización para implementar estos cambios será otorgada por las autoridades delegadas.
G. La implementación de los cambios sólo se llevará a cabo después de realizar las pruebas apropiadas (si aplica) y después de la aprobación por parte del personal autorizado.
H. Los procedimientos para revertir y recuperarse de cambios fallidos deberán ser documentados. En caso de que el resultado de un cambio difiera del resultado esperado, se deben tener en cuenta los procedimientos de recuperación y continuidad de la zona afectada. Se deben establecer procedimientos de reversión para asegurar que los sistemas puedan volver al estado anterior de la implementación de los cambios.
I. Se establecerán procedimientos específicos para asegurar el control, la autorización y la documentación adecuada de los cambios de emergencia.

5. Clasificación

Para entender el impacto de los cambios y el nivel de control y aprobaciones requeridos por cada uno de ellos, se define la siguiente clasificación de cambios:

Tipo de Cambio	**Definición**	**Ejemplos**
Emergencia de TO	Cambios para resolver un incidente de prioridad muy alta.	
Estándar	Cambios preautorizados y donde la aprobación es dada por adelantado por el personal autorizado, luego de la revisión y evaluación del impacto del cambio y de implementaciones que resultaron exitosas previamente.	En respuesta a las necesidades de negocio o de usuario. Para corregir fallos (Incidentes o Problemas). Para introducir elementos de configuración nuevos

Apéndice k

Política de administración de revisiones

1. Información general

Esta política analiza la necesidad de actualizar periódicamente las plataformas corporativas de EBSA con parches y cambios de configuración para hacer frente a los problemas de seguridad y vulnerabilidad identificados. Es importante asegurar que el parche se lleve a cabo en todas las máquinas y no sólo en aquellas de más valor para la organización. El parcheo no solo requerirá del esfuerzo de los administradores del sistema, sino que también requiere que el equipo de soporte de la empresa se ponga de acuerdo sobre una ventana de mantenimiento específica. La administración de parches desempeña un papel importante en el mantenimiento de una buena postura de seguridad de la empresa, pero no debe ser tratada como la solución para todas las vulnerabilidades de seguridad.

2. Propósito

El propósito de esta política es asegurar que los computadores de EBSA y otros equipos tecnológicos (por ejemplo, Access point, firewalls, servidores, etc.) estén parchados con las últimas actualizaciones apropiadas para reducir la vulnerabilidad del sistema y limitar el potencial de compromiso. Esta política se utilizará para identificar las vulnerabilidades, sus riesgos y las actividades de remediación apropiadas.

3. Política

A. Todos los parches deben ser revisados cuando se reciben e implementados dentro de un período de seis meses.
B. Se debe verificar cada alerta de vulnerabilidad y revisión de parches en los sistemas y servicios de EBSA antes de tomar cualquier acción para evitar parches innecesarios.
C. Todas las alertas deben leerse con mucho cuidado. No todos los parches están relacionados con problemas o versiones de sistemas reales presentes en EBSA.
D. La decisión de aplicar un parche y el plazo para hacerlo debe ser alcanzada siguiendo las pautas definidas en el documento *Instructivo para la gestión de actualizaciones.*
E. Todos los servidores, equipos de escritorio, sistemas portátiles y dispositivos de red, incluyendo todos los componentes de hardware y software, deben estar listados en un inventario para ayudar en los esfuerzos de revisión.
F. Todos los parches deben ser probados antes de su adopción definitiva ya que estos pueden tener efectos secundarios imprevistos.
G. Un plan de retroceso que permita la restauración segura de los sistemas a su estado previo al parche debe ser ideado antes de cualquier implementación del parche en caso de que este tenga efectos secundarios imprevistos.
H. Todos los parches deben cumplir con los requisitos de la Política de Gestión del Cambio.
I. Toda la documentación de configuración y de inventario debe ser actualizada inmediatamente para reflejar los parches aplicados.
J. Todos los parches deben descargarse directamente del proveedor del sistema u otras fuentes de confianza.
K. El origen de cada parche debe ser autenticado y su integridad debe ser verificada. Todos los parches deben someterse a una exploración antivirus cuando se descarguen.

L. Los sistemas que enfrentan más amenazas o que son más vulnerables o son críticos para la misión empresarial deben recibir mayor prioridad en el proceso de administración de parches.

