DIAN®

POR UNA COLOMBIA MÁS HONESTA

Seguridad en Tecnología de la Información

El emprendimiento es de todos

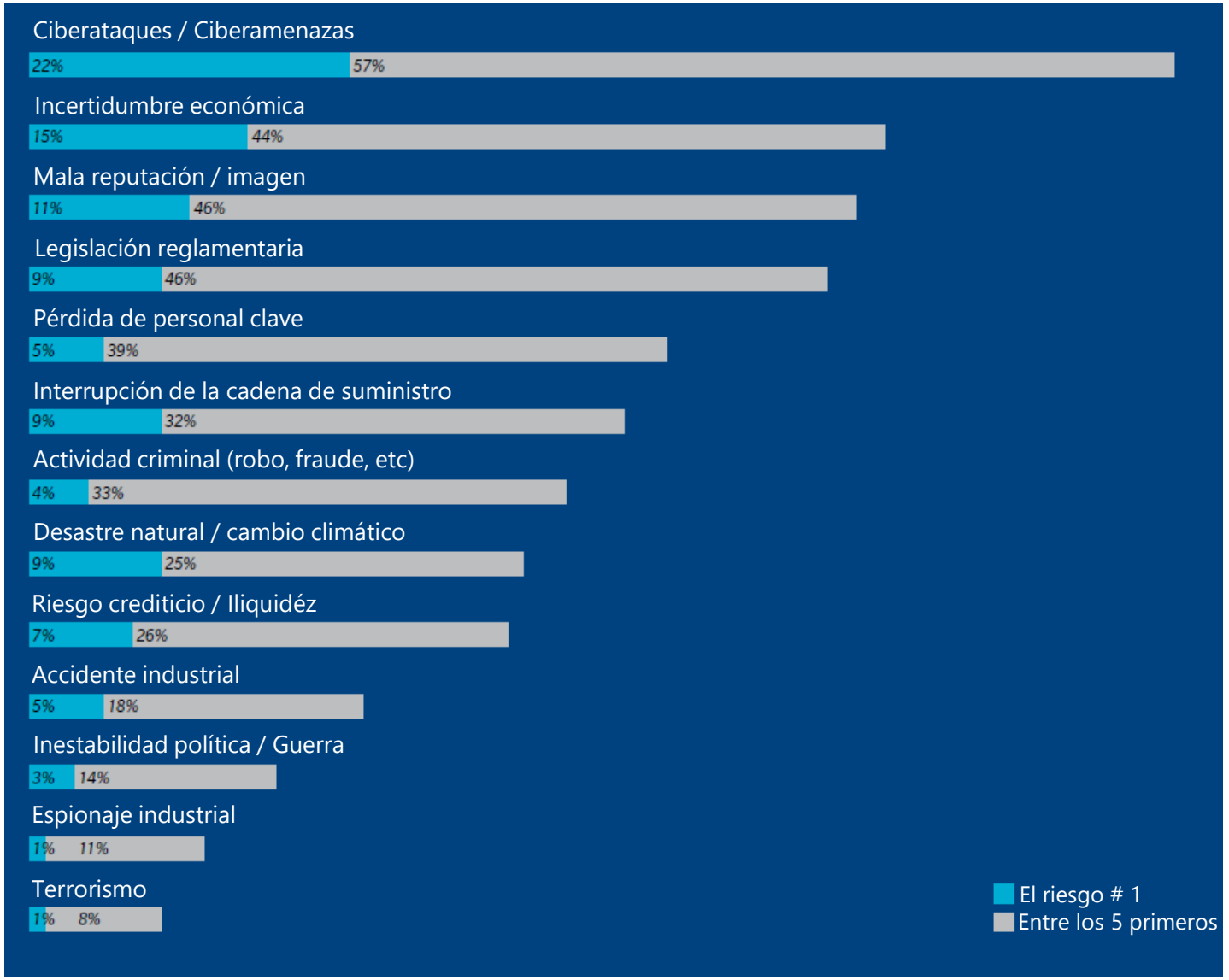
Minhacienda

Seguridad en Tecnología de la Información

Elaborado por
Operador Económico Autorizado

DIAN
POR UNA COLOMBIA MÁS HONESTA

Seguridad en Tecnología de la Información



¿Entre las siguientes amenazas comerciales, Clasifique las 5 principales preocupaciones mas importantes para su organización .

El riesgo cibernético supera a todos los demás riesgos por un amplio margen.

Fuente: Marsh Microsoft Global Cyber Risk Perception Survey 2019, Marsh & McLennan Insights analysis

DIAN
POR UNA COLOMBIA MÁS HONESTA

Seguridad en Tecnología de la Información

Operador Económico Autorizado

REQUISITO 1.9: (Importador)

Controlar el acceso y salida de información por medio de correo electrónico, soportes magnéticos, dispositivos de almacenamiento extraíble y demás.

REQUISITO 1.10: (Exportador)

Controlar el acceso y salida de información por medio de correo electrónico, soportes magnéticos, dispositivos de almacenamiento extraíble y demás.

Seguridad en Tecnología de la Información

Operador Económico Autorizado

LA MAYORÍA DE LAS VIOLACIONES DE SEGURIDAD VIENEN POR CORREO ELECTRÓNICO

96%

El correo electrónico sigue siendo el vector más común con un 96%

90%

El phishing representa más del 90% de los ataques exitosos

Fuente: Advancing Cyber Risk Management: From Security to Resilience, FireEye and Marsh & McLennan Insights

DIAN
POR UNA COLOMBIA MÁS HONESTA

Seguridad en Tecnología de la Información

Operador Económico Autorizado

Los empleados descontentos pueden robar datos fácilmente utilizando unidades USB

Una sola unidad flash puede colapsar una red completa si se administra de manera incorrecta .

los dispositivos USB son esencialmente un punto ciego para las empresas

Las organizaciones pueden emplear un sistema de gestión de seguridad USB para establecer restricciones en los dispositivos USB en su red

DIAN
POR UNA COLOMBIA MÁS HONESTA

Seguridad en Tecnología de la Información

Operador Económico Autorizado

Las unidades USB Booby-trapped pueden destruir su red.

Hay unidades USB , conocidas como Booby-trapped, que son capaces de controlar las computadoras de los usuarios sin permiso .

En 2015, los piratas informáticos desarrollaron un pen drive USB que puede entregar una carga de 220 voltios a una computadora, destruyéndolo instantáneamente

Solo unos años antes, en 2010, el infame gusano Stuxnet infectó las instalaciones nucleares iraníes, disminuyendo la eficiencia en un 30 por ciento

Las USB Booby-trapped son peligrosas porque los usuarios no son conscientes del daño que se inflige.

DIAN
POR UNA COLOMBIA MÁS HONESTA

Seguridad en Tecnología de la Información

Operador Económico Autorizado

Los dispositivos no identificados pueden causar estragos en su organización.

Las organizaciones deben implementar un sistema que permita estos dispositivos y al mismo tiempo proteger sus negocios.

Se debe tener una base de datos que contenga información sobre todos los dispositivos de almacenamiento portátiles en su red corporativa.

Programar exploraciones periódicas para controlar cómo se utilizan los dispositivos USB.

DIAN
POR UNA COLOMBIA MÁS HONESTA

La capacidad de bloquear y desbloquear dispositivos USB mejora la seguridad del USB.

Una empresa puede evitar las amenazas anteriores controlando todos los dispositivos USB en su red. Controlar dispositivos USB es tan simple como bloquearlos y desbloquearlos según sus necesidades.

Seguridad en Tecnología de la Información

Operador Económico Autorizado

REQUISITO 8.1:

Utilizar sistemas informáticos para el control y seguimiento de su negocio, sus operaciones financieras, contables, aduaneras y comerciales.

Seguridad en Tecnología de la Información

Operador Económico Autorizado

REQUISITO 8.2:

Tener políticas y procedimientos documentados de seguridad informática que comprendan: los responsables del manejo de la información, la creación, administración y asignación de roles, administración de cuentas de acceso a los sistemas de información y correo electrónico, uso de Internet; la interconexión con sistemas de información externos, el correcto uso de recursos informáticos, así como los controles necesarios que garanticen la confidencialidad de la información.