4. Prueba de parches

La prueba de parches es vital para determinar si un nuevo parche afectará o no al funcionamiento normal de cualquier software existente. Es importante que esta prueba se realice en un sistema de espejo que tenga una configuración idéntica o muy similar a la del sistema de producción objetivo. Esto es para asegurarse de que la instalación del parche no provoque consecuencias no deseadas en el sistema de producción.

A. Los sistemas de gestión de parches pueden clasificarse en dos áreas:

i. Sistemas de gestión de revisiones multiplataforma. Esta categoría de productos puede manejar parches de más de un sistema operativo, o productos de diferentes proveedores.
ii. Soluciones de gestión de parches específicas de la plataforma. Esta categoría de productos solo admite parches de un proveedor o plataforma específico.

5. Terminología definida por EBSA para las actualizaciones de software

Término	**Definición**
Parche de seguridad	Es una corrección generalizada para un producto específico, que enfrenta una vulnerabilidad de seguridad. La mayoría de los proveedores proporcionan un parche mensual para hacer frente a nuevas vulnerabilidades u otros problemas que puedan afectar la seguridad del entorno.
Actualización crítica	Es una corrección ampliamente publicada para un problema específico, que trata un error crítico no relacionado con la seguridad.
Actualización	Es una corrección generalizada para un problema específico, que trata un error no crítico no relacionado con la seguridad.
Hotfix	Es un solo paquete compuesto de uno o más archivos utilizados para solucionar un problema en un producto. Las revisiones se dirigen a una situación específica del cliente, solo están disponibles a través del soporte del proveedor y no pueden distribuirse fuera de la organización del cliente sin el consentimiento legal y escrito del proveedor.
Resumen de actualizaciones	Es una colección de parches de seguridad, actualizaciones críticas, actualizaciones y revisiones publicadas por un proveedor como una oferta acumulativa o dirigida a un solo componente de producto. Este enfoque permite una implementación más sencilla de varias actualizaciones de software.

Paquete de servicio	Es un conjunto acumulativo de revisiones, parches de seguridad, actualizaciones críticas y actualizaciones desde la publicación del producto, incluyendo muchos problemas resueltos que no se han puesto a disposición a través de otras actualizaciones de software. Los paquetes de servicio también pueden contener un número limitado de cambios o características de diseño solicitados por el cliente. Los paquetes de servicio son ampliamente distribuidos y probados por el proveedor más que cualquier otra actualización de software.
Paquetes de servicio integrados	Son una combinación de un producto y un paquete de servicio.
Paquete de funciones	Es una nueva versión de funciones para un producto que añade funcionalidad, normalmente se inserta en el producto en la siguiente versión.

Apéndice L

Política de desarrollo de software

1. Información general

Para proteger mejor a la organización, la seguridad debe integrarse en las nuevas aplicaciones y sistemas desde su inicio y durante todo el desarrollo de su ciclo de vida. Los detalles incluidos en esta política son un conjunto mínimo de requisitos a considerar para desarrollar aplicaciones y bases de datos con el nivel de seguridad adecuado.
Todo software desarrollado en EBSA debe ser configurado de manera segura para proteger la información contenida en el sistema y debe hacerse en conformidad con los lineamientos de esta política. La función de Seguridad de la Información debe revisar todos los proyectos de desarrollo en la fase de iniciación para determinar el riesgo y su implicación. El plan de cumplimiento y la línea de tiempo deben programarse con la función de Seguridad de la Información.

2. Propósito

El propósito de esta política es proporcionar a los desarrolladores de aplicaciones, administradores de bases de datos y administradores un conjunto de directrices relacionadas con el desarrollo seguro de aplicaciones y bases de datos. Esta política no pretende cubrir el software comercialmente disponible como servicio.

3. Política

El ciclo de vida del desarrollo se define como un período que comienza con la concepción de un nuevo proyecto de desarrollo y termina con la retirada o eliminación del software desarrollado de todo uso activo. Un ciclo de vida de un desarrollo normalmente incluye las siguientes fases, las cuales son independientes de la metodología de desarrollo:

- Inicio
- Desarrollo/Adquisición
- Implementación
- Operación y mantenimiento
- Eliminación