Seguridad en Tecnología de la Información

Operador Económico Autorizado

Elementos principales de una política de seguridad de la información

1. Propósito

- ✓ Cree un enfoque general para la seguridad de la información.
- ✓ Detectar y evitar violaciones de seguridad de la información, como el mal uso de redes, datos, aplicaciones y sistemas informáticos.
- ✓ Mantener la reputación de la organización y respetar las responsabilidades éticas y legales.
- ✓ Respete los derechos de los clientes, incluido cómo reaccionar ante las consultas y quejas sobre incumplimiento

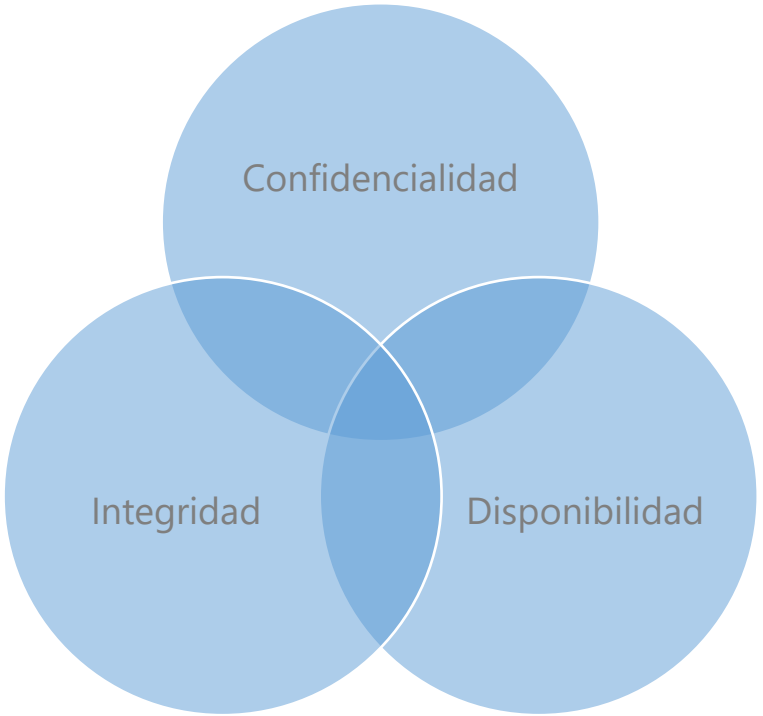
2. Alcance

- ✓ Defina el alcance a la que se aplica la política de seguridad de la información.

DIAN
POR UNA COLOMBIA MÁS HONESTA

Elementos principales de una política de seguridad de la información

3. Objetivos de seguridad de la información



Elementos principales de una política de seguridad de la información

4. Autoridad y política de control de acceso

- ✓ La política de seguridad puede tener diferentes términos para un gerente senior frente a un empleado junior. La política debe describir el nivel de autoridad sobre los datos y los sistemas de TI para cada rol organizacional.

- ✓ Los usuarios solo pueden acceder a las redes y servidores de la empresa a través de inicios de sesión únicos que exigen autenticación, incluidas contraseñas, datos biométricos, tarjetas de identificación o tokens. Debe monitorear todos los sistemas y registrar todos los intentos de inicio de sesión

Elementos principales de una política de seguridad de la información

5. Clasificación de datos

- ✓ Para garantizar que personas con niveles de autorización más bajos no puedan acceder a los datos confidenciales.
- ✓ Para proteger datos muy importantes y evitar medidas de seguridad innecesarias para datos sin importancia.

Elementos principales de una política de seguridad de la información

6. Soporte de datos y operaciones

- ✓ La mayoría de los estándares de seguridad requieren, como mínimo, cifrado, firewall y protección antimalware.
- ✓ Almacene de forma segura los medios de copia de seguridad o mueva la copia de seguridad a un almacenamiento seguro en la nube.
- ✓ Movimiento de datos: solo transfiera datos a través de protocolos seguros.

Elementos principales de una política de seguridad de la información

7. Conciencia y comportamiento de seguridad

- ✓ Comparta las políticas de seguridad de TI con su personal.
- ✓ Haga que los empleados sean responsables de notar, prevenir y denunciar tales ataques.
- ✓ Política de escritorio limpia.
- ✓ Política de uso aceptable de Internet: defina cómo se debe restringir Internet.

Elementos principales de una política de seguridad de la información

8. Responsabilidades, derechos y deberes del personal.

- ✓ Nombrar personal para llevar a cabo revisiones de acceso de usuarios, educación, gestión de cambios, gestión de incidentes, implementación y actualizaciones periódicas de la política de seguridad. Las responsabilidades deben definirse claramente como parte de la política de seguridad.