A. <u>Fase de inicio</u>

i. El director de Informática debe asegurar que se lleva a cabo una evaluación que evalúa la sensibilidad y criticidad de la información a procesar por el software planificado, así como del propio sistema. Las políticas y procedimientos relacionados con lo anterior están en desarrollo y hasta que se complete el mismo, se debe hacer todo lo posible por cumplirlas. La evaluación considerará las siguientes necesidades de información y de sistema, según lo prescrito en las leyes, reglamentos, prácticas de la industria y políticas internas:

a. Seguridad de la información
b. Privacidad de la información/protección de datos
c. Disponibilidad de la información
d. Integridad de la información
e. Confidencialidad de la información

B. <u>Fase de desarrollo</u>

i. Antes de que se desarrolle una nueva aplicación o se rediseñe una aplicación existente, el director del proyecto debe haber especificado claramente los requisitos de seguridad pertinentes y asegurarse de que se incorporen a las especificaciones de diseño de software. Las alternativas deben ser revisadas con los desarrolladores y/o vendedores para que se logre un equilibrio adecuado entre los objetivos de seguridad y los del negocio (facilidad de uso, simplicidad de operación, capacidad de actualización, costo aceptable, etc.).

ii. Si el software en desarrollo se ha adquirido total o parcialmente de otra fuente, ya sea de un vendedor, otro tercero o como parte de un esfuerzo interno de desarrollo previo, el director del proyecto deberá cumplir con los estándares internos de seguridad.

iii. El Equipo de Seguridad de la Información revisará nuevos proyectos de desarrollo de software para evaluar el riesgo. Una evaluación de los riesgos de datos e información se llevará a cabo en un esfuerzo conjunto por parte del jefe del proyecto, y de los grupos de seguridad de la información y desarrollo antes de desarrollar las aplicaciones. Las políticas y procedimientos relacionados con lo anterior están en desarrollo y hasta que sean completadas, usted debe hacer todo lo posible por cumplirlas.

iv. Desarrollo de Aplicaciones Web. La funcionalidad basada en la web debe ser codificada de forma segura para asegurar que no sea vulnerable, incluyendo:

a. Control de acceso inadecuado.
b. Entrada no válida.
c. Uso malicioso de ID de usuario.
d. Uso malicioso de credenciales de cuenta y cookies de sesión.
e. Scripts de sitios (XSS).
f. Falsificación de Petición en Sitios Cruzados (CSRF).
g. Desbordamientos de buffer debido a entradas no válidas y a otras causas.
h. La inyección de SQL y otras fallas de la inyección del comando del OS, de LDAP, y de XPath.
i. Manejo incorrecto de errores.
j. Almacenamiento de cifrado no seguro.
k. Comunicaciones no seguras.
l. Denegación de Servicio (DoS).
m. Gestión de configuración insegura.

v. Prohibición de Eludir los Controles de Acceso

a. Los programadores y otro personal de orientación técnica no deben instalar trampillas u otras infraestructuras que eludan los mecanismos de control de acceso que se encuentran en las aplicaciones, sistemas operativos y/o paquetes de control de acceso.

vi. Pruebas

a. Todos los servidores deben residir detrás de un firewall. Cualquier cambio en los servidores debe ser probado en un entorno de prueba separado antes de promover los cambios en la producción. Se deben seguir las siguientes directrices para los entornos de pruebas de aplicaciones de software:
    - Los entornos de prueba/desarrollo deben estar separados con los controles de acceso adecuados para imponer la separación.
    - Debe haber una separación de tareas entre las pruebas de desarrollo y los entornos de producción.
    - Las cuentas de aplicaciones personalizadas, nombres de usuario y/o contraseñas deben eliminarse antes de que el sistema entre en producción o se active.

b. Todas las pruebas deben seguir un plan de prueba documentado y aprobado que incluya pruebas de todas las funciones de seguridad.

vii. Contraseñas

a. Cuando una aplicación no utiliza autenticación de red, la aplicación requiere de un mecanismo que de la opción de implementar la Política de contraseñas de EBSA.

viii. Cifrado

a. Si los datos se clasifican como confidenciales (es decir, números de tarjetas de crédito, números de seguridad social, información financiera, etc.) deben ser enviados por sistemas de comunicaciones electrónicas (redes) o deben ser almacenados, se debe implementar el cifrado u otras tecnologías similares para proteger los datos.

b. El algoritmo estándar es AES (Estándar de cifrado avanzado) con una fuerza de clave estándar mínima de 256 bits. Otros algoritmos de cifrado simétricos y asimétricos fuertes son aceptables.

ix. Programas Privilegiados

a. Utilice programas y cuentas privilegiadas sólo cuando sea necesario debido a los elevados derechos de acceso al sistema y al archivo. En lo posible, considere el uso de una cuenta especial menos privilegiada para realizar la operación deseada.

x. Revisión de cuentas

a. Diseñe y construya la aplicación con la capacidad de auditar y registrar el acceso de usuarios, transacciones importantes y cambios en los parámetros operativos de la aplicación.

xi. Herramientas de depuración

a. Una vez completados, los archivos de registro se deben quitar.