Seguridad en Tecnología de la Información

Operador Económico Autorizado

- A través de una transferencia interna, el Sr. Regal se une al equipo de Análisis de Marketing dentro de la división de Patrimonio
- Está entusiasmado por el potencial de estar asociado con un estilo de vida lujosa.
- Él tiene un interés particular en los clientes de Alto Patrimonio Neto.

- El Sr. Regal busca los medios para obtener acceso a la información personal e información no publica de los clientes
- Cuando sabe que su jefe pasa ocupado, el Sr. Regal le pide que apruebe el acceso a algunas "nuevas campañas importantes"
- Mr. Regal asegura un amplio acceso privilegiado

- El Sr. Regal desarrolla un conjunto de consultas para recopilar datos sobre los clientes más valiosos.
- A altas horas de la noche, ejecuta scripts para extraer los datos del cliente y carga los conjuntos de datos (cada uno de unos 10.000 registros) en un sitio web de intercambio de archivos poco conocido

- El estilo de vida "champaña con ingresos limitados" del Sr. Regal le resulta muy costoso, así que explora los medios para monetizar los datos de clientes de alto patrimonio que continúa acumulando.
- Se acerca a varios compradores potenciales. Pero no logra vender la información

- El señor Regal contacta a grupos criminales a través de la dark web
- El Sr. Regal comparte los datos y recibe un pago acordado.
- Se le da una memoria USB para descargas de datos adicionales que, sin que él lo sepa, tiene malware malicioso para permitir el acceso remoto no detectado por personas externas.

DIAN
POR UNA COLOMBIA MÁS HONESTA

Seguridad en Tecnología de la Información

Operador Económico Autorizado

"En 2019, de los 5 mil millones de registros robados o comprometidos, más de 2 mil millones fueron el resultado de circunstancias internas".

Risk based security:
Data Breach Trends Report 2019

"El 75% de las empresas creen que tienen los controles adecuados para mitigar la amenaza interna, pero más del 50% de las empresas tuvieron un ataque interno confirmado en los últimos 12 meses".

Crowd research partners:
2019 Insider Threat Report

DIAN
POR UNA COLOMBIA MÁS HONESTA

Seguridad en Tecnología de la Información

Operador Económico Autorizado

MITOS Y VERDADES

1. Una buena cultura de la empresa es suficiente para protegerse de los empleados internos
2. La amenaza interna proviene de contratistas
3. El riesgo interno se mitiga a través del entorno de control general
4. La actividad interna maliciosa se puede detectar de inmediato
5. La prevención de pérdida de datos (DLP) es un programa eficaz de riesgo interno
6. La amenaza interna es solo un problema para las industrias estratégicas
7. El reclutamiento tiene un buen proceso para filtrar empleados potencialmente maliciosos

DIAN®
POR UNA COLOMBIA MÁS HONESTA

Seguridad en Tecnología de la Información

Operador Económico Autorizado

REQUISITO 8.3:

Asignar cuentas individuales de acceso a la plataforma de tecnología que exijan su cambio periódico, y que cuenten con características que incrementen los niveles de seguridad.

Seguridad en Tecnología de la Información

Operador Económico Autorizado

Interceptación
Las contraseñas pueden ser interceptadas mientras viajan por la red.

Fuerza Bruta
Busqueda automatica de billones de contraseñas hasta que se encuentra la correcta.

Key logging
Instalar un keylogger para interceptar las contraseñas cuando son ingresadas.

Busqueda Manual
Detalles tales como fechas de cumpleaños o nombres de mascotas se pueden usar para adivinar las contraseñas.

Shoulder surfing
Observar a alguien escribir su contraseña.

Robar contraseñas
Las contraseñas almacenadas sin seguridad puede ser robadas, tales como las guardadas en notas en su escritorio.

Robar hashes
Robar archivos hash que pueden romperse para mostrar la contraseña.

Filtración de Datos
Usar contraseñas filtradas de un sistema para atacar otros sistemas.

Password spraying
Probar un número pequeño de contraseñas comunmente usadas para acceder a un gran numero de cuentas.

DIAN
POR UNA COLOMBIA MÁS HONESTA

Seguridad en Tecnología de la Información

Operador Económico Autorizado

Cuanto tiempo tomará descifrar su contraseña				
Longitud de las contraseñas (Caracteres)	Sólo números	Mezcla de letras mayúsculas y minúsculas	Mezcla de números y letras mayúsculas y minúsculas	Mezcla de números y letras mayúsculas y minúsculas y símbolos
3	Instantaneamente	Instantaneamente	Instantaneamente	Instantaneamente
4	Instantaneamente	Instantaneamente	Instantaneamente	Instantaneamente
5	Instantaneamente	Instantaneamente	3 segundos	10 segundos
6	Instantaneamente	8 segundos	3 minutos	13 minutos
7	Instantaneamente	5 minutos	3 horas	17 horas
8	Instantaneamente	3 horas	10 dias	57 dias
9	4 segundos	4 dias	153 dias	12 años
10	40 segundos	169 dias	1 año	928 años
11	6 minutos	16 años	106 años	71k años
12	1 hora	600 años	6k años	5m años
13	11 horas	21k años	108k años	423m años
14	4 dias	778k años	25m años	5bn años
15	46 dias	28m años	1bn años	2tn años
16	1 año	1bn años	97bn años	193tn años
17	12 años	36bn años	6tn años	14ct años
18	126 años	1tn años	374tn años	1qt años

DIAN
POR UNA COLOMBIA MÁS HONESTA

Seguridad en Tecnología de la Información

Operador Económico Autorizado

Reduzca su dependencia de las contraseñas.

1. Solo use contraseñas donde se necesiten y sean apropiadas.
2. Considere alternativas a las contraseñas tales como SSO, tokens de serguridad y soluciones biométricas.
3. Use MFA para todas las cuentas importantes y los sistemas conectados a internet.

Implementar soluciones técnicas

1. El bloqueo de contraseñas puede defender contra ataques de fuerza bruta.
2. Para bloquear, permitir entre 5-10 intentos de ingreso antes de bloquearse.
3. Considere usar monitoreo de seguridad para defendernos contra ataques de fuerza bruta.
4. Listas negras de contraseñas previene que se usen contraseñas comunes.

Proteja todas las contraseñas

1. Asegurese que las aplicaciones web corporativas que requieran autenticación usen HTTPS.
2. Proteja cualquier sistema de administración de acceso.
3. Escoja productos y servicios que protejan las contraseñas usando estandares tales como SHA-256.
4. Proteja el acceso a las bases de datos de los usuarios.
5. Dele prioridad a las cuentas de administradores, cuentas en la nube y usuarios remotos.

DIAN®
POR UNA COLOMBIA MÁS HONESTA

Seguridad en Tecnología de la Información

Operador Económico Autorizado

Ayudar a los usuarios a crear mejores contraseñas

1. Tenga en cuenta los diferentes métodos de generación de contraseñas.
2. Use generadores de contraseñas incorporados cuando use administradores de contraseñas.
3. No use requisitos de complejidad.
4. Evite crear contraseñas que sean demasiado cortas.
5. No imponga limites artificiales en la longitud de la contraseña.

Mensajes clave para la capacitación del personal

1. Enfatizar en los riesgos de reutilizar las contraseñas en cuentas de la casa y el trabajo.
2. Ayudar a los usuarios a elegir contraseñas que sean difíciles de adivinar.
3. Ayudar a los usuarios a priorizar sus cuentas de alto valor.
4. Considere hacer que la capacitación sea aplicable a la vida personal de los usuarios.

Ayude a los usuarios a hacer frente a la sobrecarga de contraseñas

1. Permitir a los usuarios almacenar de forma segura sus contraseñas, incluyendo el uso de administradores de contraseñas.
2. No expirar automaticamente las contraseñas. Solo pídale a los usuarios que cambien sus contraseñas por indicación o por compromiso.
3. Usar herramientas de delegación en lugar de compartir contraseñas. Si existe un requisito comercial urgente para compartir contraseñas, use controles adicionales para proporcionar la supervisión requerida.