C. <u>Fase de implementación</u>

i. El equipo de desarrollo debe asegurarse de que las funciones de seguridad del software estén configuradas y habilitadas correctamente.

ii. El equipo de desarrollo debe asegurarse de que las pruebas de funcionalidad se realicen antes de la liberación del software para probar la funcionalidad de seguridad y verificar que el cambio no afecte adversamente la seguridad del sistema.

D. <u>Fase de operación/mantenimiento</u>

i. El equipo de desarrollo debe completar todas las actividades de seguridad requeridas de acuerdo con el plan de desarrollo de software y el programa de seguridad de la información de EBSA. Estas actividades pueden incluir copias de seguridad de software y datos, capacitación de usuarios, flujos de trabajo de administración de acceso y revisiones del sistema.

E. <u>Fase de Disposición</u>

i. El equipo de desarrollo puede mover una aplicación a otro sistema o archivar, descartar o destruir el código de la aplicación. Además, el hardware y el software pueden ser vendidos, regalados o descartados.

ii. La disposición del software con licencia debe cumplir con los requisitos de la licencia de software u otros acuerdos relevantes.

4. Uso del código fuente

Cuando una aplicación se desarrolla utilizando componentes de código fuente, éstos deben ser declarados y documentados. Para cada componente se requiere la siguiente información:

A. Un nombre.
B. Número de versión/lanzamiento
C. Donde se obtuvo el componente
D. Funcionalidad proporcionada
E. Problemas conocidos
F. Instrucciones de parcheo

Toda la información relacionada con los componentes del código fuente debe estar documentada en los documentos del proyecto, guías, etc. La documentación debe mantenerse durante la vida útil de la aplicación.

Apéndice M

Política de evaluación de riesgos

1. Información general

Las evaluaciones de riesgo tecnológico forman parte de la política de gestión del riesgo de la información con el fin de garantizar la gestión responsable y la seguridad de la información y de los recursos de información. Las evaluaciones de riesgo tecnológico se realizan para evaluar los riesgos de la información, los programas, sistemas, servicios y espacios físicos.

Para asegurar adecuadamente los activos de información y ciberactivos críticos, se requiere que la Dirección de informática responsable de la seguridad evalúe la postura de seguridad periódicamente realizando evaluaciones de vulnerabilidad y pruebas de penetración. El objetivo de realizar dichas evaluaciones es determinar la adecuación de los controles y salvaguardias existentes desde el punto de vista de los requisitos legislativos, reglamentarios o de la industria, las mejores prácticas, la eficiencia y el costo. Estas evaluaciones son a menudo útiles en la identificación de vulnerabilidades del sistema y pueden determinar la efectividad de los controles existentes para proteger la información o mitigar el riesgo. Con el conocimiento de estas vulnerabilidades, EBSA puede aplicar arreglos de seguridad u otros controles compensatorios para mejorar la seguridad del medio.

2. Propósito

El propósito de la Política de evaluación de riesgos es asegurar que el recurso de la Direccion de informática de EBSA sea responsable de realizar las evaluaciones de riesgo tecnológico trimestralmente en los sistemas informáticos corporativos con el propósito de determinar áreas de vulnerabilidad e iniciar cualquier esfuerzo de remediación requerido.

3. Política

Antes de realizar una evaluación inicial del riesgo, todos los objetivos empresariales, los activos de información y ciberactivos críticos los sistemas o recursos de información subyacentes que generan/almacenan, utilizan o manipulan los activos (hardware, software, bases de datos, redes, instalaciones, personas, etc.) críticos para lograr estos objetivos, deben ser identificados. El riesgo también puede cambiar cuando hay una alteración en las prioridades u objetivos del negocio. Tanto la gerencia como el equipo de la Dirección informática son responsables de identificar los sistemas y la información, y asignar un riesgo inicial.