DIAN
POR UNA COLOMBIA MÁS HONESTA

Seguridad en Tecnología de la Información

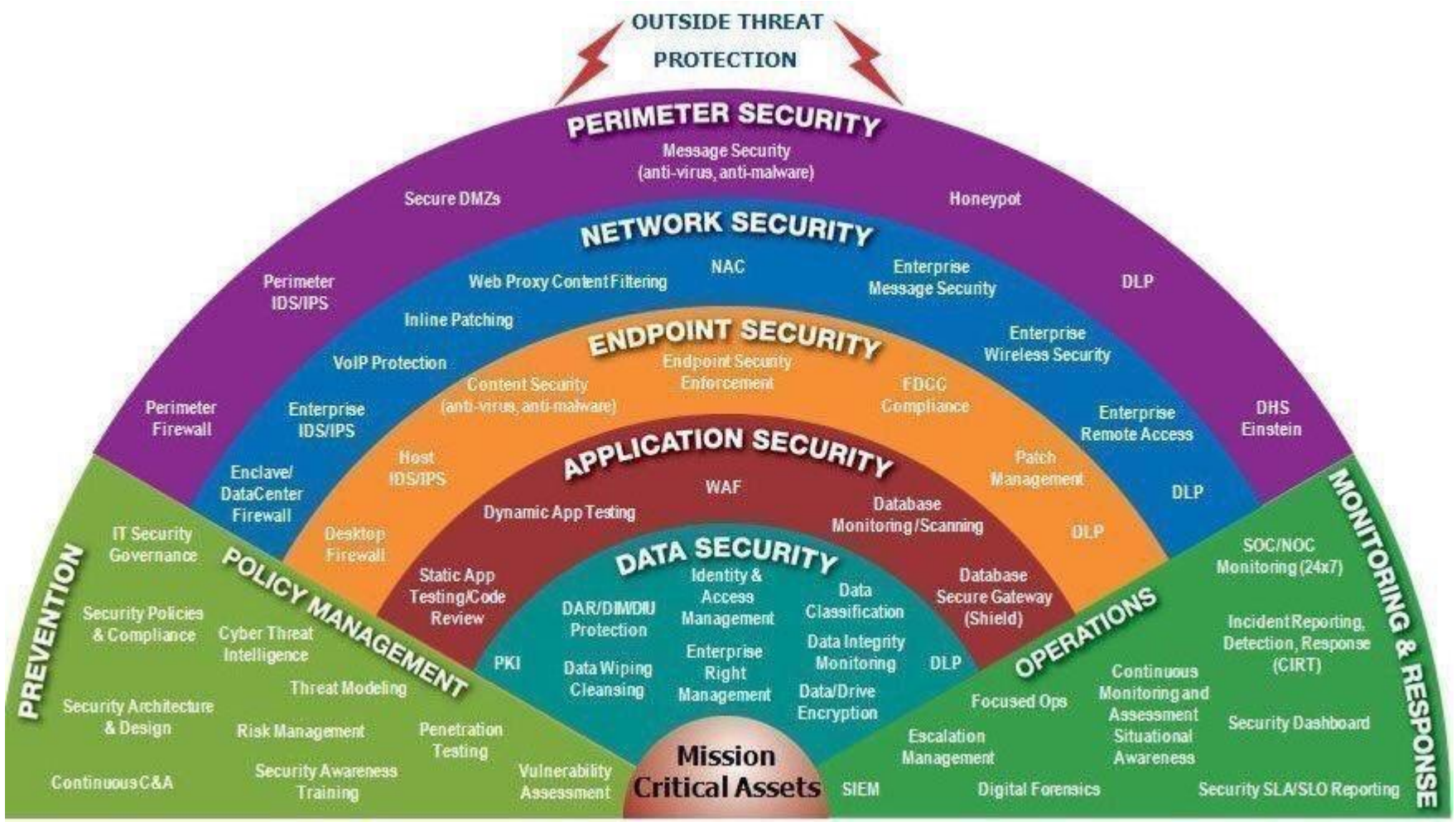
Operador Económico Autorizado

REQUISITO 8.4:

Establecer controles que permitan identificar el abuso de los sistemas de cómputo y de tecnología informática, así como detectar el acceso inapropiado y la manipulación indebida de la información.

Seguridad en Tecnología de la Información

Operador Económico Autorizado



DIAN
POR UNA COLOMBIA MÁS HONESTA

Seguridad en Tecnología de la Información

Operador Económico Autorizado

REQUISITO 8.5:

Tener un plan de contingencia informática documentado, implementado, mantenido y en proceso de mejora continua.