Una vez que se han identificado los activos de información y ciberactivos críticos, se realiza una evaluación del riesgo para identificar amenazas y determinar la probabilidad de ocurrencia y el impacto resultante. Sobre la base de la amenaza y la probabilidad, pueden ser necesarias salvaguardas adicionales para mitigar el impacto potencial a un nivel aceptable para la administración.

A continuación, se presenta un resumen del proceso de evaluación de riesgos (se está desarrollando un proceso detallado de evaluación de riesgos):
Las evaluaciones del riesgo de seguridad tecnológica para sistemas y aplicaciones de información críticos se deben realizar anualmente como mínimo y siguiendo todas las mejoras, actualizaciones, conversiones y cambios relacionados con estos sistemas. Las evaluaciones de riesgos también son necesarias si hay un cambio en los

objetivos del negocio o en el nivel de aceptación del riesgo por parte de la administración. Las evaluaciones de riesgos pueden realizarse en cualquier sistema de información, incluyendo aplicaciones, servidores y redes, y cualquier proceso o procedimiento por el cual estos sistemas sean administrados y/o mantenidos.

La ejecución, desarrollo e implementación de programas de remediación en respuesta a las evaluaciones de riesgos de seguridad tecnológica es responsabilidad conjunta del personal de informática y del grupo responsable del área de negocio que se está evaluando.

Las evaluaciones de riesgo pueden realizarse en cualquier entidad dentro de EBSA o cualquier tercero de acuerdo con su lenguaje contractual. Las evaluaciones de riesgo pueden ser conducidas en cualquier sistema de información, incluyendo aplicaciones, servidores y redes por las cuales estos sistemas son administrados y/o mantenidos. Cuando un tercero realice las revisiones, el alcance y las entregas deben ser acordadas por EBSA antes del comienzo de cualquier trabajo. Con el fin de realizar la evaluación del riesgo, se proporcionará acceso adicional o derechos, según sea necesario, durante el período de evaluación.

Apéndice N

Política de formación para la concienciación en seguridad

1. Información general

La información es un activo comercial importante para EBSA y necesita ser protegida para asegurar su confidencialidad, integridad y disponibilidad. La conciencia en seguridad es el intercambio de conocimientos sobre la protección de los activos de información de EBSA.

La seguridad efectiva siempre dependerá de las personas. Como resultado, la seguridad sólo puede ser efectiva si todos los usuarios de los sistemas o aplicaciones de información de EBSA saben lo que se espera de ellos, cuáles son sus responsabilidades y las repercusiones de violar la seguridad.

Las actividades de concienciación en seguridad están diseñadas para presentar principios de alto nivel de protección de la información a todos los usuarios de información de EBSA. El propósito de las presentaciones de sensibilización es simplemente centrar la atención en la seguridad, con el objetivo de mejorar el conocimiento y la actitud del personal con respecto a la protección de los activos de información y los ciberactivos críticos de EBSA. Los empleados que asisten a la formación de sensibilización tienen una comprensión de sus responsabilidades, una mejor rendición de cuentas, y pueden reconocer las preocupaciones de seguridad tecnológica y responder en consecuencia.

La conciencia no puede crearse en el vacío. Es el tercer nivel en una pirámide, empezando por la política y la formación. La política, la capacitación y la concienciación van de la siguiente manera:

i. La política le dice al usuario qué hacer.
ii. El entrenamiento provee las habilidades para realizarlo.
iii. La sensibilización cambia su comportamiento.

Si los usuarios no saben lo que se supone que deben hacer, es un problema de política. Si los usuarios no tienen las habilidades para realizarla, entonces se convierte en un problema de formación. Muy a menudo, los usuarios no entienden por qué se les pide que hagan estas nuevas "cosas", y por qué son importantes. Este es un problema de comportamiento relacionado con la conciencia que requiere un cambio. Promover la conciencia de seguridad es un control preventivo. Al proporcionar esta información, los empleados toman conciencia de sus responsabilidades para mantener una buena seguridad física y lógica. Esto también puede ser una medida proactiva, ya que anima a las personas a identificar y reportar posibles violaciones a la seguridad.

El programa de entrenamiento de concientización en seguridad y el material se desarrollarán tras la aprobación de la política.

2. Propósito

El propósito de esta política es asegurar que todos los empleados de EBSA reciban capacitación adecuada de sensibilización sobre seguridad para que puedan ser responsables del cumplimiento de las Políticas de Seguridad de la Información.

3. Política

A. El programa de sensibilización en seguridad será, como mínimo, un ejercicio anual y se pondrá en marcha en colaboración con Recursos humanos y el Grupo de seguridad de la información. El entrenamiento de concientización debe ser ofrecido de manera regular, facilitando que los empleados asistan a la capacitación. Los empleados de EBSA deberán reconocer que han sido informados y que están al tanto de las Políticas de seguridad de la información y de su papel en la protección de los sistemas de información,

de los activos de información y de los ciberactivos críticos de EBSA, al momento de la contratación y anualmente desde ese momento.

B. Todos los empleados deben estar bien informados de sus responsabilidades en la protección de la información de EBSA, ya sean propietarios de información, custodios o usuarios.
C. EBSA desarrollará e implementará un programa de capacitación y sensibilización sobre seguridad de la información en toda la empresa, incluyendo planes de capacitación para asegurar que el personal de EBSA que reciba, procese o almacene información de EBSA esté al tanto de las políticas de seguridad de la información, de sus responsabilidades en seguridad y de cómo estas dos están relacionados. El contenido de la formación impartida deberá adaptarse a los sistemas, funciones y niveles técnicos específicos de los asistentes a la sesión de formación.
D. El entrenamiento de concientización en seguridad se impartirá a través de varios canales, incluyendo, pero no limitado a:
    i. Intranet
    ii. Correo electrónico, boletines informativos
    iii. Entrenamiento en línea
    iv. Programa de orientación de Recursos humanos
E. La capacitación y educación de concientización sobre la seguridad de la información cubrirá los conceptos básicos de la seguridad de la información, las políticas y procedimientos asociados y las responsabilidades individuales. Además, se capacitará a los empleados para identificar, reportar y prevenir posibles incidentes de seguridad.
F. Los gerentes de EBSA se asegurarán de que todos los empleados bajo su supervisión tengan conocimiento de las Políticas de seguridad de la información y tengan acceso a las versiones actuales de este documento.
G. Los propietarios de la información deben familiarizarse con los principios y procedimientos estándar de seguridad de la información que se aplican a los recursos de información bajo su cuidado.
H. EBSA se asegurará de que los gerentes, los administradores de sistemas y otro personal que tenga acceso a software de nivel tengan capacitación técnica adecuada para desempeñar las tareas asignadas.
I. Todas las presentaciones de capacitación y concientización sobre seguridad deberán proporcionar mecanismos formales de evaluación y retroalimentación, para abordar los objetivos inicialmente establecidos por el programa de capacitación y para alentar a la retroalimentación, las preguntas o la información relacionada con la capacitación.

3. Requisitos de seguridad

El uso de herramientas que permitan realizar monitoreo y trazabilidad permitirá tomar acciones a los eventos de seguridad.
Se deben usar herramientas que permitan la administración de actualizaciones de seguridad que faciliten su gestión tales como: Windows Server Update Services (WSUS), System Center Configuration Manager y/o algunas otras que ayuden en la gestión oportuna de las actualizaciones.
Se deben usar herramientas que permitan la protección contra virus y malware, y faciliten su respectiva eliminación.
Se deben usar herramientas que permitan el bloqueo, auditoría, detección y corrección de intrusión.

4. Requisitos de desempeño

Busque otras mejoras de seguridad: Compruebe que aplican para la infraestructura de EBSA.

5. Requisitos de disponibilidad

Revise las alertas de los distintos servidores y equipos a fin de detectar problemas fallas en la disponibilidad.
La prueba de parches, PTF, arreglos, PSU y SP es vital para determinar si su aplicación afectará o no al funcionamiento normal de cualquier software existente. Es importante que esta prueba se realice en un sistema de espejo que tenga una configuración idéntica o muy similar a la del sistema de producción objetivo (si aplica). Esto es para asegurarse que no provoque consecuencias no deseadas en el sistema de producción.

6. Requisitos de monitoreo

La Dirección de informática establecerá los mecanismos que permitan asegurar el monitoreo de los activos de información y ciberactivos críticos.

7. Responsabilidades

Es responsabilidad de la Dirección de Informática y el Comité de seguridad asegurar que se implemente el estándar y se realicen las tareas allí contenidas.

8. Referencias

Cisco
https://software.cisco.com/download/navigator.html
https://www.cisco.com/c/en/us/products/index.html
Microsoft
https://support.microsoft.com/en-us/lifecycle/search
RedHat /CentOS
https://access.redhat.com/support/policy/updates/errata
https://linuxlifecycle.com/