Seguridad en Tecnología de la Información

Operador Económico Autorizado

“Mi empresa no es foco para un cibercriminal”

“Nosotros nunca hemos recibido un ataque “

Hoy en día lo que más buscan es ser eficientes, o sea, gastar la mínima cantidad de recursos (tiempo) para conseguir su objetivo.

Por tanto, bajo este nuevo escenario, el combate contra la ciberdelincuencia se vuelve aún más asimétrico y quedó demostrado con la cantidad de brechas que se producen día a día

Seguridad en Tecnología de la Información

Operador Económico Autorizado

En ciberseguridad hay 2 procesos muy importantes:

1. La evaluación de los Riesgos, que es una actividad fundamental que debe realizarse de manera constante buscando prevenir los riesgos, y la gestión de incidentes.

2. BCP o plan de continuidad de negocios. Ambos tienen directa relación cuando el riesgo no se puede prevenir y el incidente se produce. Se deben tomar acciones para entrar en estado de contingencia y mantener la continuidad operacional.

Seguridad en Tecnología de la Información

Operador Económico Autorizado

Definir (en caso de que no tuviéramos) una política, procedimiento, herramientas y estructura necesarias para recepcionar, analizar y responder a incidentes de seguridad. Lo siguiente debería ser adherirse a algún estándar o modelo. A continuación las fases del Estándar ISO 27035 y del NIST:

Modelo ISO 27035

- ✓ Planear y preparar
- ✓ Detectar y reportar
- ✓ Evaluar y decidir
- ✓ Responder
- ✓ Lecciones aprendidas

Modelo NIST SP 800-61 Rev2

- ✓ Preparación
- ✓ Detección y análisis
- ✓ Contención, erradicación y recuperación
- ✓ Post incidente

Seguridad en Tecnología de la Información

Operador Económico Autorizado

En ciberseguridad hay 2 procesos muy importantes:

1. La Evaluación de los Riesgos, que es una actividad fundamental que debe realizarse de manera constante buscando prevenir los riesgos, y la gestión de incidentes

2. BCP o plan de continuidad de negocios. Ambos tienen directa relación cuando el riesgo no se puede prevenir y el incidente se produce. Se deben tomar acciones para entrar en estado de contingencia y mantener la continuidad operacional.

Seguridad en Tecnología de la Información

Operador Económico Autorizado

REQUISITO 8.6:

Tener un lugar físico definido como centro de cómputo y comunicaciones, con las medidas de seguridad apropiadas que garanticen el acceso únicamente del personal autorizado.

Seguridad en Tecnología de la Información

Operador Económico Autorizado

Monitoreo

- Sala bajo monitoreo constante.
- Registro de mantenimiento u otras actividades desarrolladas en el data center.
- Control de temperatura constante.
- Fácil acceso a encargados o profesionales en caso de situaciones de emergencia.

Prevención

- Hacer copias de seguridad periódicas.
- Ambiente climatizado.
- Mantenimientos periódicos.

Incendios

- Desarrollar un sistema de detección de incendios.
- Emplear material resistente al fuego para salvaguardar los equipos en el data center.

Refrigeración

- Demasiada humedad puede causar daños.
- Un ambiente muy seco puede originar descargar electrostáticas.
- Es fundamental un aire acondicionado, con la temperatura precisa.
- Aplicar medidores de temperatura y humedad.

Suministro eléctrico

- Incorporar sistemas de alimentación ininterrumpida.
- Evaluar la adquisición de un grupo electrógeno para un generador.
- Realizar pruebas periódicas de estos sistemas.

Cableado

- Cables adecuados para obtener servicios de red seguros y veloces.
- Instalación de un panel eléctrico central.
- Etiquetar el cableado.
- Separar los cables de suministro eléctrico de los de comunicaciones.

Seguridad

- Acceso restringido a la sala.
- Acompañar en todo momento al personal externo.
- Mantenimiento sólo a cargo de profesionales.
- Para proteger la información, implementar acceso con reconocimiento de huella o digital.
- No ingresar elementos ajenos a la sala de servidores.

Suelo y techo

- Habilitar un suelo falso para elevar los equipos.
- Disponer de un techo técnico para facilitar la distribución del cableado.

Seguridad en Tecnología de la Información

Elaborado por
Operador Económico Autorizado

GRACIAS

El emprendimiento es de todos | Minhacienda

DIAN
POR UNA COLOMBIA MÁS HONESTA